MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

L

L- 1

LECTURE HANDOUTS

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **I - Introduction** **Date of Lecture:**

Topic of Lecture: Computer Security Concepts ,OSI security architecture

Introduction : (Maximum 5 sentences)

- Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings.
- Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Cryptography Network
- Plaintext , Cipher text
- Enciphering **or** encryption
- Deciphering **or** decryption

Detailed content of the Lecture:

- Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings.
- Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit.
- Cryptography can reformat and transform our data, making it safer on its trip betweet computers.
- The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

Computer Security - generic name for the collection of tools designed to protect data and to thwart hackers

Network Security - measures to protect data during their transmission

Internet Security - measures to protect data during their transmission over acollection of interconnected networks

THE OSI SECURITY ARCHITECTURE

Threats and Attacks

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

SECURITY SERVICES

The classification of security services are as follows:

Confidentiality: Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties.

Eg., printing, displaying and other forms of disclosure.

Authentication: Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

Integrity: Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, eleting, creating and delaying or replaying of transmitted messages.

Non repudiation: Requires that neither the sender nor the receiver of a message be able to deny the transmission.

Access control: Requires that access to information resources may be controlled by or the target system.

Availability: Requires that computer system assets be available to authorized parties when needed.

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

- **Peer Entity Authentication**

Used in association with a logical connection to provide confidence in the identity of the entities connected.

- **Data Origin Authentication**

In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

- **Connection Confidentiality**

The protection of all user data on a connection.

- **Connectionless Confidentiality**

The protection of all user data in a single data block

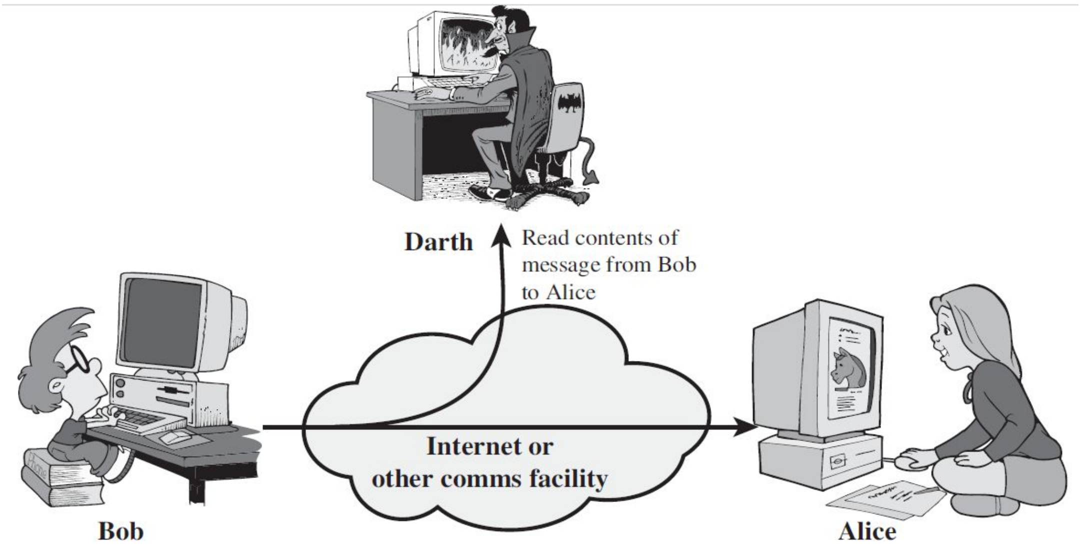
Attacks on Communication Networks

Passive attacks

- Attempts to learn or make use of information from the system but does not affect system resources
- Eaves dropping or monitoring of transmissions

Active attacks

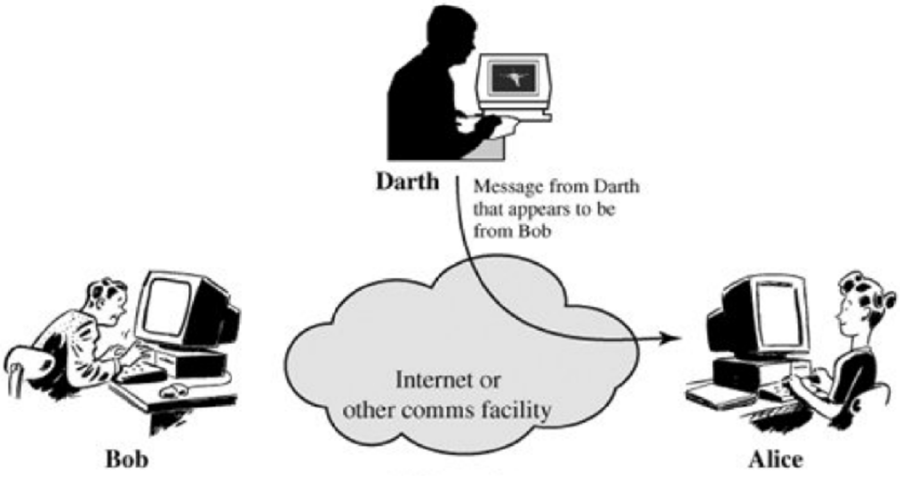
Attempts to alter system resources or affect their operation.


Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Passive Attacks

- ❑ Release of message contents / snooping
- ❑ Traffic analysis / spoofing
- ❑ Passive attacks are hard to detect!

Active Attacks


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

- ❑ Replay attack: Passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Video Content / Details of website for further learning (if any):
http://www.brainkart.com/article/The-OSI-Security-Architecture_8337/

Important Books/Journals for further learning including the page nos.:

Book: William Stallings," Cryptography and Network Security Principles and Practices", Pearson Education, 2010
Page No: (33-38)

Course Teacher

Verified by HOD

L

L-2

LECTURE HANDOUTS

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **I - Introduction** **Date of Lecture:**

Topic of Lecture: Security attacks, Services, Mechanisms
Introduction : (Maximum 5 sentences) • A service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers • A processing or communication service provided by a system to give a specific kind of protection to system resources
Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics) • **Cryptography** • **Network security** • **Encryption** **Decryption**

Detailed content of the Lecture:

- ❑ A service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers
- ❑ A processing or communication service provided by a system to give a specific kind of protection to system resources

Authentication - assurance that communicating entity is the one claimed

- o have both peer-entity & data origin authentication

Access Control - prevention of the unauthorized use of a resource

Data Confidentiality – protection of data from unauthorized disclosure

- o Connection, Connectionless, Selective-Field & Traffic-Flow Confidentiality

Data Integrity - assurance that data received is as sent by an authorized entity

- o With Recovery & Without Recovery

Non-Repudiation - protection against denial by one of the parties in a communication i.e origin & Destination

SECURITY MECHANISMS

One of the most specific security mechanisms in use is cryptographic techniques Encryption or encryption-like transformations of information are the most common means of providing security. Some of the mechanisms are:

- Encipherment
- Digital Signature
- Access Control

SECURITY ATTACKS

There are four general categories of attack which are listed below.

Interruption

An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on

availability.
e.g., destruction of piece of hardware, cutting of a communication line or disabling of file Management system.

Interception

An unauthorized party gains access to an asset. This is an attack on confidentiality.
Unauthorized party could be a person, a program or a computer.
e.g., wiretapping to capture data in the network, illicit copying of files

Modification

An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity.
e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network.

Fabrication

An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity.
e.g., insertion of spurious message in a network or addition of records to a file.

Symmetric and public key algorithms

Encryption/Decryption methods fall into two categories.

- ❑ Symmetric key
- ❑ Public key

In symmetric key algorithms, the encryption and decryption keys are known both to sender and receiver. The encryption key is shared and the decryption key is easily calculated from it. In many cases, the encryption and decryption keys are the same.

In public key cryptography, encryption key is made public, but it is computationally infeasible to find the decryption key without the information known to the receiver.

Video Content / Details of website for further learning (if any):
http://www.brainkart.com/article/The-OSI-Security-Architecture_8337/

Important Books/Journals for further learning including the page nos.:

Book: William Stallings," Cryptography and Network Security Principles and Practices", Pearson Education, 2010

Page No: 39-48

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L

L-3

LECTURE HANDOUTS

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **I - Introduction** **Date of Lecture:**

Topic of Lecture: Model for Network security

Introduction : **(Maximum 5 sentences)**

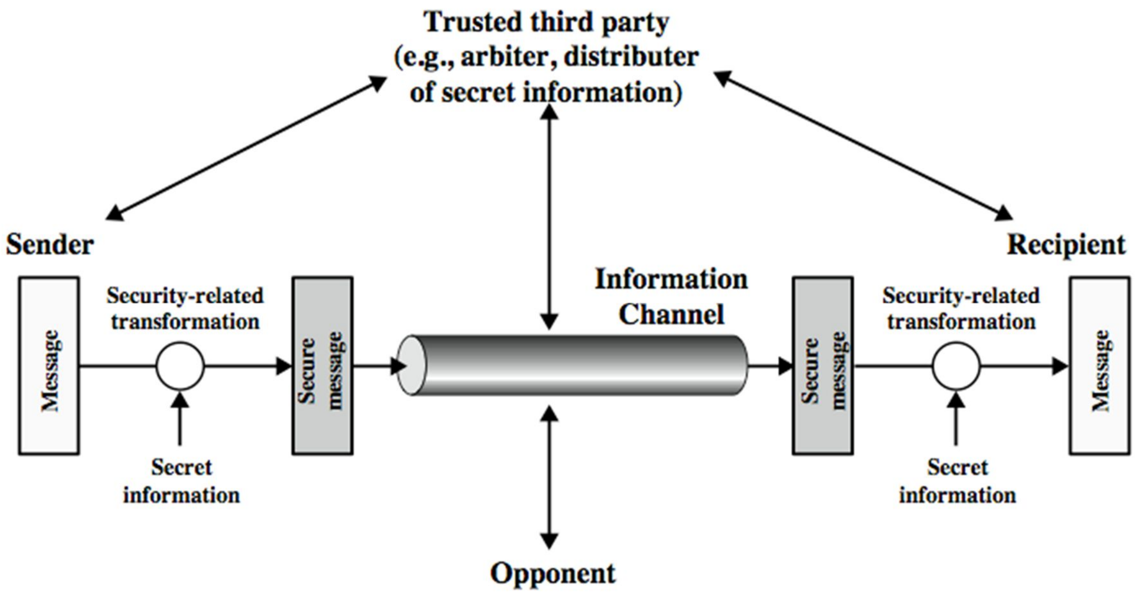
- monitoring of system for successful penetration
- monitoring of authorized users for misuse
- audit logging for forensic uses, etc.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Cryptography Network
- Plaintext , Cipher text
- Enciphering **or** encryption

Detailed content of the Lecture:
Using this model requires us to:

1. design a suitable algorithm for the security transformation
2. generate the secret information (keys) used by the algorithm
3. develop methods to distribute and share the secret information
4. specify a protocol enabling the principals to use the transformation and secret information for a security service



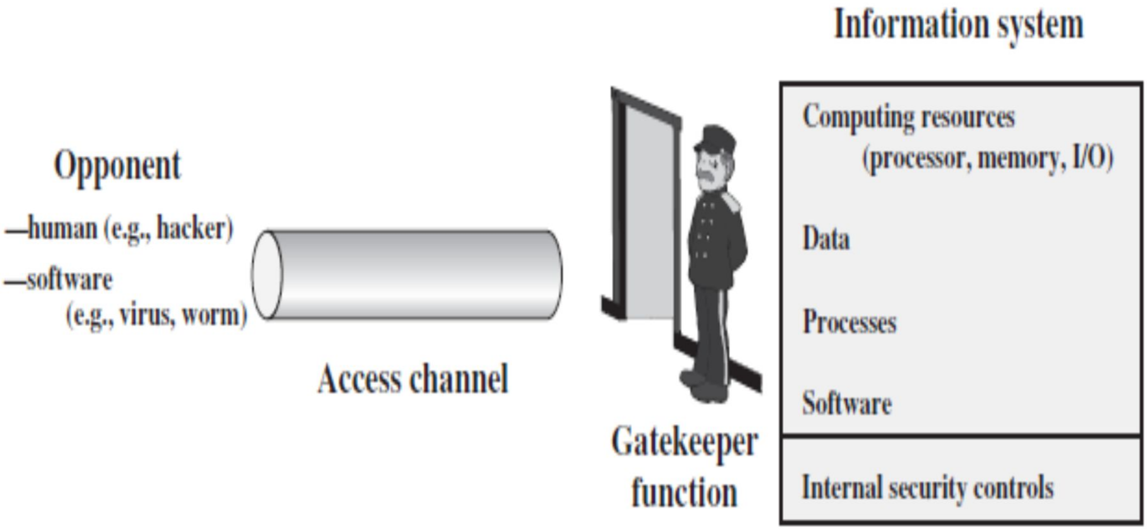
Model for Network security

- In considering the place of encryption, its useful to use the following two models from Stallings section .
- The first, illustrated in Figure 1.4, models information being transferred from one party to another over an insecure communications channel, in the presence of possible opponents.
- The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. They can use an appropriate security transform (encryption algorithm), with suitable keys, possibly negotiated using the presence of a trusted third party.
- Parts One through Four of this book concentrates on the types of security mechanisms and services that fit into the model shown here.

Model for Network Access Security

- using this model requires us to:
  1. select appropriate gatekeeper functions to identify users
  2. implement security controls to ensure only authorized users access designated information or resources

- note that model does not include:
  1. monitoring of system for successful penetration
  2. monitoring of authorized users for misuse
  3. Audit logging for forensic uses, etc.



Video Content / Details of website for further learning (if any):
http://www.brainkart.com/article/The-OSI-Security-Architecture_8337/

Important Books/Journals for further learning including the page nos.:

Book: William Stallings," Cryptography and Network Security Principles and Practices", Pearson Education, 2010
Page No: (49-50)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

L

L-4

LECTURE HANDOUTS

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **I - Introduction** **Date of Lecture:**

Topic of Lecture: Classical Encryption

Introduction : (Maximum 5 sentences)
There are two basic building blocks of all encryption techniques:

- substitution and
- transposition.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Cryptography Network
- Plaintext , Cipher text
- Enciphering **or** encryption

Detailed content of the Lecture:

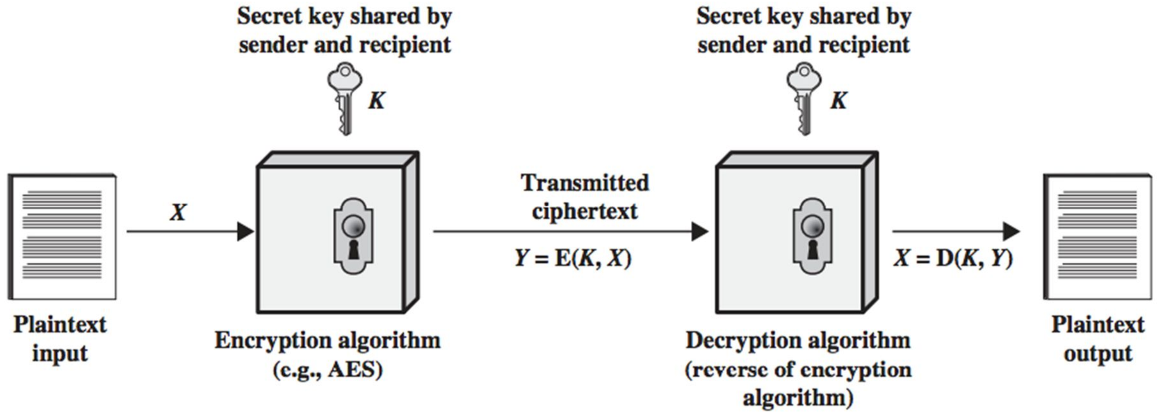
CLASSICAL CRYPTO SYSTEMS

CONVENTIONAL ENCRYPTION

- referred conventional / private-key / single-key
- sender and recipient share a common key
- all classical encryption algorithms are private-key
- was only type prior to invention of public-key in 1970‟**plaintext** - the original message

Some basic terminologies used :

- **ciphertext** - the coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - the field of both cryptography and cryptanalysis


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Video Content / Details of website for further learning (if any):
http://www.brainkart.com/article/The-OSI-Security-Architecture_8337/

Important Books/Journals for further learning including the page nos.:

Book: William Stallings," Cryptography and Network Security Principles and Practices", Pearson Education, 2010
Page No: (49-50)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

DESIGNING YOUR FUTURE
Estd. 2000

L

L-5

LECTURE HANDOUTS

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **I - Introduction** **Date of Lecture:**

Topic of Lecture: substitution techniques

Introduction : (Maximum 5 sentences)

- A service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers
- A processing or communication service provided by a system to give a specific kind of protection to system resources

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- **Cryptography**
- **Network security**
- **Encryption**
  Decryption

Detailed content of the Lecture:

Substitution Techniques

A substitution technique is one in which the letters of plain text are replaced by other letters or by numbers or symbols. The plaintext is viewed as a sequence of bits , then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

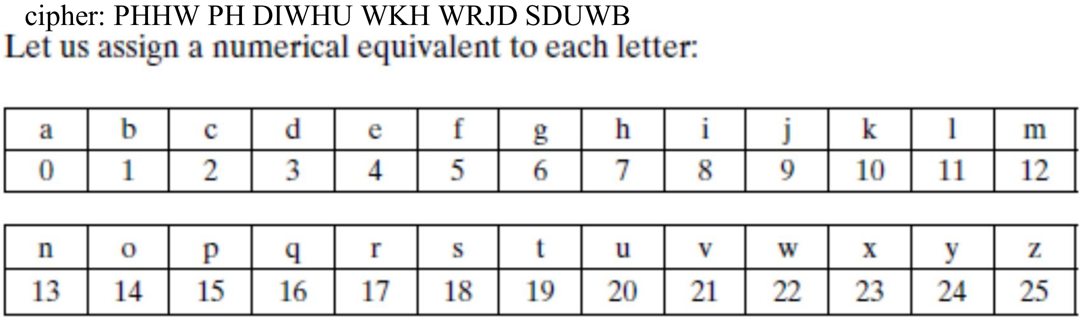
- Caesar cipher
- Monoalphabetic ciphers
- Playfair cipher
- Hill cipher
- Polyalphabetic cipher
- One-Time pad

CAESAR CIPHER

The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places or Key Value further down the alphabet or Key Value.

For example:

plain: meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB



Let us assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Then the algorithm can be expressed as follows. For each plaintext p, substitute the cipher letter C:

General Caesar algorithm is
C=E(k , p)= (p + k) mod 26
Encryption algorithm C=E(3,p)=(p+3) mod 26
Decryption algorithm is
p=D (k , C)=(C - k) mod 26

Three important characteristics of this problem enabled us to use a bruteforce cryptanalysis:

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try.
3. The language of the plaintext is known and easily recognizable.

Monoalphabetic ciphers

- Only 25 possible keys , the Caesar cipher is secure.
- Recall the assignment for the Caesar cipher:
- A **permutation** of a finite set of elements *S* is an ordered sequence of all the elements of *S*.
- For example, if S = {a, b, c}, there are six permutations of S:
  abc, acb, bac, bca, cab, cba

There are 26! or greater than 4 X 1026 possible keys. This is 10 orders of magnitude greater than the key space for DES and would seem to eliminate   brute-force techniques for cryptanalysis. Such an approach is referred to as a **monoalphabetic substitution cipher** , because a single cipher alphabet is used per message.

Playfair cipher

- The best-known multiple-letter encryption cipher is the Playfair,
- The playfair algorithm is based on the use of a 5 X 5 matrix of letters constructed using a keyword is monarchy.
- The matrix is constructed by filling in the letter of the keyword from left to right and from top to bottom , and then filling in the remainder of the matrix with the remaining letters in alphabetic order.
- The letters I and J count as one letter
  Plain Text : MEET ME TOMORROW
  Key : MONARCHY
- Separate the plaintext into pair of Letters
  ME   ET   ME   TO   MO   RR   OW
- Repeating plaintext letters that are in the same pair are separated with a filler letter , such as X
  ME   ET   ME   TO   MO   RX   RO   WX

  <u>Rule to Convert Plain text to Cipher text</u>
- Letter if in the same column – Move each letter down 1
- If it is in the same row – Move each letter right 1
- If it is form a rectangle – Swap the letter one end

  Plain text: ME   ET   ME   TO   MO   RX   RO   WX
  Cipher text: CL   KL   CL   RP   ON   AZ   MN   XZ

M	**O**	**N**	**A**	**R**
C	**H**	**Y**	**B**	**D**
E	**F**	**G**	**I/J**	**K**
L	**P**	**Q**	**S**	**T**
U	**V**	**W**	**X**	**Z**

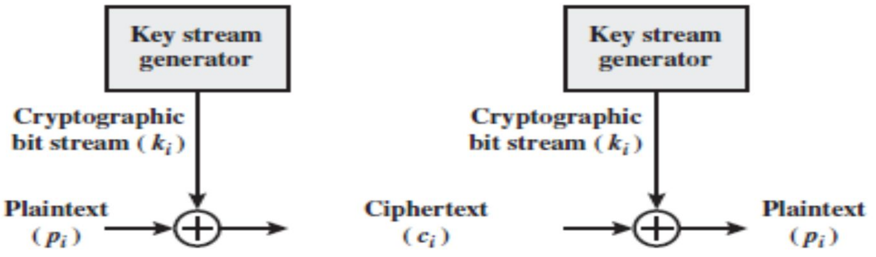
Polyalphabetic cipher

- Vigenere Cipher is a method of encrypting alphabetic text.
  It uses a simple form of polyalphabetic substitution.
- A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets .
- The encryption of the original text is done using the Vigenère square or Vigenère table.
- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.

One-Time pad

exclusive or Operator (XOR)

A	*B*	$c = a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0



Eg:, message =‘IF’

- then its ASCII code =(1001001 1000110)
- key = (1010110 0110001)

Encryption:

- 1001001 1000110 plaintext **$C_i = P_i + K_i$**
- 1010110 0110001 key
- 0011111 1110110 ciphertext **$P_i = C_i + K_i$**

Decryption:

- 0011111 1110110 ciphertext
- 1010110 0110001 key
- 1001001 1000110 plaintext

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/substitution-cipher/

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page.no: (8-28)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L

L-6

LECTURE HANDOUTS

CSE

III/V

Course Name with Code **: Cryptography and Network Security/16CSD09**

Course Teacher **:**

Unit **: I - Introduction** **Date of Lecture:**

Topic of Lecture: substitution techniques – Hill Cipher

Introduction : (Maximum 5 sentences)

- A service provided by a protocol layer of communicating open systems, which ensures adequate security of systems or of data transfers
- A processing or communication service provided by a system to give a specific kind of protection to syst resources

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- **Cryptography**
- **Network security**
- **Encryption**
  Decryption

Detailed content of the Lecture:

Substitution Techniques

A substitution technique is one in which the letters of plain text are replaced by other letters or by numbers or symbols. T plaintext is viewed as a sequence of bits , then substitution involves replacing plaintext bit patterns with cipher text patterns.

- Caesar cipher
- Monoalphabetic ciphers
- Playfair cipher
- Hill cipher
- Polyalphabetic cipher
- One-Time pad

Hill cipher

- Another interesting multiletter cipher is the Hill cipher, developed by the mathematician Lester Hill in 1929.
- Some terminology from linear algebra, matrix arithmetic modulo 26.

- **Encryption :**
  Cipher Text =(Plain Text x Key) Mod 26

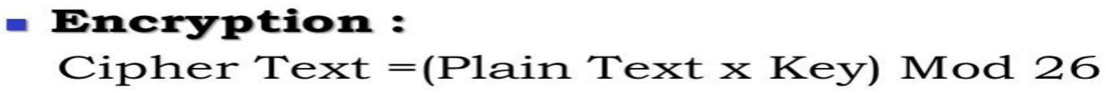
- **Decryption:**
  Plain Text =(Cipher Text x Key^{-1}) Mod 26

Plain Text : P A Y
15 0 24

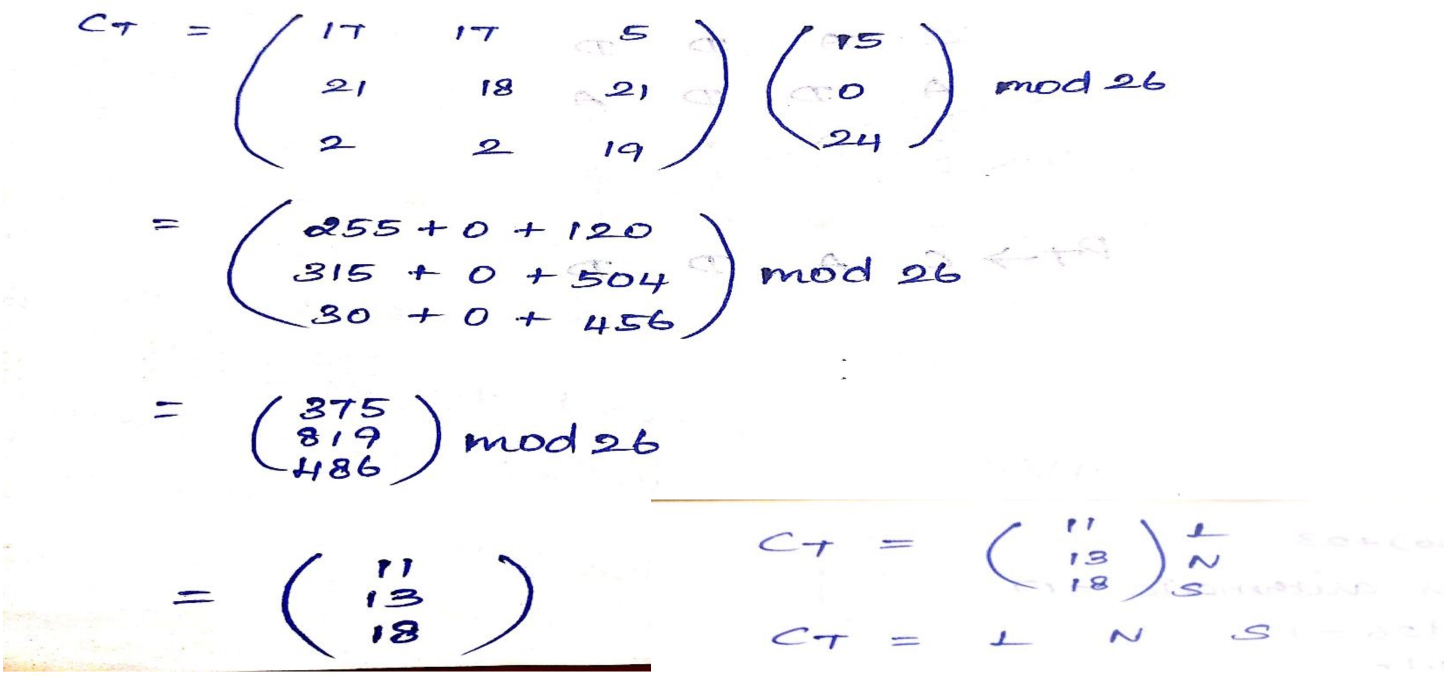
$$\text{Key:}\quad \begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix}$$

Key: R R F V S V C C T

It follows 3 X 3 Matrix



- **Encryption :**
  Cipher Text =(Plain Text x Key) Mod 26



$$C_T = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} \bmod 26$$

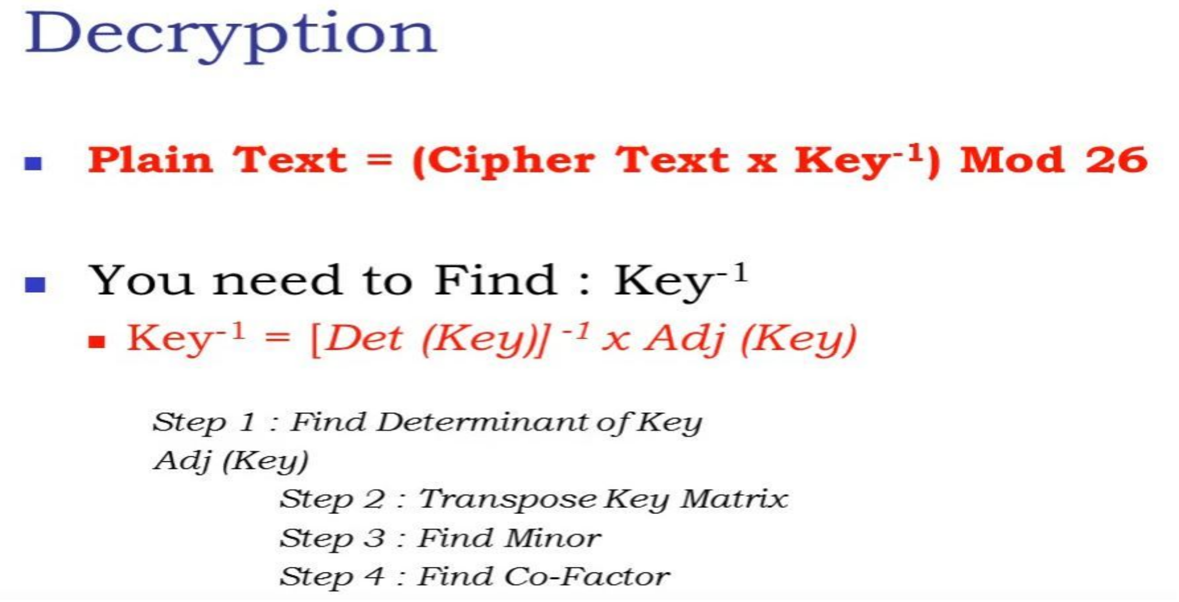
$$= \begin{pmatrix} 255 + 0 + 120 \\ 315 + 0 + 504 \\ 30 + 0 + 456 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix}$$

$$C_T = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} \begin{matrix} L \\ N \\ S \end{matrix}$$

$C_T = L \quad N \quad S$



Decryption

- **Plain Text = (Cipher Text x Key^{-1}) Mod 26**

- You need to Find : Key^{-1}
  - Key^{-1} = [*Det (Key)]$^{-1}$ x Adj (Key)*

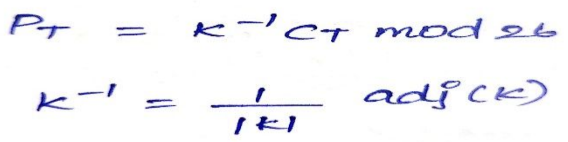
Step 1 : Find Determinant of Key

Adj (Key)

Step 2 : Transpose Key Matrix

Step 3 : Find Minor

Step 4 : Find Co-Factor



$P_T = K^{-1} C_T \bmod 26$

$$K^{-1} = \frac{1}{|K|} \text{adj}(K)$$

Step 1: Find the Determinant of Key

$$|K| = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

$$= 17(18 \times 19 - 2 \times 21) - 17(21 \times 19 - 2 \times 21) + 5(21 \times 2 - 2 \times 18)$$

$$|K| = -939$$

Modular arithmetic:

$a = qn + r$ $\quad -939 = -37(26) + 23$

$(-939 \text{ mod } 26)$ modular arithmetic

$$26 \times 37 = \underbrace{962 > 939}_{23} = 23 \text{ mod } 26$$

Decryption

- **Plain Text = (Cipher Text x Key^{-1}) Mod 26**

$$C_T = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} \begin{matrix} L \\ N \\ S \end{matrix}$$

$C_T = L \quad N \quad S$

$$= \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix}$$

$$= \begin{pmatrix} 431 \\ 494 \\ 570 \end{pmatrix}$$

$$= \begin{pmatrix} 431 \\ 494 \\ 570 \end{pmatrix} \text{mod } 26 \qquad P_T = 15 \quad 0 \quad 24$$

$$= \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} \begin{matrix} P \\ A \\ Y \end{matrix} \qquad P_T = P \quad A \quad Y$$

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/substitution-cipher/

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page.no: (8-28)

Course Teacher

Verified by HOD

LECTURE HANDOUTS

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **I - Introduction** **Date of Lecture:**

Topic of Lecture: substitution techniques - Vernam, Vigenere Cipher

Introduction : (Maximum 5 sentences)

- A service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers
- A processing or communication service provided by a system to give a specific kind of protection to system resources

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- **Cryptography**
- **Network security**
- **Encryption**
  Decryption

Detailed content of the Lecture:

Substitution Techniques

A substitution technique is one in which the letters of plain text are replaced by other letters or by numbers or symbols. The plaintext is viewed as a sequence of bits , then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

- Caesar cipher
- Monoalphabetic ciphers
- Playfair cipher
- Hill cipher
- Polyalphabetic cipher
- One-Time pad

Polyalphabetic cipher or Vigenere Cipher

- Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution.
- A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets .
- The encryption of the original text is done using the Vigenère square or Vigenère table.
- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.

In this scheme, the set of related monoalphabetic substitution rules consisting of 26 caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter. e.g.,

Caesar cipher with a shift of 3 is denoted by the key value 'd" (since a=0, b=1, c=2 and so on).
To aid in understanding the scheme, a matrix known as vigenere tableau is constructed. Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal alphabet for the plaintext runs across the top. The process of encryption is simple:

Given a key letter X and a plaintext letter y, the cipher text is at the intersection of the row labeled x and the column labeled y; in this case, the ciphertext is V.

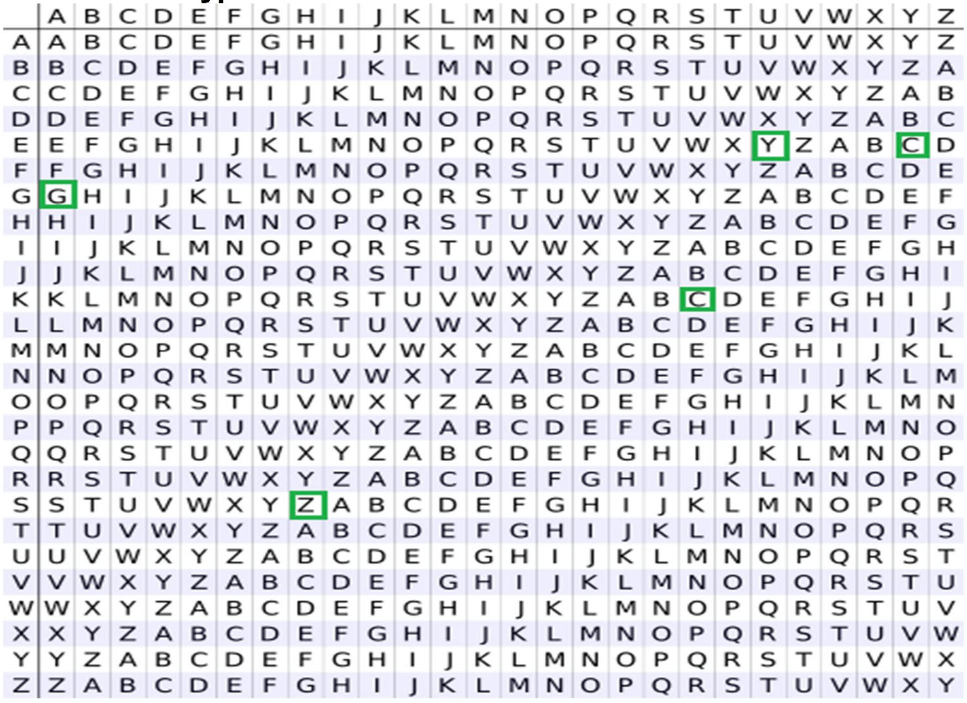
To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.

e.g.,

key = d e c e p t i v e d e c e p t i v e d e c e p t i v e

PT = wearediscoveredsaveyourself
CT = ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Table to encrypt –



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Strength of Vigenere cipher

- There are multiple ciphertext letters for each plaintext letter
- Letter frequency inforamiton is obscured.

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/substitution-cipher/

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page.no: (8-28)

Course Teacher

Verified by HOD

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **I - Introduction** **Date of Lecture:**

Topic of Lecture: Transposition techniques

Introduction : (Maximum 5 sentences) :

- A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters.
- This technique is referred to as a transposition cipher.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Permutation
- Substitution techniques

Detailed content of the Lecture:

- A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

Types are

- Rail fence
- Row Transposition Ciphers

Rail fence

- Railfence is simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Plaintext = meet at the school house

- To encipher this message with a rail fence of depth 2, we write the message as follows:

m e a t e c o l o s
e t t h s H o h u e

The encrypted message is

MEATECOLOSETTHSHOHUE

Row Transposition Ciphers-

- A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns.
- The order of columns then becomes the key of the algorithm.

e.g., plaintext = meet at the school house

Key = 4 3 1 2 5 6 7
PT = m e e t a t t
h e s c h o o
l h o u s e

CT = ESOTCUEEHMHLAHSTOETO

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is more complex permutation that is not easily reconstructed.

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/closure-properties-of-regular-languages/

Important Books/Journals for further learning including the page nos.:

1. William Stallings, Cryptography and Network Security, Prentice Hall, 2014.page no (29-32)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **I - Introduction** **Date of Lecture:**

Topic of Lecture: LFSR Sequences

Introduction : (Maximum 5 sentences) :

- A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters.
- This technique is referred to as a transposition cipher.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Permutation
- Substitution techniques

Detailed content of the Lecture:

LINEAR FEEDBACK SHIFT REGISTER (LFSR)

• An LFSR of length m consists of m stages numbered 1, 2, . . . ,m, each storing one bit and having one input and one output; together with a clock which controls the movement of data.

• The vector (k1, k2, · · · , km) would be used to initialize the shift register. During each unit of time the following operations would be performed concurrently

(i) k1 would be tapped as the next keystream bit

(ii) k2, · · · , km would each be shifted one stage to the left

(iii) the "new" value of km would be computed to be

$$\sum_{j=1}^{m-1} c_j k_j+1$$

the linear feedback is carried out by tapping certain stages of the register (as specified by the constants cj having the value "1") and computing a sum modulo 2 (which is an exclusive-or).

Applications:

• Pseudo-random number

• Pseudo-noise sequences

• Digital counters

RSA Implementation in Practice

• **Software implementations**

generally perform at 1-10 bits/second on block sizes of 256-512 bits

two main types of implementations:

▪ - on micros as part of a key exchange mechanism in a hybrid scheme

▪ - on larger machines as components of a secure mail system

• **Harware Implementations**

○ generally perform 100-10000 bits/sec on blocks sizes of 256-512 bits

○ all known implementations are large bit length conventional ALU units

Video Content / Details of website for further learning (if any):

https://www.geeksforgeeks.org/closure-properties-of-regular-languages/

Important Books/Journals for further learning including the page nos.:
William Stallings, Cryptography and Network Security, Prentice Hall, 2014.page no (29-32)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **I - Introduction** **Date of Lecture:**

Topic of Lecture: Basic Concepts in Number Theory and Finite Fields

Introduction : (Maximum 5 sentences) :

- The first stage of key-generation for RSA involves finding two large primes p, q
- Because of the size of numbers used, must find primes by trial and error
- Modern primality tests utilize properties of primes eg:
  - ○ $a_{n-1} = 1$ mod n where GCD(a,n)=1
  - ○ all primes numbers 'n' will satisfy this equation

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Encryption
- Decryption

Detailed content of the Lecture:

Primality Testing and RSA

- The first stage of key-generation for RSA involves finding two large primes p, q
- Because of the size of numbers used, must find primes by trial and error
- Modern primality tests utilize properties of primes eg:
  - ○ $a_{n-1} = 1$ mod n where GCD(a,n)=1
  - ○ all primes numbers 'n' will satisfy this equation
  - ○ some composite numbers will also satisfy the equation, and are called pseudo primes.
- Most modern tests guess at a prime number 'n', then take a large number (eg 100) of numbers 'a', and apply this test to each. If it fails the number is composite, otherwise it is is probably prime.
- There are a number of stronger tests which will accept fewer composites as prime than the above test. eg:

$$\mathrm{GCD}(a,n) = 1, \quad \text{and} \quad \left(\frac{a}{n}\right) (\operatorname{mod} n) = a^{\frac{(n-1)}{2}} (\operatorname{mod} n)$$

$$\text{where} \left(\frac{a}{n}\right) \text{is the Jacobi symbol}$$

RSA Implementation in Practice

- **Software implementations**
  - ○ generally perform at 1-10 bits/second on block sizes of 256-512 bits
  - ○ two main types of implementations:
    - ▪ - on micros as part of a key exchange mechanism in a hybrid scheme
    - ▪ - on larger machines as components of a secure mail system
- **Hardware Implementations**
  - ○ generally perform 100-10000 bits/sec on blocks sizes of 256-512 bits
  - ○ all known implementations are large bit length conventional ALU units

Group

- A set of numbers with some addition operation whose result is also in the set (closure)
- Obeys associative law, has an identity, has inverses
- If also is commutative its an Abelian group

Ring

- An Abelian group with a multiplication operation also
- Multiplication is associative and distributive over addition
- If multiplication is commutative, its a commutative ring

e.g., integers mod N for any N

Field

- An Abelian group for addition
- A ring
- An Abelian group for multiplication (ignoring 0)

e.g., integers mod P where P is prime

Divisor

b|a (“b divides a”, “b is a divisor of a”),

if a = k b for some k,

The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.

$\frac{24}{1}$, $\frac{24}{2}$ $\frac{24}{12}$

where a, b, and k are integers, and b ≠ 0

- If a|1, then a = ±1
- If a|b and b|a, then a = ±b
- Any b ≠ 0 divides 0
- If a|b and b|c, then a|c

Eg: $\frac{66}{11}$ and $\frac{198}{66} = \frac{198}{11}$ a=11, b=66 & C=198

- *If b|g and b|h, then b|(mg + nh) for arbitrary integers m and n*

$$\boxed{mg + nh = mbg1 + nbh1 = b * (mg1 + nh1)}$$

and therefore b divides mg + nh.

Video Content / Details of website for further learning (if any):
http://www.brainkart.com/article/Basic-Concepts-in-Number-Theory-and-Finite-Fields_8398/

Important Books/Journals for further learning including the page nos.:
William Stallings, Cryptography and Network Security, Prentice Hall, 2014. pg.no(228-230)

Course Teacher

Verified by HOD

Course Name with Code	**: Cryptography and Network Security/16CSD09**	
Course Teacher	**:**	
Unit	**: I - Introduction**	**Date of Lecture:**

Topic of Lecture: Euclidean algorithm

Introduction : (Maximum 5 sentences) :

- **Euclid's Algorithm** is used to find the Greatest Common Divisor (GCD) of two numbers a and n, a<n

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Encryption
- Decryption

Detailed content of the Lecture:

- The greatest common divisor (a,b) of a and b is the largest number that divides evenly into both a and b
- **Euclid's Algorithm** is used to find the Greatest Common Divisor (GCD) of two numbers a and n, a<n use fact if a and b have divisor d so does a-b, a-2b

GCD (a,n) is given by:
let g0=n
g1=a
gi+1 = gi-1 mod gi
when gi=0 then (a,n) = gi-1
eg find (56,98)
g0=98
g1=56
g2 = 98 mod 56 = 42
g3 = 56 mod 42 = 14
g4 = 42 mod 14 = 0
hence (56,98)=14

Finite Fields or Galois Fields

- Finite Field: A field with finite number of elements
- Also known as Galois Field
- The number of elements is always a power of a prime number. Hence, denoted as GF(pn)
- GF(p) is the set of integers {0,1, …, p-1} with arithmetic operations modulo prime p
- Can do addition, subtraction, multiplication, and division without leaving the field GF(p)
- GF(2) = Mod 2 arithmetic

GF(8) = Mod 8 arithmetic

- There is no GF(6) since 6 is not a power of a prime

Polynomial Arithmetic

$f(x) = a_nx_n + a_{n-1}x_{n-1} + \cdots + a_1x + a_0 = \Sigma\ a_ix_i$

1. Ordinary polynomial arithmetic:

- Add, subtract, multiply, divide polynomials,

- Find remainders, quotient.
- Some polynomials have no factors and are prime.

2. Polynomial arithmetic with mod p coefficients
3. Polynomial arithmetic with mod p coefficients and mod m(x) operations

Polynomial Arithmetic with Mod 2 Coefficients

- All coefficients are 0 or 1, e.g.,

let $f(x) = x3 + x2$ and $g(x) = x2 + x + 1$
$f(x) + g(x) = x3 + x + 1$
$f(x)$ x $g(x) = x5 + x2$

- Polynomial Division: $f(x) = q(x)\ g(x) + r(x)$
- can interpret $r(x)$ as being a remainder
- $r(x) = f(x)$ mod $g(x)$
- if no remainder, say $g(x)$ divides $f(x)$
- if $g(x)$ has no divisors other than itself & 1 say it is irreducible (or prime) polynomial
- Arithmetic modulo an irreducible polynomial forms a finite field
- Can use Euclid"s algorithm to find gcd and inverses

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/euclidean-algorithms-basic-and-extended/

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014. pg.no(68-71)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

L-12

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **I - Introduction** **Date of Lecture:**

Topic of Lecture: Fermat's theorem

Introduction : **(Maximum 5 sentences)** :

- If consider arithmetic modulo n, then a **reduced set of residues** is a subset of the complete set of residues modulo n which are relatively prime to n
- The number of elements in the reduced set of residues is called the **Euler Totient function [[phi]](n)**

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Encryption
- Decryption
- GCD

Detailed content of the Lecture:

Fermat's Little Theorem

- Euler's theorem states that for every *a* and *n* that are relatively prime:
  $\mathbf{a^{\phi(n)} \equiv 1 (mod\ n)}$
  (i.e) $a^{\phi(n)}$ mod n = 1 mod n
- An alternative form of the theorem is also useful: for 2 positive integers a and n
  $\mathbf{a^{\phi(n)+1} \equiv a\ (mod\ n)}$

Eg: $\mathbf{4^{532}}$ **mod 11**

a^{p-1} mod p = 1

So, a^{11-1} mod 11

a^{10} mod 11 = 1

Now, 4^{532} mod 11 = $4^{10(53)} * 4^{(2)}$ mod 11 [532 = 10*53 + 2]

= $1^{(53)} * 4^{(2)}$ mod 11

= 1 * 16 mod 11

4^{532} mod 11 = 16 mod 11 = 5

Video Content / Details of website for further learning (if any):
http://www.brainkart.com/article/Fermat---s-And-Euler---s-Theorems_8430/

Important Books/Journals for further learning including the page nos.:
Book: William Stallings," Cryptography and Network Security Principles and Practices", Pearson Education, 2010.Pg no: (272-278)

Course Teacher

Verified by HOD

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **I - Introduction** **Date of Lecture:**

Topic of Lecture: Euler’s theorem

Introduction : (Maximum 5 sentences) :

- If consider arithmetic modulo n, then a **reduced set of residues** is a subset of the complete set of residues modulo n which are relatively prime to n
- The number of elements in the reduced set of residues is called the **Euler Totient function [[phi]](n)**

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- Encryption
- Decryption
- GCD

Detailed content of the Lecture:

Euler Totient Function [[phi]](n)

• if consider arithmetic modulo n, then a **reduced set of residues** is a subset of the complete set of residues modulo n which are relatively prime to n

○ eg for n=10,

○ the complete set of residues is {0,1,2,3,4,5,6,7,8,9}

○ the reduced set of residues is {1,3,7,9}

• the number of elements in the reduced set of residues is called the **Euler Totient function [[phi]](n)**

• there is no single formula for [[phi]](n) but for various cases count how many elements are excluded:

p (p prime) [[phi]](p) =p-1

pr (p prime) [[phi]](p) =pr-1(p-1)

p.q (p,q prime) [[phi]](p.q) =(p-1)(q-1)

several important results based on [[phi]](n) are:

- Euler’s theorem states that for every *a* and *n* that are relatively prime:

$$\mathbf{a^{\phi(n)} \equiv 1 (mod\ n)}$$

(i.e) $a^{\phi(n)}$ mod n = 1 mod n

- An alternative form of the theorem is also useful: for 2 positive integers a and n

$$\mathbf{a^{\phi(n)+1} \equiv a\ (mod\ n)}$$

• **Theorem (Euler's Generalization)**

○ let gcd(a,n)=1 then

○ $a_{[[phi]](n)}$ mod n = 1

• Fermat's Theorem

○ let p be a prime and gcd(a,p)=1 then

○ a_{p-1} mod p = 1

• Algorithms to find **Inverses** a_{-1} mod n

1. search 1,...,n-1 until an a_{-1} is found with a.a_{-1} mod n

2. if [[phi]](n) is known, then from Euler's Generalization

a_{-1} = $a_{[[phi]](n)-1}$ mod n

3. otherwise use Extended Euclid's algorithm for inverse

Eg: Determine ϕ(37) and ϕ(35).

Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37. Thus ϕ(37) = 36.

- To determine ϕ(35), we list all of the positive integers less than 35 that are relatively prime to

it:
{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18
19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34}
There are 24 numbers on the list, so $\phi(35) = 24$.
$\phi(240)=2/240=p$

- Let p and q be distinct prime numbers, $n = pq$.
- Then
$\phi(n) = \phi(pq) = \phi(p) * \phi(q) = (p-1)(q-1)$
- Eg: $\phi(35)$
$35 = 5 * 7$
$\phi(35) = \phi(5) * \phi(7)$
$= (5-1) * (7-1)$
$= (4) * (6)$
$\phi(35) = 24$
$\phi(21) =$
$= \phi(3) * \phi(7)$
$= (3 - 1) * (7 - 1)$
$= 2 * 6 = 12$

Video Content / Details of website for further learning (if any):
http://www.brainkart.com/article/Fermat---s-And-Euler---s-Theorems_8430/

Important Books/Journals for further learning including the page nos.:
Book: William Stallings," Cryptography and Network Security Principles and Practices", Pearson Education, 2010.Pg no: (272-278)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L-14

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **I - Introduction** **Date of Lecture:**

Topic of Lecture: Legendre and Jacobi symbols

Introduction : (Maximum 5 sentences) :

- where a is a positive integer and p is prime. It is defined to be 0 if a is a multiple of p, 1 if a has a square root mod p, and -1 otherwise.
- The Jacobi symbol is a generalization of the Legendre symbol and uses the same notation.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- GCD
- Euler's theorem

Detailed content of the Lecture:

In a earlier post I introduce the Legendre symbol

$$\left(\frac{a}{p}\right)$$

where *a* is a positive integer and *p* is prime. It is defined to be 0 if *a* is a multiple of *p*, 1 if *a* has a square root mod *p*, and -1 otherwise.The Jacobi symbol is a generalization of the Legendre symbol and uses the same notation.

It relaxes the requirement that *p* be prime and only requires that *p* is odd.

If *m* has prime factors *pi* with exponents *ei*, then the Jacobi symbol is defined by

$$\left(\frac{n}{m}\right) = \prod \left(\frac{n}{p_i}\right)^{e_i}$$

Note that the symbol on the left is a Jacobi symbol while the symbols on the right are Legendre symbols.

The Legendre and Jacobi symbols are **not** fractions, but they act in some ways like fractions, and so the notation is suggestive. They come up in applications of number theory, so it's useful to be able to compute them.

A prime number

- A prime number is divisible only by 1 and itself
- For example: {2, 3, 5, 7, 11, 13, 17, …}
- 1 could also be considered prime, but it's not very useful.
- To factor a number *n* is to write it as a product of other numbers.
- $n = a * b * c$
- 143 = 11 * 13
- Or, 100 = 5 * 5 * 2 * 2 = $5^2 * 2^2$
- Prime factorization of a number *n* is writing
- it as a product of prime numbers.
- Eg: 91 = 7 * 13

Relatively Prime Numbers

- Two numbers are relatively prime if they have no common divisors other than 1.
- 10 and 21 are relatively prime, in respect to each other, as 10 has factors of 1, 2, 5, 10 and 21

has factors of 1, 3, 7, 21.

- The Greatest Common Divisor (GCD) of two relatively prime numbers can be determined by comparing their prime factorizations and selecting the least powers.

Modular Exponentiation

a^e mod n

a is an integer and e the exponent and mod n is divisor

$e = M_1 + M_2 + M_3 + \ldots M_n$

To find 11^{13} mod 53

Step1:

$13 = 8 + 4 + 1$ so $11^{13} = 11^{8+4+1} = 11^8 * 11^4 * 11^1$

- We can compute successive squares of 11 to obtain 11, 11^2, 11^4, 11^8 and then multiply together $11^1 * 11^4 * 11^8$ to get the answer 11^{13} .
- Because we are working mod 53, we will "take mods" at every stage of the calculation.

Thus we have:

11 mod 53 = 11

$11^2 = 121$,

121 mod 53 = 121 – 2*53 = 15 [a = qn + r (i.e) a – qn =r]

$11^4 = (11^2)^2 = 15^2$ mod 53

= 225 mod 53

= 225 – 4*53 = 13

$11^8 = (11^4)^2 = 13^2$ mod 53

= 169 mod 53

= 169 – 3*53 = 10

Therefore 11^{13} mod 53

= $11^8 * 11^4 * 11^1$ mod 53

= 10 * 13 * 11 mod 53

= 1430 mod 53

= 1430 – 26*53 = 52

The answer is 11^{13} mod 53 = 52

Video Content / Details of website for further learning (if any):
https://www.sciencedirect.com/science/article/pii/S0022314X13002357

Important Books/Journals for further learning including the page nos.:
Website Content

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L-15

LECTURE HANDOUTS

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **I - Introduction** **Date of Lecture:**

Topic of Lecture: Continued fractions

Introduction : (Maximum 5 sentences) :

- A continued fraction is just another way of writing fractions. It is a way to compute the square root of a number extremely accurately.

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- GCD
- Euler's theorem

Detailed content of the Lecture:

A continued fraction is just another way of writing fractions. It is a way to compute the square root of a number extremely accurately.

The form of continued fractions is shown below:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots}}}$$

This form is called a continued fraction. The value of an must be an integer. A continued fraction can also be rational or irrational, it depends on the number. Continued fraction representation of numbers such as π or e are infinitely long. Given a number, α, a continued fraction can be created by using the recursive algorithm:

$$a_i = [\alpha_i]$$

$$\alpha_{i+1} = \frac{1}{\alpha_i - a_i}$$

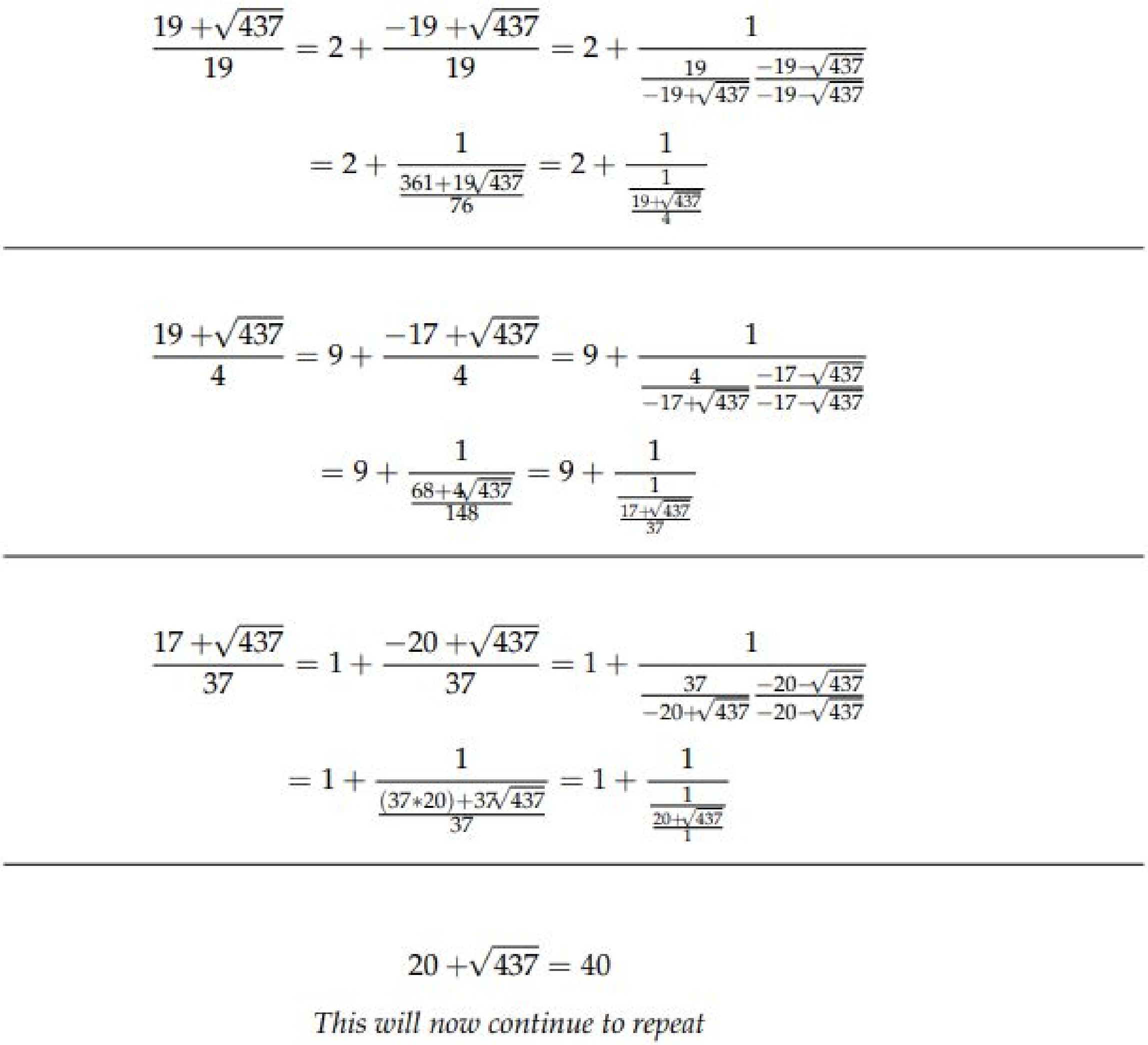
To understand continued fractions better, we shall look at an example:

Let $\alpha = 437$

$$\sqrt{437} = 20 + (\sqrt{437} - 20)$$

$$= 20 + \frac{1}{\frac{1}{\sqrt{437}-20}\frac{\sqrt{437}+20}{\sqrt{437}+20}}$$

$$= 20 + \frac{1}{\frac{20+\sqrt{437}}{37}}$$



$$\frac{19+\sqrt{437}}{19} = 2 + \frac{-19+\sqrt{437}}{19} = 2 + \frac{1}{\frac{19}{-19+\sqrt{437}}\frac{-19-\sqrt{437}}{-19-\sqrt{437}}}$$

$$= 2 + \frac{1}{\frac{361+19\sqrt{437}}{76}} = 2 + \frac{1}{\frac{1}{\frac{19+\sqrt{437}}{4}}}$$

$$\frac{19+\sqrt{437}}{4} = 9 + \frac{-17+\sqrt{437}}{4} = 9 + \frac{1}{\frac{4}{-17+\sqrt{437}}\frac{-17-\sqrt{437}}{-17-\sqrt{437}}}$$

$$= 9 + \frac{1}{\frac{68+4\sqrt{437}}{148}} = 9 + \frac{1}{\frac{1}{\frac{17+\sqrt{437}}{37}}}$$

$$\frac{17+\sqrt{437}}{37} = 1 + \frac{-20+\sqrt{437}}{37} = 1 + \frac{1}{\frac{37}{-20+\sqrt{437}}\frac{-20-\sqrt{437}}{-20-\sqrt{437}}}$$

$$= 1 + \frac{1}{\frac{(37*20)+37\sqrt{437}}{37}} = 1 + \frac{1}{\frac{1}{\frac{20+\sqrt{437}}{1}}}$$

$$20+\sqrt{437} = 40$$

This will now continue to repeat

We know to stop there because for square roots every continued fraction repeats eventually. So in this example it went: 20, 1, 9, 2, 9, 1, 40 When we finally see the repetition, the final number in the sequence will be double the first number (i.e. 20 ∗ 2 = 40).

In Cryptography, continued fractions can actually be used to factor. Continued fractions can also be used for √ n and it will continue to use the form we saw above.

Video Content / Details of website for further learning (if any):
https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1294&context=honors_proj

Important Books/Journals for further learning including the page nos.:
Website Content

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

L

LECTURE HANDOUTS

CSE

III/V

L-16

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **II - Symmetric Ciphers & Public Key Cryptography**

Date of Lecture:

Topic of Lecture: Classical Encryption Techniques

Introduction : (Maximum 5 sentences)

- The many schemes used for encryption constitute the area of study known as cryptography**.** Such a scheme is known as **a** cryptographic system (cryptosystem) or a cipher.
- Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis.
- Cryptanalysis is what the layperson calls "breaking the code". The areas of cryptography and cryptanalysis together are called cryptology**.**

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Plaintext
- Ciphertext
- Enciphering **or** encryption
- Deciphering **or** decryption

Detailed content of the Lecture:

Definitions of Terms

- Plaintext**:** original message
- Ciphertext: coded message
- Enciphering **or** encryption**:** the process of converting from plaintext to ciphertext
- Deciphering **or** decryption**:** the process of restoring the plaintext from the ciphertext

The many schemes used for encryption constitute the area of study known as cryptography. Such a scheme is known as a cryptographic system (cryptosystem) or a cipher.

Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis. Cryptanalysis is what the layperson calls "breaking the code".

The areas of cryptography and cryptanalysis together are called cryptology.

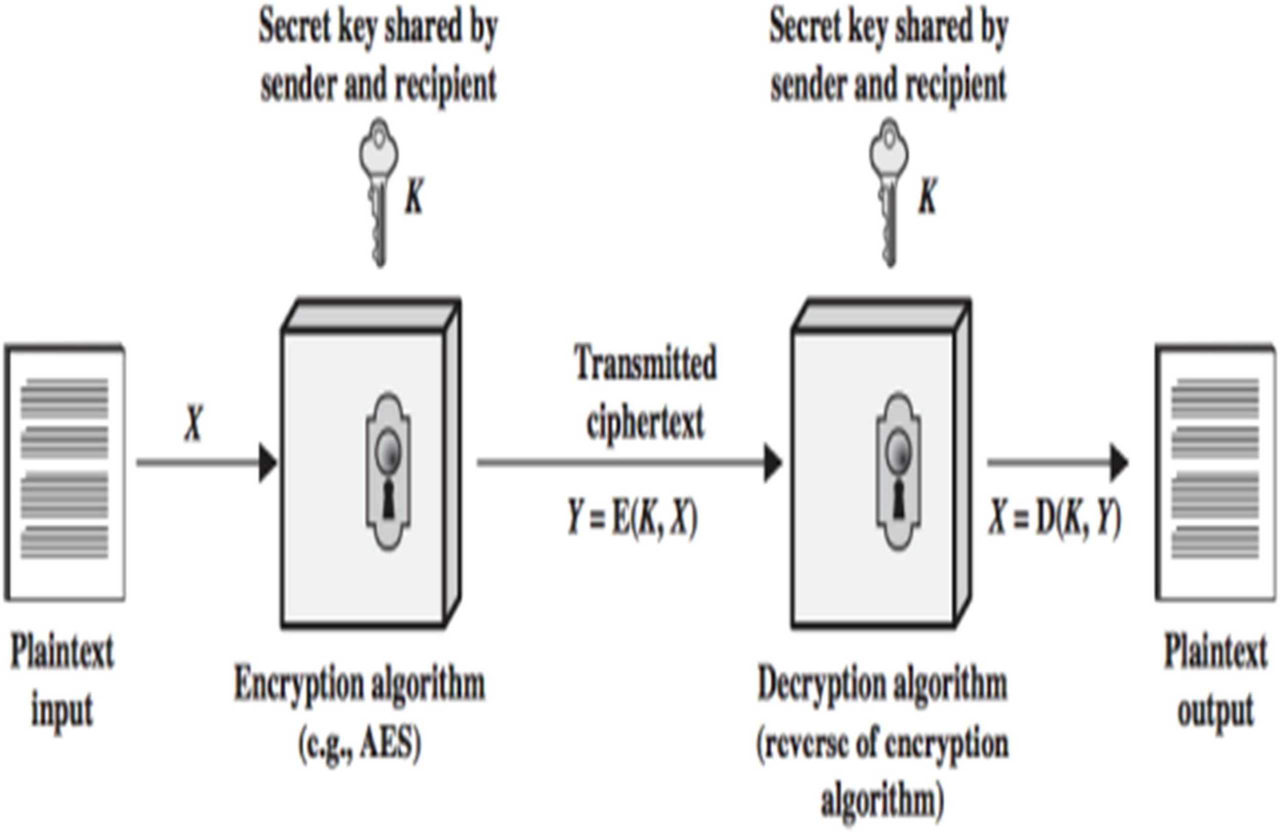
Symmetric Cipher Model

A symmetric encryption scheme has five ingredients (as shown in the following figure):

- **Plaintext**: This is the original intelligible message or data that is fed into the algorithm as input.
- **Encryption algorithm**: The encryption algorithm performs various substitutions and transformations on

the plaintext.

- **Secret key**: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.
- **Ciphertext**: This is the scrambled (unintelligible) message produced as output.
  - It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.
- **Decryption algorithm**: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

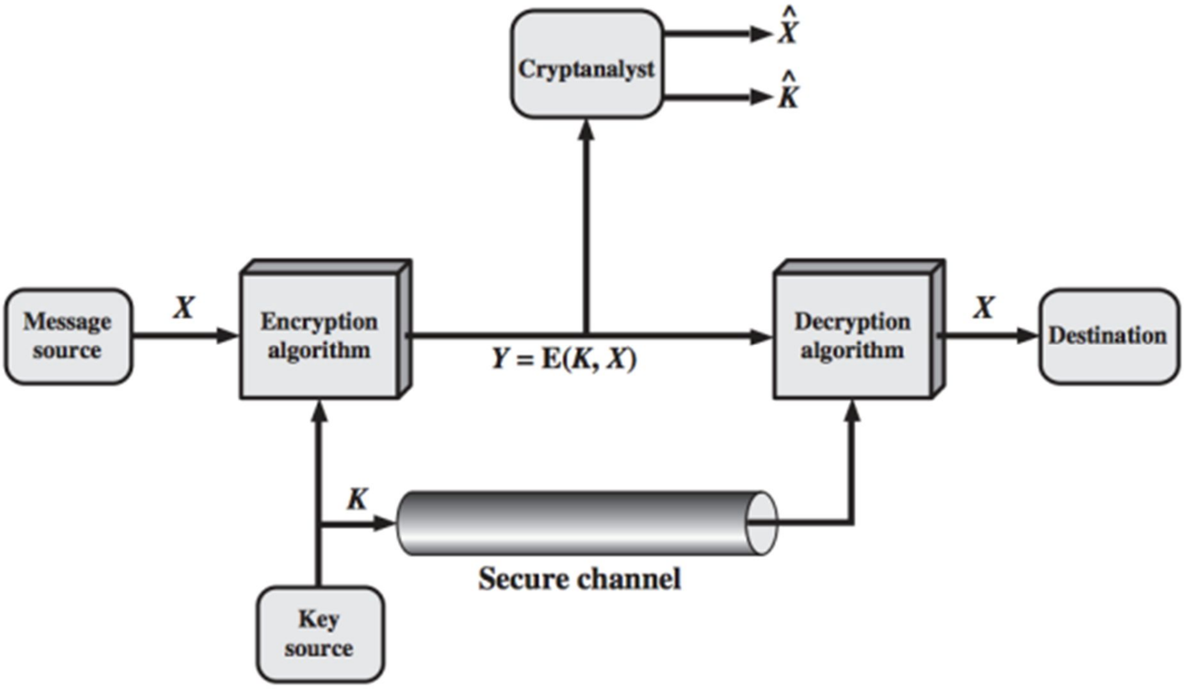
Encryption Requirements *

There are two requirements for secure use of conventional encryption:

1. The encryption algorithm must be strong.

   - At a minimum, an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key.
   - In a stronger form, the opponent should be unable to decrypt ciphertexts or discover the key even if he or she has a number of ciphertexts together with the plaintext for each ciphertext.

2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.



- A source produces a message in plaintext, X=[X1,X2,...,XM]X=[X1,X2,...,XM].
- A key of the form K=[K1,K2,...,KJ]K=[K1,K2,...,KJ] is generated.
  - If the key is generated at the message source, then it must also be provided to the destination by means of some secure channel.
  - Alternatively, a third party could generate the key and securely deliver it to both source and destination.
- The cipher text Y=[Y1,Y2,...,YN]Y=[Y1,Y2,...,YN] is produced by the encryption algorithm with the message X and the encryption key K as input.

The encryption process is:

Y=E(K,X)Y=E(K,X)

This notation indicates that Y is produced by using encryption algorithm E as a function of the plaintext X, with the specific function determined by the value of the key K.

The intended receiver with the key is able to invert the transformation:

X=D(K,Y)X=D(K,Y)

An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both. It is assumed that the opponent knows the encryption (E) and decryption (D) algorithms. The opponent may do one of the following:

- Recover X by generating a plaintext estimate X^X^, if the opponent is interested in only this particular message.
- Recover K by generating an estimate K^K^, if the opponent is interested in being able to read future messages.

Cryptography

Cryptographic systems are characterized along three independent dimensions:

1. **Type of operations for transforming plaintext to ciphertext**. All encryption algorithms are based on two general principles:
   - **Substitution**: each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element,
   - **Transposition**: elements in the plaintext are rearranged.

The fundamental requirement is that no information be lost (all operations are reversible). Product systems involve multiple stages of substitutions and transpositions.

2. **Number of keys used**.

   - If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption.
   - If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.

3. **How the plaintext is processed**.

   - A block cipher processes the input one block of elements at a time, producing an output block for each input block.
   - A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

Cryptanalysis and Brute-Force Attack

The objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext. There are two general approaches to attacking a conventional encryption scheme:

- **Cryptanalysis** (cryptanalytic attacks): This attack relies on the nature of the algorithm plus some knowledge of the general characteristics of the plaintext or some sample plaintext–ciphertext pairs. It exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
- **Brute-force attack**: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

If either type of attack succeeds in deducing the key, then future and past messages encrypted with that key are compromised.

Cryptanalytic attacks *

The following table summarizes the various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst.

Type of Attack	**Known to Cryptanalyst**
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen	• Encryption algorithm

Ciphertext	• Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	Combination of "Chosen Plaintext" and "Chosen Ciphertext"

In general, we can assume that the opponent does know the algorithm used for encryption. If the key space is very large, the brute-force approach of trying all possible keys, which is one possible attack, becomes impractical. Thus, the opponent must anaylyze the ciphertext itself, applying various statistical tests to it. To use this approach, the opponent must have some general idea of the type of plaintext that is concealed.

Ciphertext-only attack *

The ciphertext-only attack is the easiest to defend against because the opponent has the least amount of information to work with.

Known-plaintext attack *

In many cases, the analyst has more information than ciphertext only:

- The analyst may be able to capture one or more plaintext messages and their encryptions.
- The analyst may know that certain plaintext patterns will appear in a message.

A **brute-force attack** involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.

Video Content / Details of website for further learning (if any):
https://notes.shichao.io/cnspp/ch2/

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (164-175)

Course Teacher

Verified by HOD

L

LECTURE HANDOUTS

CSE

III/V

L-17

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **II - Symmetric Ciphers & Public Key Cryptography**

Date of Lecture:

Topic of Lecture: Block Ciphers: Modes of operation- ECB & CCB

Introduction : (Maximum 5 sentences)

- Encryption algorithms are divided into two categories based on input type, as block cipher and stream cipher.
- **Block cipher** is an encryption algorithm which takes fixed size of input say b bits and produces a ciphertext of b bits again. If input is larger than b bits it can be divided further.
- For different applications and uses, there are several modes of operations for a block cipher.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- ✓ Electronic Code Book (ECB) Mode. Electronic Code Block (ECB) is the simplest block cipher mode of operation.
- ✓ Cipher Chaining Block(CCB) Mode.
- ✓ Output Feedback (OFB) Mode.
- ✓ Counter (CTR) Mode.
- ✓ Galois Counter Mode

Detailed content of the Lecture:

Block Cipher modes of Operation

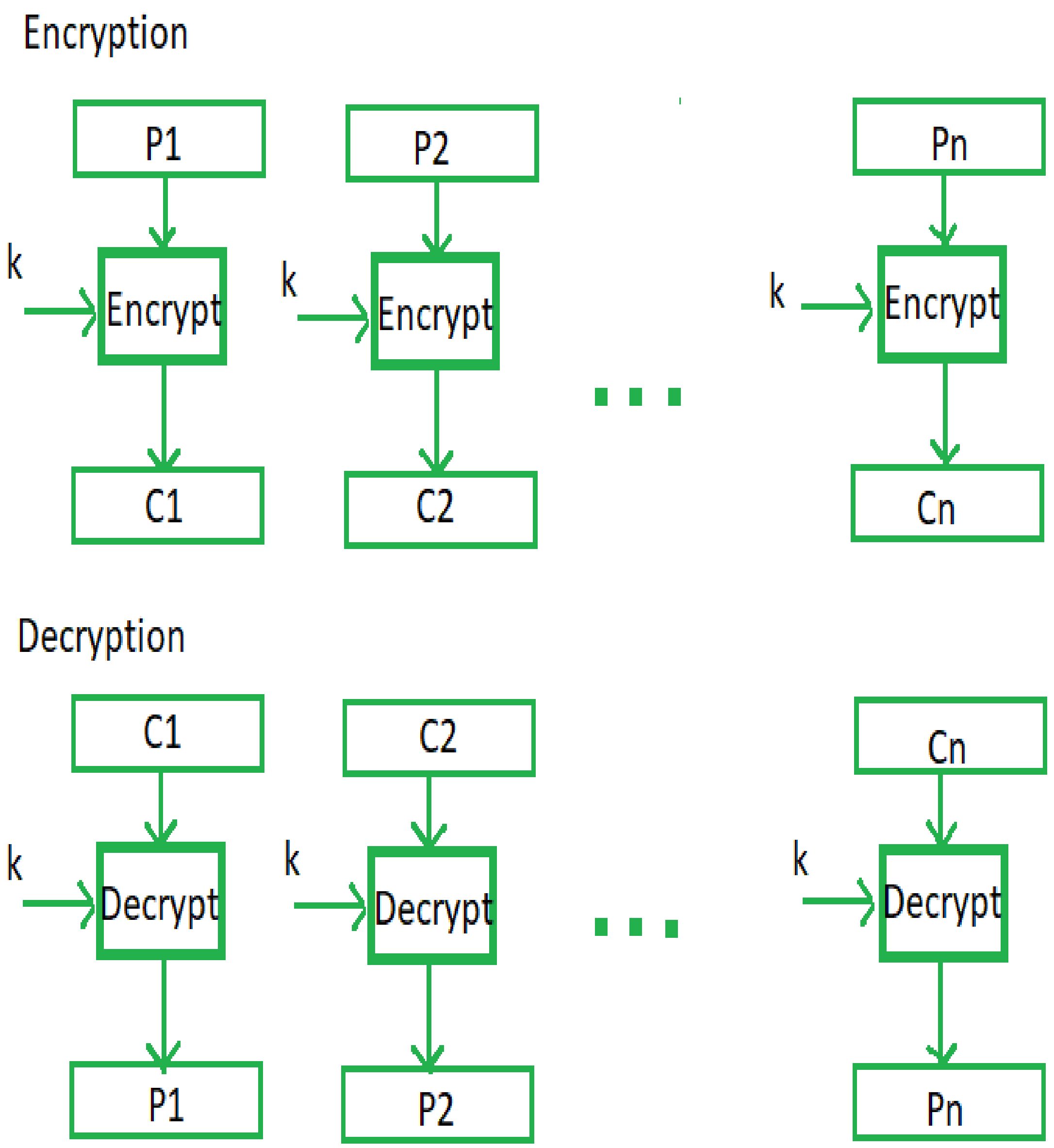
Encryption algorithms are divided into two categories based on input type, as block cipher and stream cipher.

Block cipher is an encryption algorithm which takes fixed size of input say b bits and produces a ciphertext of b bits again.
If input is larger than b bits it can be divided further. For different applications and uses, there are several modes of operations for a block cipher.

Electronic Code Book (ECB)

Electronic code book is the easiest block cipher mode of functioning.
It is easier because of direct encryption of each block of input plaintext and output is in form of blocks of encrypted ciphertext.
Generally, if a message is larger than b bits in size, it can be broken down into bunch of blocks and the procedure is repeated.

Procedure of ECB is illustrated below:



Advantages of using ECB

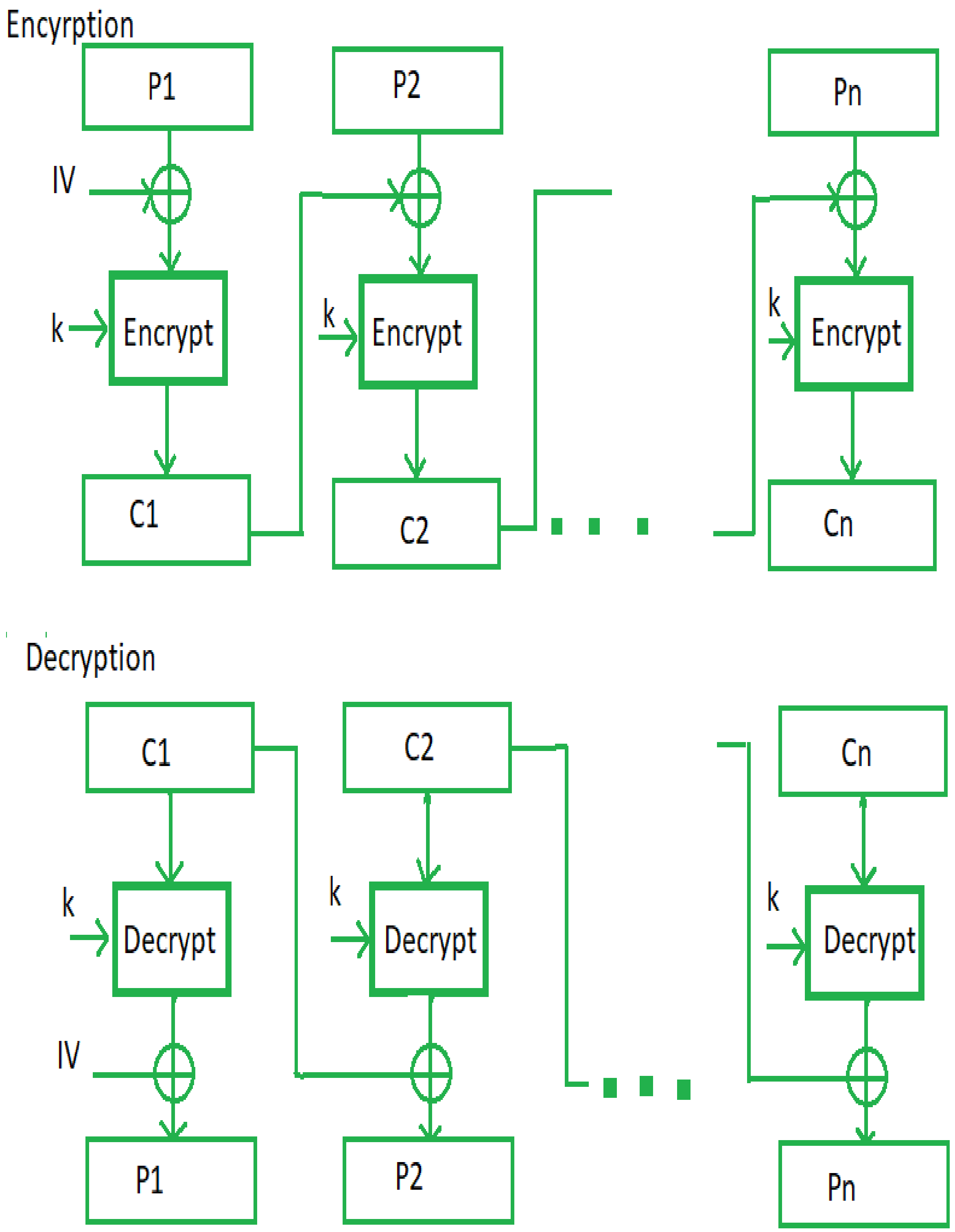
- Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption.
- Simple way of block cipher.

Disadvantages of using ECB

- Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext.

Cipher Chaining Block

- Cipher block chaining or CBC is an advancement made on ECB since ECB compromises some security requirements. In CBC, previous cipher block is given as input to next encryption algorithm after XOR with original plaintext block.
- In a nutshell here, a cipher block is produced by encrypting a XOR output of previous cipher block and present plaintext block.
- The process is illustrated here:



Advantages of CCB :

- CBC works well for input greater than b bits.
- CBC is a good authentication mechanism.
- Better resistive nature towards cryptanalsis than ECB.

Disadvantages of CCB ;

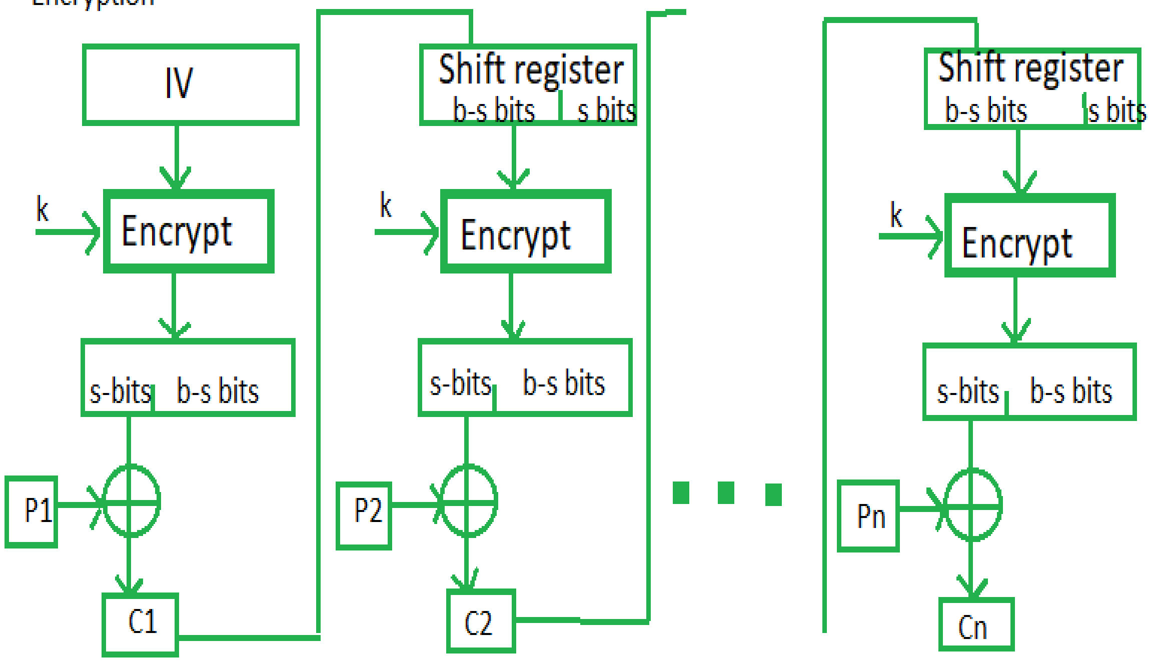
- Parallel encryption is not possible since every encryption requires previous cipher.

Cipher Feedback Mode (CFB) :

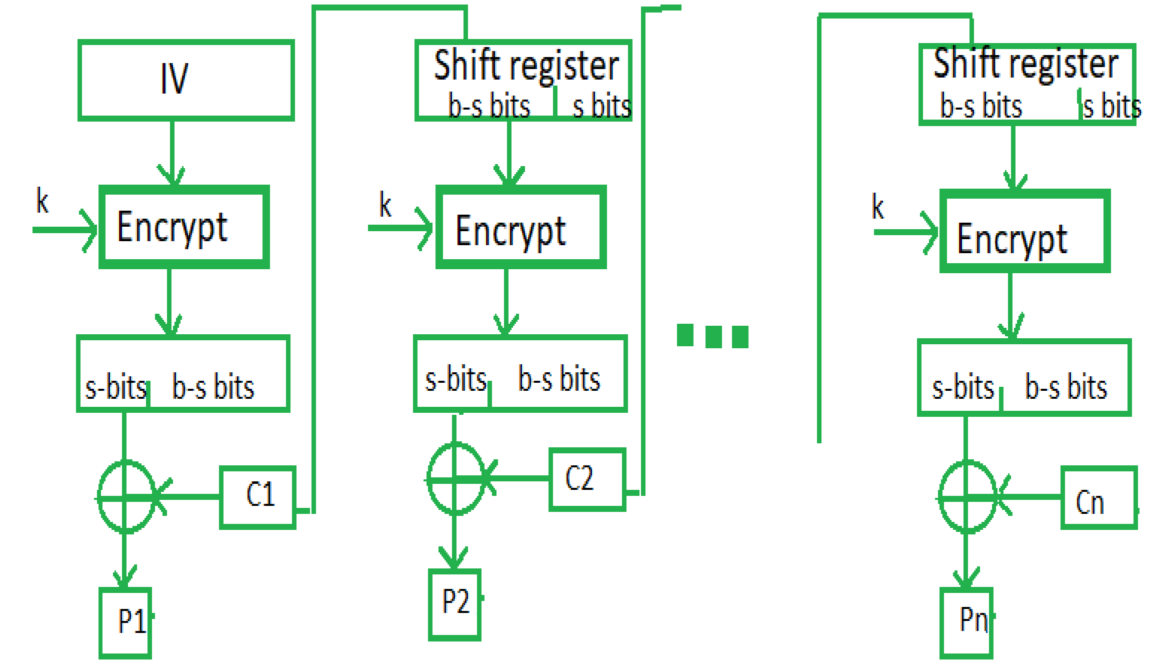
- In this mode the cipher is given as feedback to the next block of encryption with some new specifications: first an initial vector IV is used for first encryption and output bits are divided as set of sandb-s bits the left hand side sbits are selected and are applied an XOR operation with plaintext bits.

- The result given as input to a shift register and the process continues. The encryption and decryption process for the same is shown below, both of them use encryption algorithm.

Encryption



Decryption

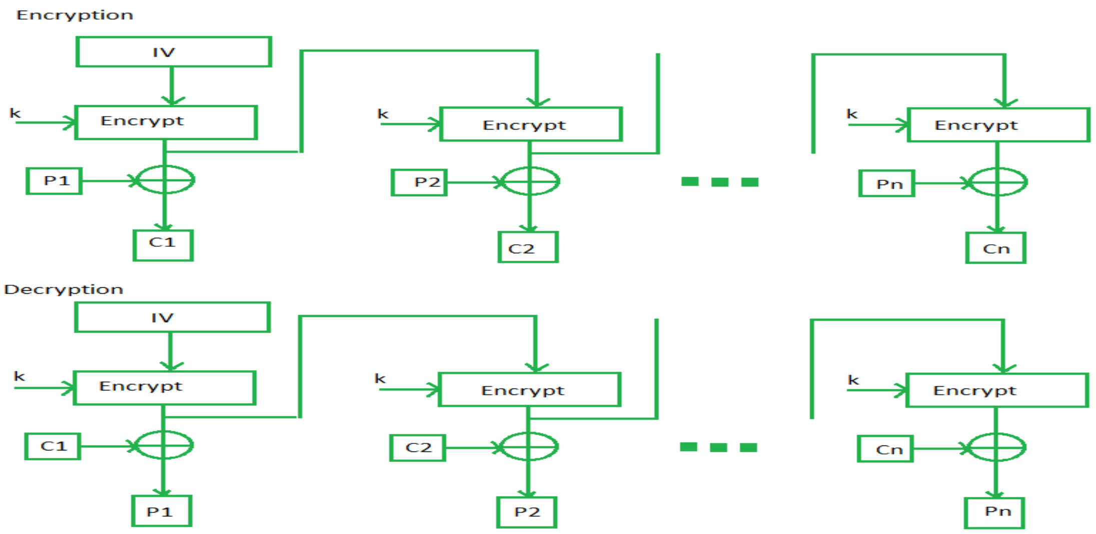


Advantages of CFB

- Since, there is some data loss due to use of shift register, thus it is difficult for applying cryptanalysis.

Output Feedback Mode

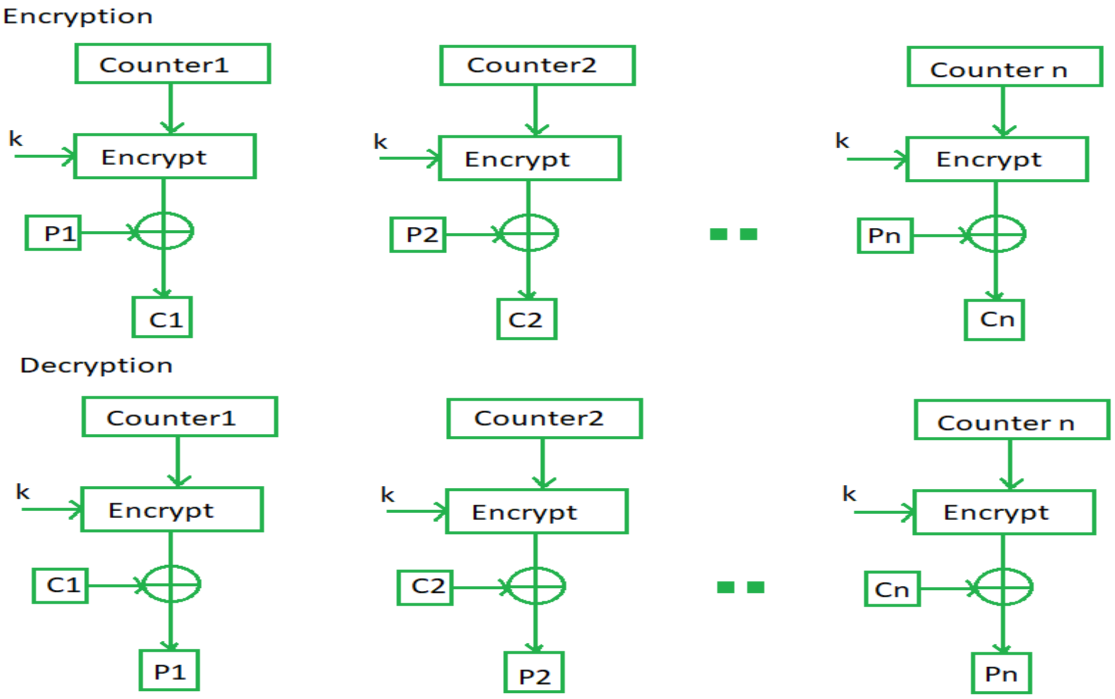
- The output feedback mode follows nearly same process as the Cipher Feedback mode except that it sends the encrypted output as feedback instead of the actual cipher which is XOR output. In this output feedback mode, all bits of the block are send instead of sending selected s bits.
- The Output Feedback mode of block cipher holds great resistance towards bit transmission errors. It also decreases dependency or relationship of cipher on plaintext.



Counter Mode

- The Counter Mode or CTR is a simple counter based block cipher implementation.
- Every time a counter initiated value is encrypted and given as input to XOR with plaintext which results in ciphertext block.
- The CTR mode is independent of feedback use and thus can be implemented in parallel.

Its simple implementation is shown below:



Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/block-cipher-modes-of-operation/

Important Books/Journals for further learning including the page nos.:

Book: William Stallings," Cryptography and Network Security Principles and Practices", Pearson Education, 2010
Page No: (92-101)

Course Teacher

Verified by HOD

Estd. 2000

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L

L-18

LECTURE HANDOUTS

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **II - Symmetric Ciphers & Public Key Cryptography**

Date of Lecture:

Topic of Lecture: Block cipher modes of operation (CFM, OFM, Counter)

Introduction : (Maximum 5 sentences)

- Encryption algorithms are divided into two categories based on input type, as block cipher and stream cipher.
- **Block cipher** is an encryption algorithm which takes fixed size of input say b bits and produces a ciphertext of b bits again. If input is larger than b bits it can be divided further.
- For different applications and uses, there are several modes of operations for a block cipher.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- ✓ Electronic Code Book (ECB) Mode. Electronic Code Block (ECB) is the simplest block cipher mode of operation.
- ✓ Cipher Chaining Block(CCB) Mode.
- ✓ Output Feedback (OFB) Mode.
- ✓ Counter (CTR) Mode.
- ✓ Galois Counter Mode

Detailed content of the Lecture:

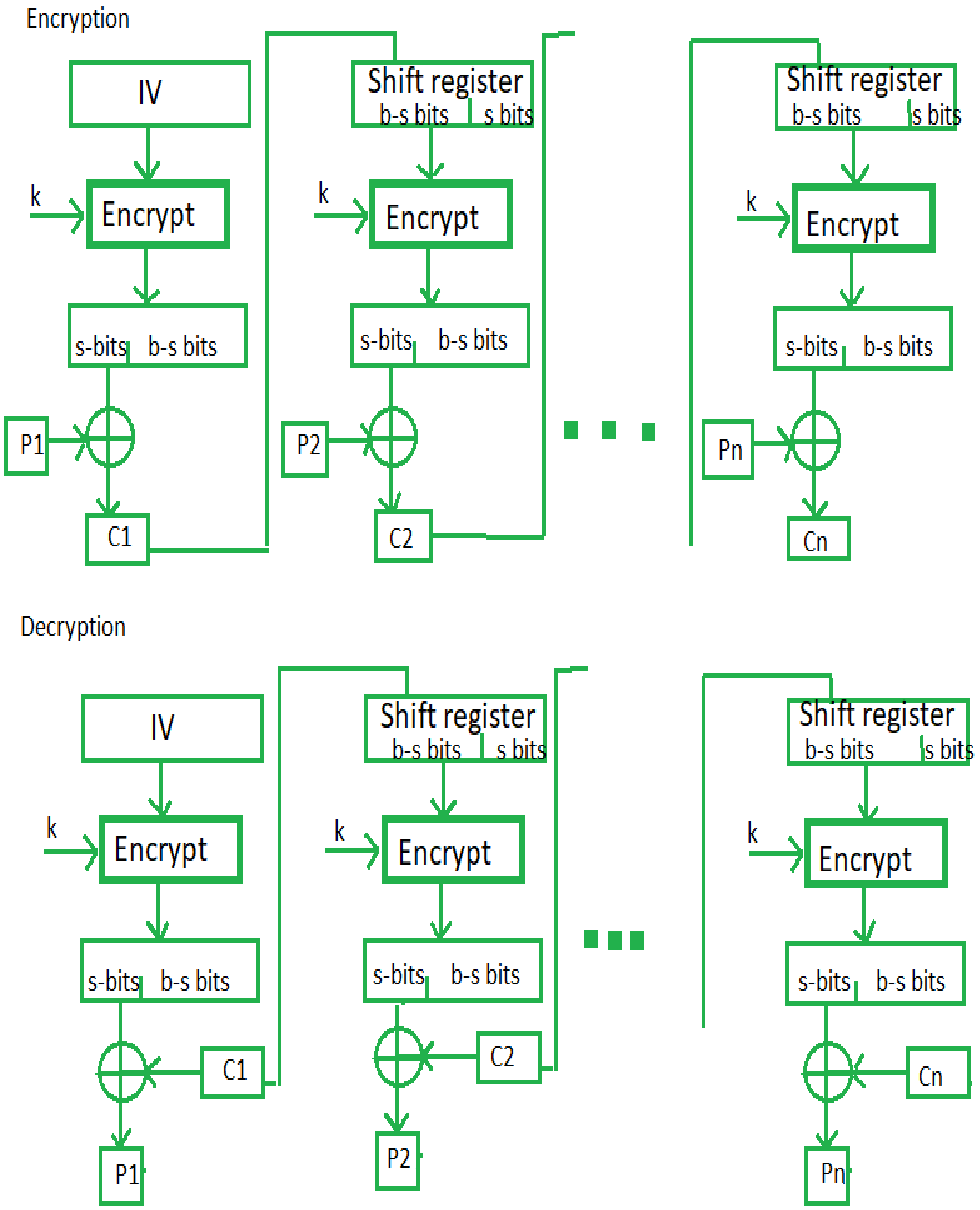
Cipher Feedback Mode (CFB) :

- In this mode the cipher is given as feedback to the next block of encryption with some new specifications:

  first an initial vector IV is used for first encryption and output bits are divided as set of sandb-s bits the left hand side sbits are selected and are applied an XOR operation with plaintext bits.

- The result given as input to a shift register and the process continues.

- The encryption and decryption process for the same is shown below, both of them use encryption algorithm.

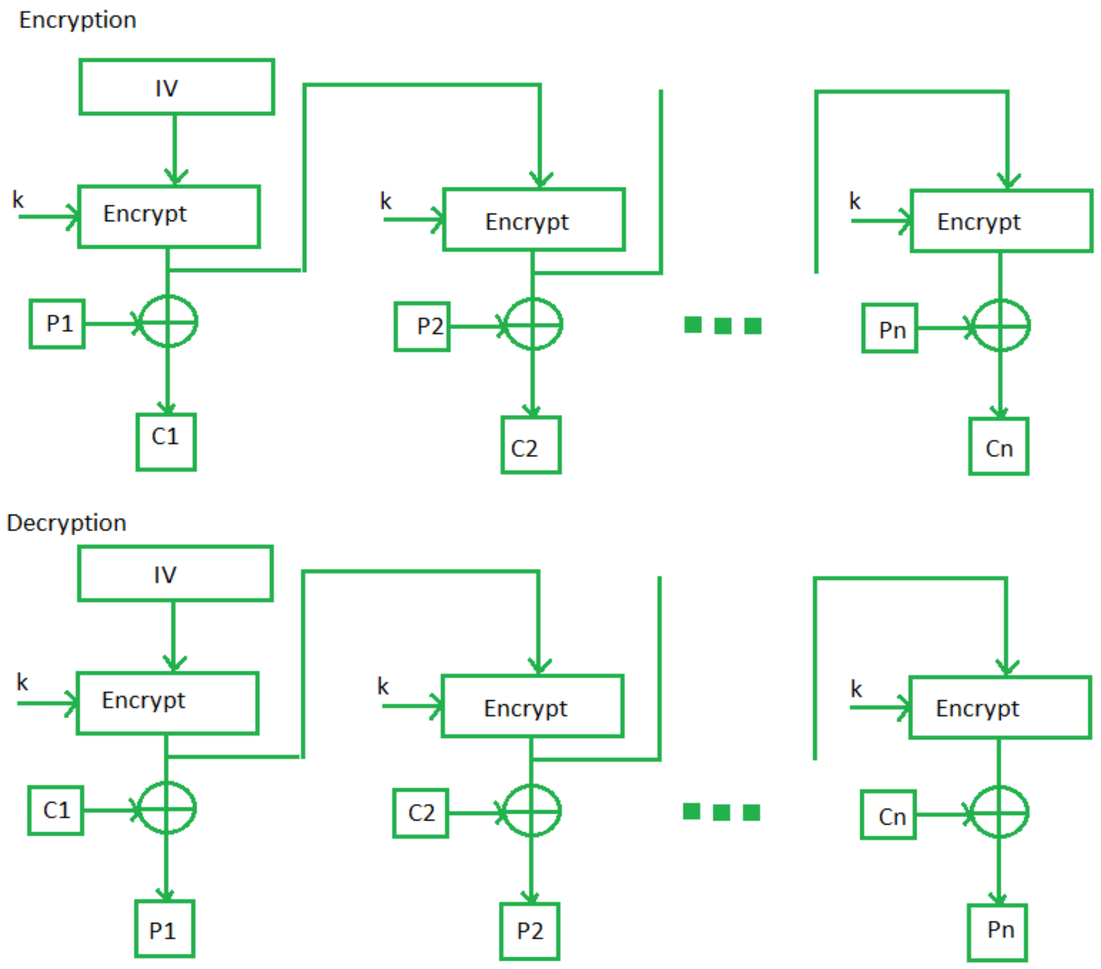


Advantages of CFB

- Since, there is some data loss due to use of shift register, thus it is difficult for applying cryptanalysis.

Output Feedback Mode

- The output feedback mode follows nearly same process as the Cipher Feedback mode except that it sends the encrypted output as feedback instead of the actual cipher which is XOR output. In this output feedback mode, all bits of the block are send instead of sending selected s bits.
- The Output Feedback mode of block cipher holds great resistance towards bit transmission errors. It also decreases dependency or relationship of cipher on plaintext.



Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/block-cipher-modes-of-operation/

Important Books/Journals for further learning including the page nos.:

Book: William Stallings," Cryptography and Network Security Principles and Practices", Pearson Education, 2010
Page No: (92-101)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L

L-19

LECTURE HANDOUTS

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **II - Symmetric Ciphers & Public Key Cryptography**

Date of Lecture:

Topic of Lecture: Block cipher Principles

Introduction : (Maximum 5 sentences)

- Encryption algorithms are divided into two categories based on input type, as block cipher and stream cipher.
- **Block cipher** is an encryption algorithm which takes fixed size of input say b bits and produces a ciphertext of b bits again. If input is larger than b bits it can be divided further.
- For different applications and uses, there are several modes of operations for a block cipher.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- ✓ Electronic Code Book (ECB) Mode. Electronic Code Block (ECB) is the simplest block cipher mode of operation.
- ✓ Cipher Chaining Block(CCB) Mode.
- ✓ Output Feedback (OFB) Mode.
- ✓ Counter (CTR) Mode.
- ✓ Galois Counter Mode

Detailed content of the Lecture:

Block Cipher Principles:

- Block ciphers are built in the Feistel cipher structure. Block cipher has a specific number of rounds and keys for generating ciphertext.
- For defining the complexity level of an algorithm few design principles are to be considered.

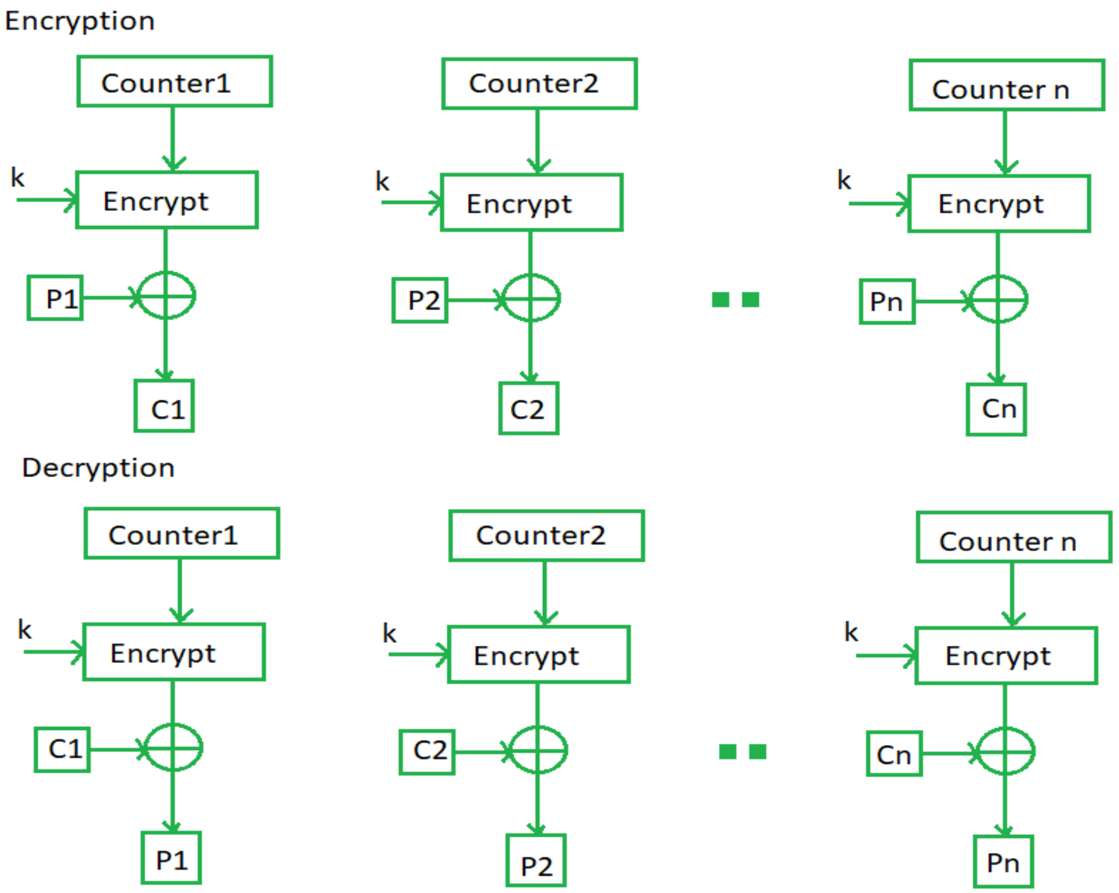
These are explained as following below :

- Numbers of Rounds
- Design of Function F
- Key Schedules Algorithms

Counter Mode

- ➢ The Counter Mode or CTR is a simple counter based block cipher implementation.
- ➢ Every time a counter initiated value is encrypted and given as input to XOR with plaintext which results in cipher text block.
- ➢ The CTR mode is independent of feedback use and thus can be implemented in parallel.

Its simple implementation is shown below:



Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/block-cipher-design-principles/

Important Books/Journals for further learning including the page nos.:

Book: William Stallings," Cryptography and Network Security Principles and Practices", Pearson Education, 2010
Page No: (92-101)

Course Teacher

Verified by HOD

L-20

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **II - Symmetric Ciphers & Public Key Cryptography**

Date of Lecture:

Topic of Lecture: Data Encryption Standard-DES Example

Introduction : (Maximum 5 sentences)

- ✓ Data encryption standard (DES) has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on decline.
- ✓ DES is a block cipher, and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text.
- ✓ The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Electronic Code Book (ECB) Mode. Electronic Code Book (ECB) is the simplest block cipher mode of operation.
- ✓ Cipher Block Chaining (CBC) Mode.
- ✓ Output Feedback (OFB) Mode.
- ✓ Counter (CTR) Mode.
- ✓ Galois Counter Mode

Detailed content of the Lecture:

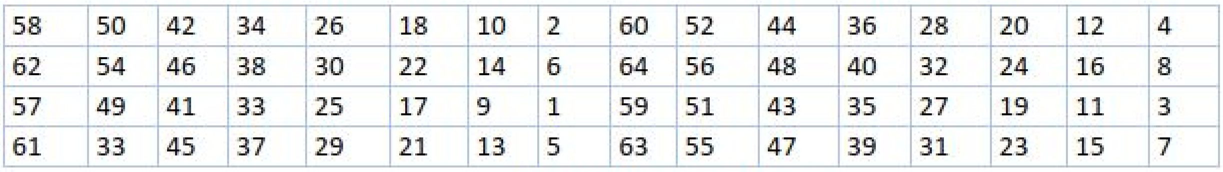
Data encryption standard (DES)

- Data encryption standard (DES) has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on decline.
- DES is a block cipher, and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text.
- The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.
- Actually, the initial key consists of 64 bits.
- However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56 bit key. That is bit position 8, 16, 24, 32, 40, 48, 56 and 64 are discarded.

Initial Permutation (IP)

- As we have noted, the Initial permutation (IP) happens only once and it happens before the first round.
- It suggests how the transposition in IP should proceed, as show in figure.
- For example, it says that the IP replaces the first bit of the original plain text block with the 58th bit of the original plain text, the second bit with the 50th bit of the original plain text block and so on.

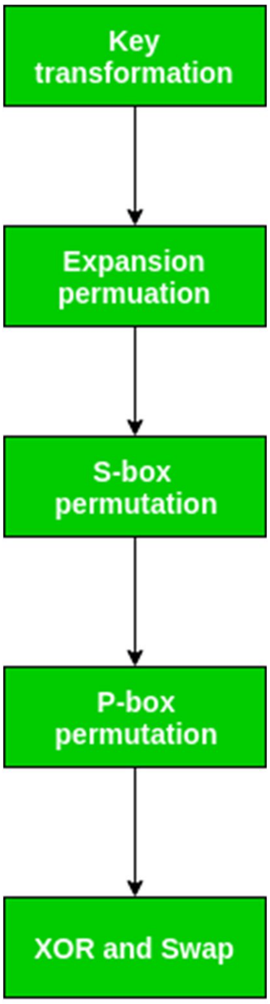
This is nothing but jugglery of bit positions of the original plain text block. the same rule applies for all the other bit positions which shows in the figure.



58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	33	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Figure - Initial permutation table

As we have noted after IP done, the resulting 64-bit permuted text block is divided into two half blocks. Each half block consists of 32 bits, and each of the 16 rounds, in turn, consists of the broad level steps outlined in figure.

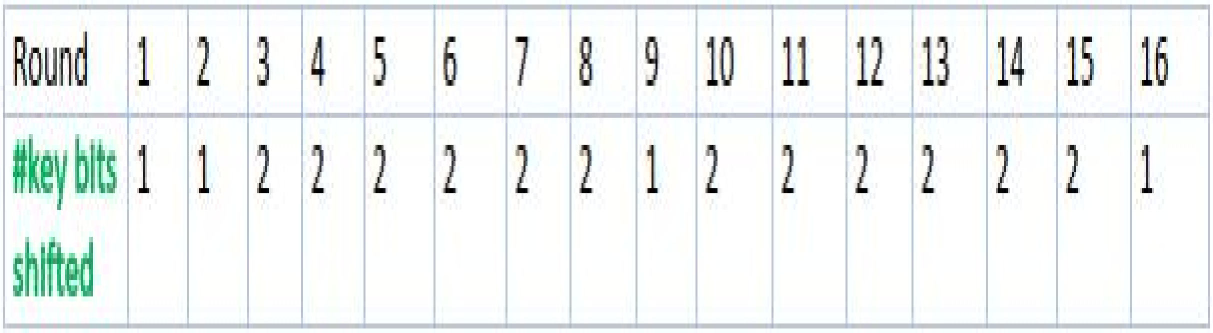


Step-1: Key transformation

We have noted initial 64-bit key is transformed into a 56-bit key by discarding every 8th bit of the initial key. Thus, for each a 56-bit key is available.

- From this 56-bit key, a different 48-bit Sub Key is generated during each round using a process called as key transformation. For this the 56 bit key is divided into two halves, each of 28 bits. These halves are circularly shifted left by one or two positions, depending on the round.
- For example, if the round number 1, 2, 9 or 16 the shift is done by only position for other rounds, the circular shift is done by two positions.

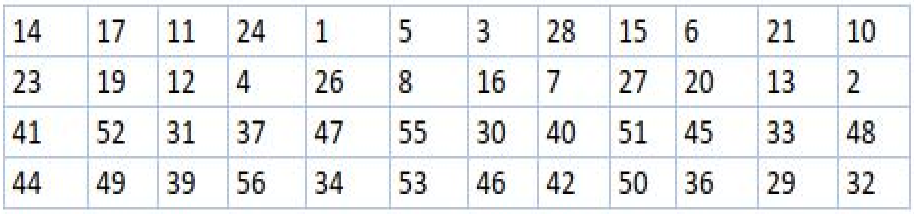
The number of key bits shifted per round is show in figure.



Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
#key bits shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Figure - number of key bits shifted per round

- ✓ After an appropriate shift, 48 of the 56 bit are selected. for selecting 48 of the 56 bits the table show in figure given below.
- ✓ For instance, after the shift, bit number 14 moves on the first position, bit number 17 moves on the second position and so on.
- ✓ If we observe the table carefully, we will realize that it contains only 48 bit positions. Bit number 18 is discarded (we will not find it in the table), like 7 others, to reduce a 56-bit key to a 48-bit key.
- ✓ Since the key transformation process involves permutation as well as selection of a 48-bit sub set of the original 56-bit key it is called Compression Permutation.



14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Figure - compression permutation

Because of this compression permutation technique, a different subset of key bits is used in each round. That's make DES not easy to crack.

Step-2: Expansion Permutation

- ✓ Recall that after initial permutation, we had two 32-bit plain text areas called as Left Plain Text(LPT) and Right Plain Text(RPT).
- ✓ During the expansion permutation, the RPT is expanded from 32 bits to 48 bits.
- ✓ Bits are permuted as well hence called as expansion permutation.
- ✓ This happens as the 32 bit RPT is divided into 8 blocks, with each block consisting of 4 bits.
- ✓ Then, each 4 bit block of the previous step is then expanded to a corresponding 6 bit block, i.e., per 4 bit block, 2 more bits are added.

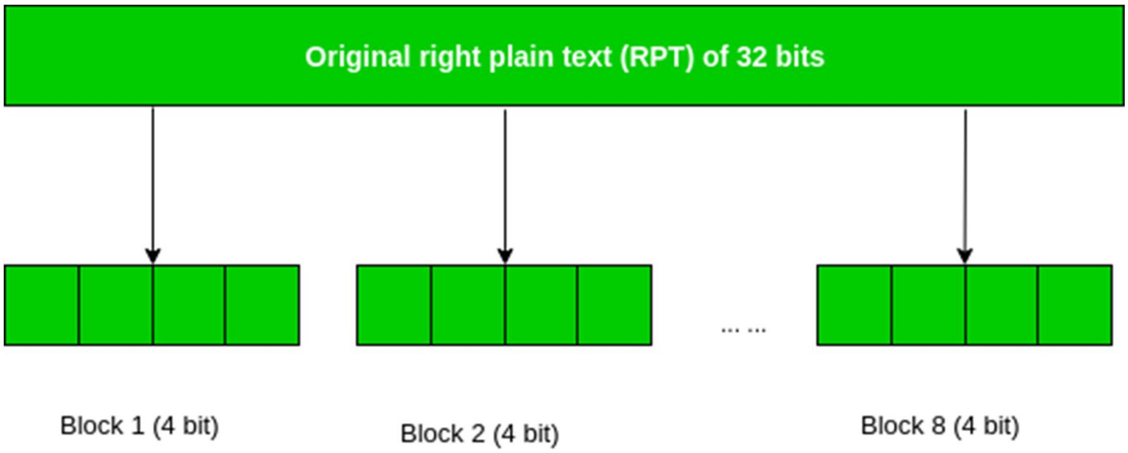


Figure - division of 32 bit RPT into 8 bit blocks

- ✓ This process results into expansion as well as permutation of the input bit while creating output. Key transformation process compresses the 56-bit key to 48 bits.
- ✓ Then the expansion permutation process expands the 32-bit RPT to 48-bits. Now the 48-bit key is XOR with 48-bit RPT and resulting output is given to the next step, which is the S-Box substitution.

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (52-56)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

L-21

LECTURE HANDOUTS

CSE **III/V**

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **II - Symmetric Ciphers & Public Key Cryptography**

Date of Lecture:

Topic of Lecture: Data Encryption Standard-Decryption

Introduction : (Maximum 5 sentences)

- ✓ Data encryption standard (DES) has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on decline.
- ✓ DES is a block cipher, and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text.
- ✓ The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Electronic Code Book (ECB) Mode. Electronic Code Book (ECB) is the simplest block cipher mode of operation.
- ✓ Cipher Block Chaining (CBC) Mode.
- ✓ Output Feedback (OFB) Mode.
- ✓ Counter (CTR) Mode.
- ✓ Galois Counter Mode

Detailed content of the Lecture:

Data encryption standard (DES)

- Data encryption standard (DES) has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on decline.
- DES is a block cipher, and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text.
- The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.

The encryption-decryption process is as follows −

- Encrypt the plaintext blocks using single DES with key K_1.
- Now decrypt the output of step 1 using single DES with key K_2.
- Finally, encrypt the output of step 2 using single DES with key K_3.
- The output of step 3 is the ciphertext.
- Decryption of a ciphertext is a reverse process. User first decrypt using K_3, then encrypt with K_2, and

finally decrypt with K_1.

DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

- **Avalanche effect** − A small change in plaintext results in the very great change in the ciphertext.
- **Completeness** − Each bit of ciphertext depends on many bits of plaintext.

During the last few years, cryptanalysis have found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.

DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.

- The speed of exhaustive key searches against DES after 1990 began to cause discomfort amongst users of DES.
- However, users did not want to replace DES as it takes an enormous amount of time and money to change encryption algorithms that are widely adopted and embedded in large security architectures.
- The pragmatic approach was not to abandon the DES completely, but to change the manner in which DES is used. This led to the modified schemes of Triple DES (sometimes known as 3DES).
- Incidentally, there are two variants of Triple DES known as 3-key Triple DES (3TDES) and 2-key Triple DES (2TDES).

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014 Page No: (52-56)

Course Teacher

Verified by HOD

L13

LECTURE HANDOUTS

L-22

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **II - Symmetric Ciphers & Public Key Cryptography**

Date of Lecture:

Topic of Lecture: Strength of DES - Triple DES- the Origins

Introduction : (Maximum 5 sentences)

Data **Encryption** Standard (**DES**) is a block cipher algorithm that takes plain text in blocks of 64 bits and converts them to ciphertext using keys of 48 bits.

It is a symmetric key algorithm, which means that the same key is used for encrypting and decrypting data.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Plaintext
- Cipher text
- Encryption
- Decryption

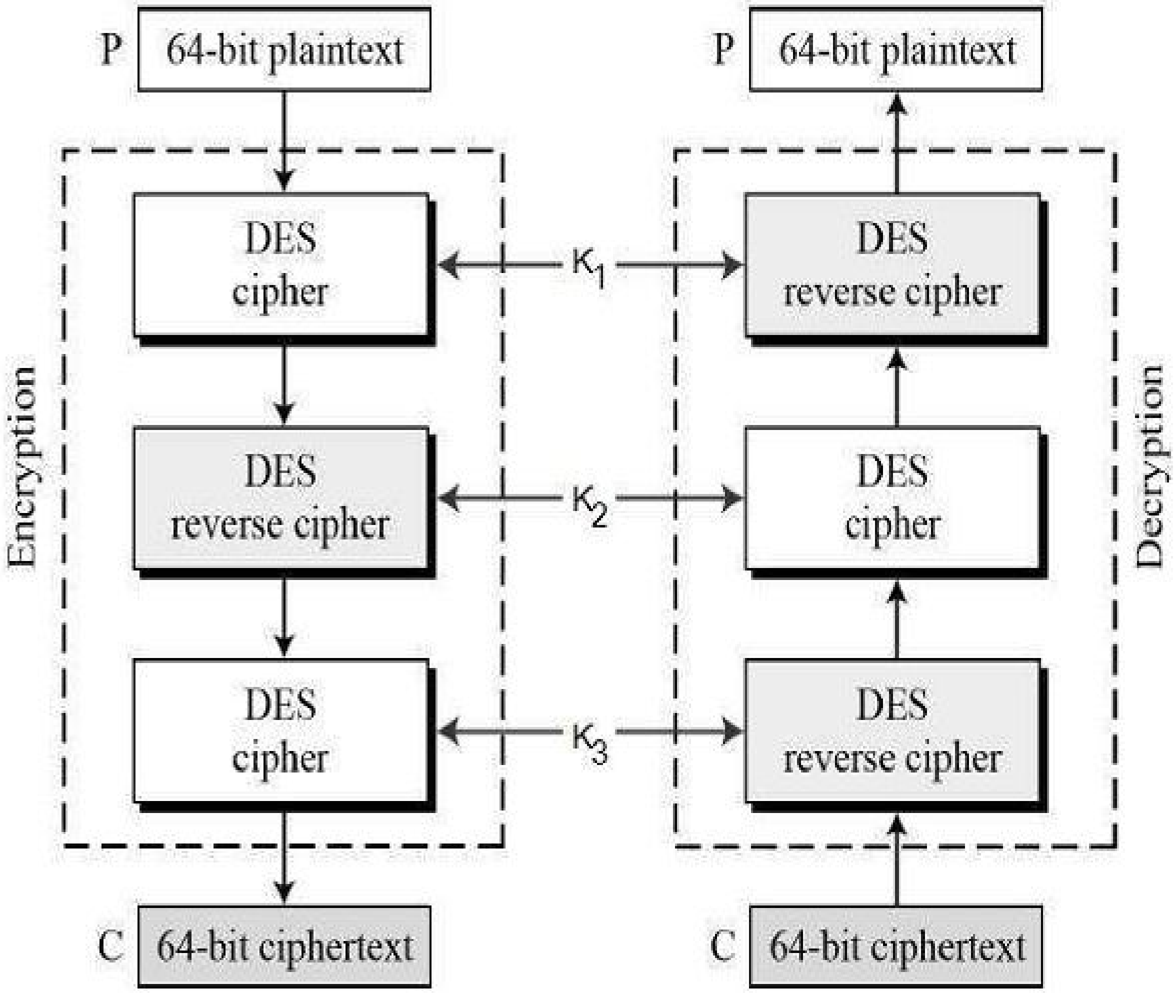
Detailed content of the Lecture:

Strength- The strength of DES lies on two facts:

a. The use of 56-bit keys: 56-bit key is used in encryption, there are 256 possible keys. A brute force attack on such number of keys is impractical.
b. The nature of algorithm: Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness.

3-KEY Triple DES

Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys K_1, K_2 and K_3. This means that the actual 3TDES key has length 3×56 = 168 bits. The encryption scheme is illustrated as follows −



The encryption-decryption process is as follows −

- Encrypt the plaintext blocks using single DES with key K_1.
- Now decrypt the output of step 1 using single DES with key K_2.
- Finally, encrypt the output of step 2 using single DES with key K_3.
- The output of step 3 is the ciphertext.
- Decryption of a ciphertext is a reverse process. User first decrypt using K_3, then encrypt with K_2, and finally decrypt with K_1.

Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K_1, K_2, and K_3 to be the same value. This provides backwards compatibility with DES.

Second variant of Triple DES (2TDES) is identical to 3TDES except that $K_3$is replaced by K_1. In other words, user encrypt plaintext blocks with key K_1, then decrypt with key K_2, and finally encrypt with K_1 again. Therefore, 2TDES has a key length of 112 bits.

Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

- AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware.
- Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael, with a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.
- By contrast, Rijndael per se is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4 × 4 column-major order array of bytes, termed the state.[note 3] Most AES calculations are done in a particular finite field.

For instance, if there are 16 bytes, these bytes are represented as this two-dimensional array:

The key size used for an AES cipher specifies the number of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of rounds are as follows:

- 10 rounds for 128-bit keys.
- 12 rounds for 192-bit keys.
- 14 rounds for 256-bit keys.

Each round consists of several processing steps, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

Important Books/Journals for further learning including the page nos.:
Book: William Stallings," Cryptography and Network Security Principles and Practices", Pearson Education, 2010

Page No: (56)(220-222)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

L-23

LECTURE HANDOUTS

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **II - Symmetric Ciphers & Public Key Cryptography**

Date of Lecture:

Topic of Lecture: The Origins AES

Introduction : (Maximum 5 sentences)

- ✓ Human being from ages had two inherent needs –
- ✓ (a) to communicate and share information and
- ✓ (b) to communicate selectively.

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ DES
- ✓ Encrypt and Decrypt

Detailed content of the Lecture:

Human being from ages had two inherent needs –

(a) to communicate and share information and

(b) to communicate selectively.

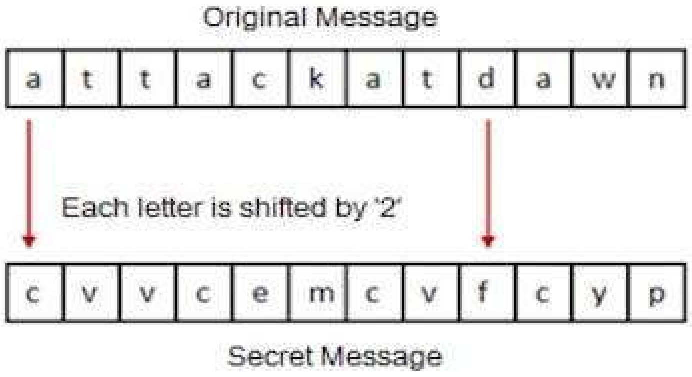
These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information. Unauthorized people could not extract any information, even if the scrambled messages fell in their hand.

The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography.

The word ‘cryptography’ was coined by combining two Greek words, ‘Krypto’ meaning hidden and ‘graphene’ meaning writing.

Hieroglyph − The Oldest Cryptographic Technique

- The first known evidence of cryptography can be traced to the use of ‘hieroglyph’. Some 4000 years ago, the Egyptians used to communicate by messages written in hieroglyph.
- This code was the secret known only to the scribes who used to transmit messages on behalf of the kings.
- The earlier Roman method of cryptography, popularly known as the **Caesar Shift Cipher,** relies on shifting the letters of a message by an agreed number (three was a common choice), the recipient of this message would then shift the letters back by the same number and obtain the original message.



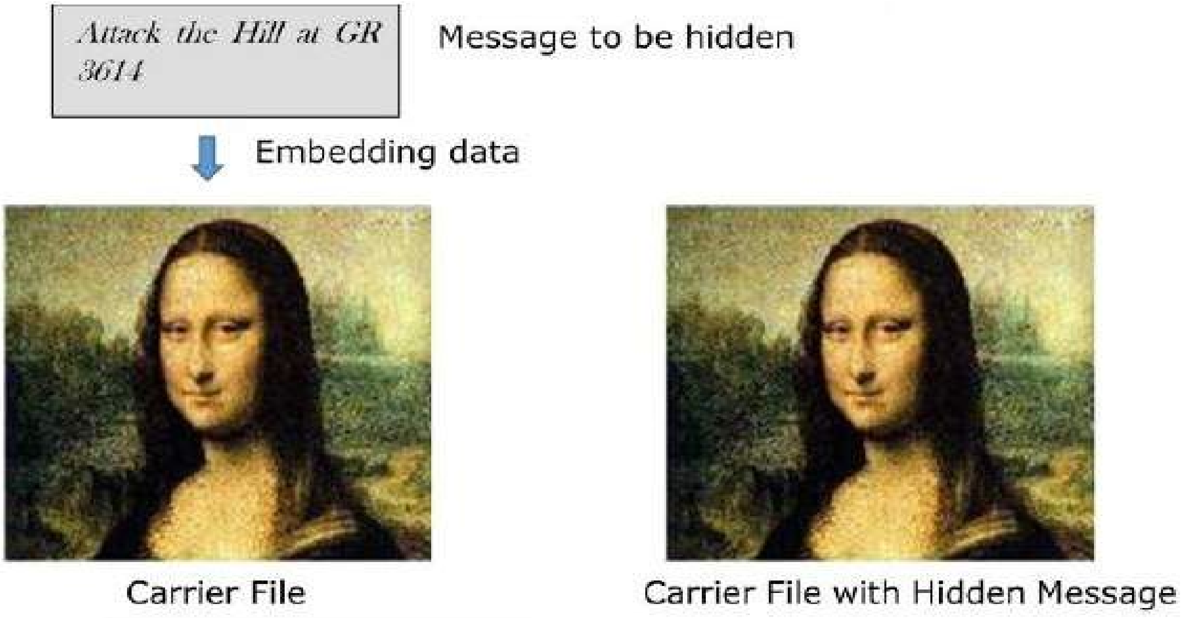
Steganography

- Steganography is similar but adds another dimension to Cryptography. In this method, people not only want to protect the secrecy of an information by concealing it, but they also want to make sure any unauthorized person gets no evidence that the information even exists.

For example, **invisible watermarking**.

In steganography, an unintended recipient or an intruder is unaware of the fact that observed data contains hidden information.

In cryptography, an intruder is normally aware that data is being communicated, because they can see the coded/scrambled message.



Evolution of Cryptography

It is during and after the European Renaissance, various Italian and Papal states led the rapid proliferation of cryptographic techniques. Various analysis and attack techniques were researched in this era to break the secret codes.

- Improved coding techniques such as **Vigenere Coding** came into existence in the 15th century, which offered moving letters in the message with a number of variable places instead of moving them the same number of places.
- Only after the 19th century, cryptography evolved from the ad hoc approaches to encryption to the more sophisticated art and science of information security.
- In the early 20th century, the invention of mechanical and electromechanical machines, such as the **Enigma rotor machine,** provided more advanced and efficient means of coding the

information.

- During the period of World War II, both **cryptography** and **cryptanalysis** became excessively mathematical.

Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/cryptography/origin_of_cryptography.htm

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014 Page No: (52-56)

Course Teacher

Verified by HOD

LECTURE HANDOUTS

L-24

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **II - Symmetric Ciphers & Public Key Cryptography**

Date of Lecture:

Topic of Lecture: AES – Transformation

Introduction : (Maximum 5 sentences)

- ✓ The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES).
- ✓ It is found at least six time faster than triple DES.

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ DES
- ✓ Encrypt and Decrypt

Detailed content of the Lecture:

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

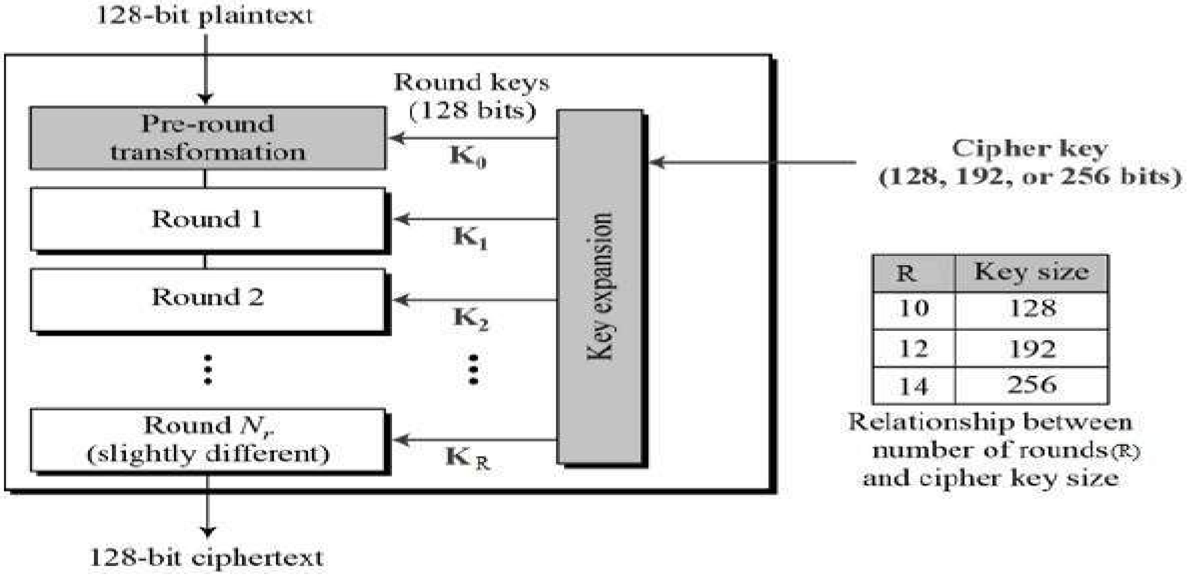
Operation of AES

AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration −

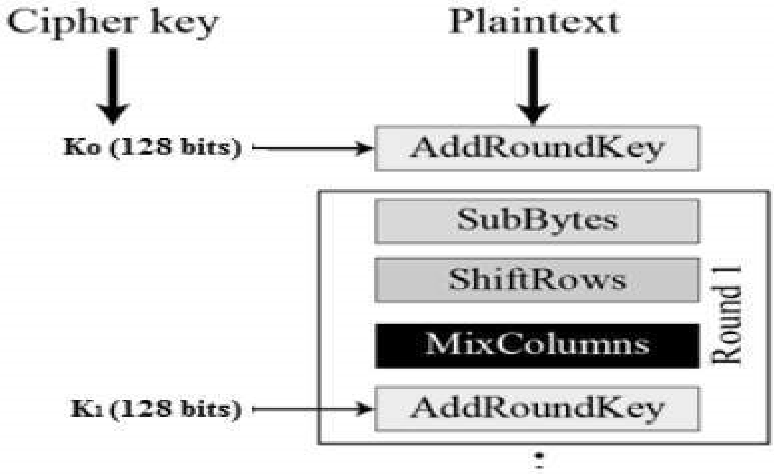


R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below −



Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

Shift rows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

Mix Columns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Add roundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014 Page No: (56-59)

Course Teacher

Verified by HOD

Estd. 2000

LECTURE HANDOUTS

L-25

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **II - Symmetric Ciphers & Public Key Cryptography**

Date of Lecture:

Topic of Lecture: AES – Analysis

Introduction : (Maximum 5 sentences)

- ✓ The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES).
- ✓ It is found at least six time faster than triple DES.

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ DES
- ✓ Encrypt and Decrypt

Detailed content of the Lecture:

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

AES Analysis

- In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered.
- Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches.

However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

- we will discuss the different modes of operation of a block cipher. These are procedural rules for a generic block cipher.
- Interestingly, the different modes result in different properties being achieved which add to the security of the underlying block cipher.

A block cipher processes the data blocks of fixed size. Usually, the size of a message is larger than the block size. Hence, the long message is divided into a series of sequential message blocks, and the cipher operates on these blocks one at a time.

Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014 Page No: (56-59)

Course Teacher

Verified by HOD

LECTURE HANDOUTS

L-26

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **II - Symmetric Ciphers & Public Key Cryptography**

Date of Lecture:

Topic of Lecture: Public key cryptography: Principles of public key cryptosystems

Introduction : (Maximum 5 sentences)

- Public key cryptography (PKC) is an encryption technique that uses a paired public and private key (or asymmetric key) algorithm for secure data communication.
- A message sender uses a recipient's public key to encrypt a message.
- To decrypt the sender's message, only the recipient's private key may be used.
- The two types of PKC algorithms are RSA, which is an acronym named after this algorithm's inventors: Rivest, Shamir and Adelman, and Digital Signature Algorithm (DSA).
- PKC encryption evolved to meet the growing secure communication demands of multiple sectors and industries, such as the military.

PKC is also known as public key encryption, asymmetric encryption, asymmetric cryptography, asymmetric cipher, asymmetric key encryption and Diffie-Hellman encryption.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Plaintext
- Cipher text
- Encryption
- Decryption

Detailed content of the Lecture:

Principles of Public Key Cryptography Also called asymmetric cryptography

• Different from secret key cryptography, algorithms for encoding and decoding differ considerably

• Working with two keys → A private key d (known only to the owner) → A public key e (known by possibly everyone)

• Public key cryptography principle (e.g. RSA): plaintext cipher text plaintext cipher text encryption decryption public key e private key d

• More easily configurable than secret key cryptography, but slower

• Often combined with secret key: authentication and distribution of a secret key (e.g. Diffie-Hellman for establishment of a shared secret)

Security in Public Key Algorithms Security in many public key algorithms is based on the difficulty to factorise and compute discrete logarithms Factorising

→ Find the prime factors for a given number

→ One of the oldest problems in number theory, very time consuming

→ Most popular method: Quadratic Sieve Discrete logarithm

→ Problem to find the inverse to modular exponentiation: Find an x with ax = b mod n for given a and b

→ Not all discrete logarithms have solutions

→ Very time consuming process to find solutions for big numbers

→ Frequently used method: Index-Calculus method

Video Content / Details of website for further learning (if any):
https://www.techopedia.com/definition/9021/public-key-cryptography-pkc

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (244-252)

Course Teacher

Verified by HOD

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **II - Symmetric Ciphers & Public Key Cryptography**

Date of Lecture:

Topic of Lecture: The RSA algorithm-Key management

Introduction : (Maximum 5 sentences)

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and Private key is kept private.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Public key
- Private key

Detailed content of the Lecture:

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and Private key is kept private.

An example of asymmetric cryptography :

1. A client (for example browser) sends its public key to the server and requests for some data.
2. The server encrypts the data using client's public key and sends the encrypted data.
3. Client receives this data and decrypts it.

Key Generation Algorithm:

This is the original algorithm.

1. Generate two large random primes, pp and qq, of approximately equal size such that their product n=pqn=pq is of the required bit length, e.g. 1024 bits. [See note 1].
2. Compute n=pqn=pq and ϕ=(p−1)(q−1)ϕ=(p−1)(q−1). [See note 6].
3. Choose an integer ee, 1<e<ϕ1<e<ϕ, such that gcd(e,ϕ)=1gcd(e,ϕ)=1. [See note 2].
4. Compute the secret exponent dd, 1<d<ϕ1<d<ϕ, such that ed≡1modϕed≡1modϕ. [See note 3].
5. The public key is (n,e)(n,e) and the private key (d,p,q)(d,p,q). Keep all the values d, p, q and ϕϕ secret. [Sometimes the private key is written as (n,d)(n,d) because you need the value of n when using d. Other times we might write the key pair as ((N,e),d)((N,e),d).]

- n is known as the modulus.
- e is known as the public exponent or encryption exponent or just the exponent.
- d is known as the secret exponent or decryption exponent.

Practical Key exchange Algorithm

Incorporating the advice given in the notes below, a practical algorithm to generate an RSA key pair is given below. Typical bit lengths are k=1024,2048,3072,4096,...k=1024,2048,3072,4096,..., with increasing computational expense for larger values. You will not go far wrong if you choose ee as 65537 (=0x10001) in step (1).

Algorithm: Generate an RSA key pair.

INPUT: Required modulus bit length, kk.
OUTPUT: An RSA key pair ((N,e),d)((N,e),d) where N is the modulus, the product of two primes (N=pqN=pq) not exceeding kk bits in length; ee is the public exponent, a number less than and coprime to (p−1)(q−1)(p−1)(q−1); and dd is the private exponent such that ed≡1mod(p−1)(q−1)ed≡1mod(p−1)(q−1).

```
1.  Select a value of ee from 3,5,17,257,655373,5,17,257,65537
2.  repeat
3.     p ← genprime(k/2)
4.  until (pmode)≠1(pmode)≠1
5.  repeat
6.     q ← genprime(k - k/2)
7.  until (qmode)≠1(qmode)≠1
8.  N ← pq
9.  L ← (p-1)(q-1)
10. d ← modinv(e, L)
11. return (N,e,d)(N,e,d)
```

The function genprime(b) returns a prime of exactly bb bits, with the bbth bit set to 1. Note that the operation k/2k/2 is integer division giving the integer quotient with no fraction.

If you've chosen e=65537e=65537 then the chances are that the first prime returned in steps (3) and (6) will pass the tests in steps (4) and (7), so each repeat-until loop will most likely just take one iteration. The final value of NN may have a bit length slightly short of the target kk. This actually does not matter too much (providing the message m is always < N), but some schemes require a modulus of exact length. If this is the case, then just repeat the entire algorithm until you get one. It should not take too many goes. Alternatively, use the trick setting the two highest bits in the prime candidates described in note 1.

Encryption:

Sender A does the following:-

1. Obtains the recipient B's public key (n,e)(n,e).
2. Represents the plaintext message as a positive integer mm with 1<m<n1<m<n [see note 4].
3. Computes the ciphertext c=memodnc=memodn.
4. Sends the ciphertext cc to B.

Decryption:

Recipient B does the following:-

1. Uses his private key (n,d)(n,d) to compute m=cdmodnm=cdmodn.

2. Extracts the plaintext from the message representative mm.

Digital signing

Sender A does the following:-

1. Creates a message digest of the information to be sent.
2. Represents this digest as an integer mm between 1 and n−1n−1 [See note 5].
3. Uses her private key (n,d)(n,d) to compute the signature s=mdmodns=mdmodn.
4. Sends this signature ss to the recipient, B.

Signature Verification:

Recipient B does the following (older method):-

1. Uses sender A's public key (n,e)(n,e) to compute integer v=semodnv=semodn.
2. Extracts the message digest HH from this integer.
3. Independently computes the message digest H′H′ of the information that has been signed.
4. If both message digests are identical, i.e. H=H′H=H′, the signature is valid.

More secure method:-

1. Uses sender A's public key (n,e)(n,e) to compute integer v=semodnv=semodn.
2. Independently computes the message digest H′H′ of the information that has been signed.
3. Computes the expected representative integer v′v′ by encoding the expected message digest H′H′.
4. If v=v′v=v′, the signature is valid

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

https://www.di-mgt.com.au/rsa_alg.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (252-266)

Course Teacher

Verified by HOD

LECTURE HANDOUTS

L-28

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **II - Symmetric Ciphers & Public Key Cryptography**

Date of Lecture:

Topic of Lecture: Diffie Hellman Key exchange

Introduction : (Maximum 5 sentences)

- **Diffie-Hellman key exchange**, also called exponential **key exchange**, is a method of digital encryption that uses numbers raised to specific powers to produce decryption **key**s on the basis of components that are never directly transmitted, making the task of a would-be code breaker mathematically overwhelming.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Plaintext
- Cipher text
- Encryption
- Decryption
- Private key
- Public key

Detailed content of the Lecture:

Diffie-Hellman key exchange, also called exponential **key exchange**, is a method of digital encryption that uses numbers raised to specific powers to produce decryption **key**s on the basis of components that are never directly transmitted, making the task of a would-be code breaker mathematically overwhelming.

The mod function

The main ingredient is the "remainder" or "modulo" or "mod" function, denoted % in Perl. For example, 25%10 is 5 (say "25 mod 10 is 5") and 25%16 is 9 ("25 mod 16 is 9"). For n%10, the result will always be one of 0,1,...,9.

As you can see, any positive integer modulo 10 is just the last digit in base 10: 1537%10 is 7, etc. You can think of "modulo 10" for positive integers as meaning "ignore all decimal digits except the last one".

Doing "modular arithmetic" with "modulus" 10 means doing addition, subtraction, and multiplication (including powers) where you only care about the remainder modulo 10. You can use some other modulus m instead of 10, as long as it's the same through the whole problem. It works very smoothly.

Example 1. To find 1537 x 4248 modulo 10, you could multiply out and take the last digit, but a better way would be to replace 1537 by 7 and 4248 by 8 to start, find 7 x 8 = 56, and then take 56 mod 10 to get 6 as the answer.

A handy standard notation is to write a $\equiv$ b (mod m) if a and b have the same remainder modulo m. This is read "a is congruent to b modulo m". In this notation the example just mentioned looks like this: 1537 x 4248 $\equiv$ 7 x 8 = 56 $\equiv$ 6 (mod 10).

Example 3. Find **all** the powers of 2 up to 2^{10}, each modulo 11.

Solution. Keep doubling, taking remainders modulo 11 whenever possible:

2, 4, 8, 16 $\equiv$ 5, 10, 20 $\equiv$ 9, 18 $\equiv$ 7, 14 $\equiv$ 3, 6, 12 $\equiv$ 1 (mod 11). So the answer is 2, 4, 8, 5, 10, 9, 7, 3, 6, 1.

Notice that the powers of 2 run through all possible remainders modulo 11, except 0. We say 2 is a "generator" modulo 11. There is a theorem that if you take a **prime** modulus, then there is always **some** generator, and in fact 2 often works. If 2 doesn't, maybe 3 will.

The Diffie-Hellman method

The idea of Diffie and Hellman is that it's easy to compute powers modulo a prime but hard to reverse the process: If someone asks **which** power of 2 modulo 11 is 7, you'd have to experiment a bit to answer, even though 11 is a small prime. If you use a huge prime istead, then this becomes a very difficult problem even on a computer. Steps:

1. Alice and Bob, using insecure communication, agree on a huge prime p and a generator g. They don't care if someone listens in.
2. Alice chooses some large random integer $x_A < p$ and keeps it secret. Likewise Bob chooses $x_B < p$ and keeps it secret. These are their "private keys".
3. Alice computes her "public key" $y_A \equiv g^{x_A}$ (mod p) and sends it to Bob using insecure communication. Bob computes his public key $y_B \equiv g^{x_B}$ and sends it to Alice. Here $0 < y_A < p$, $0 < y_B < p$.

   As already mentioned, sending these public keys with insecure communication is safe because it would be too hard for someone to compute x_A from y_A or x_B from y_B, just like the powers of 2 above.

4. Alice computes $z_A \equiv y_B^{x_A}$ (mod p) and Bob computes $z_B \equiv y_A^{x_B}$ (mod p). Here $z_A < p$, $z_B < p$.

   But $z_A = z_B$, since $z_A \equiv y_B^{x_A} \equiv (g^{x_B})^{x_A} = g^{(x_A x_B)}$ (mod p) and similarly $z_B \equiv (g^{x_A})^{x_B} = g^{(x_A x_B)}$ (mod p). So this value is their **shared secret key**. They can use it to encrypt and decrypt the rest of their communication by some faster method.

   In this calculation, notice that the step $y_B^{x_A} \equiv (g^{x_B})^{x_A}$ involved replacing g^{x_B} by its remainder y_B, (in the reverse direction) so we were really using the "as often as you want" principle.

Video Content / Details of website for further learning (if any):
https://www.math.ucla.edu/~baker/40/handouts/rev_DH/node1.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014
Page No: (277-281)

Course Teacher

Verified by HOD

Estd. 2000

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L17

LECTURE HANDOUTS

L-29

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **II - Symmetric Ciphers & Public Key Cryptography**

Date of Lecture:

Topic of Lecture: Elliptic curve arithmetic

Introduction : (Maximum 5 sentences)

- ✓ Elliptic Curve Arithmetic. The principal attraction of ECC, compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead.
- ✓ Most of the products and standards that use public-key cryptography for encryp- tion and digital signatures use RSA.

Prerequisite knowledge for Complete understanding and learning of Topic:

- ➢ RSA Algorithm
- ➢ Diffie Hellman
- ➢ Public Key
- ➢ Private Key

Detailed content of the Lecture:

- ✓ Elliptic Curve Arithmetic. The principal attraction of ECC, compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead.
- ✓ Most of the products and standards that use public-key cryptography for encryp- tion and digital signatures use RSA.

Elliptic Curves Let K be a field.

An elliptic curve E over K is defined by the Weierstrass equation:

E : y 2 +a1xy+a3y = x 3 +a2x 2 +a4x+a6, ai ∈ K.

The curve should be smooth (no singularities).

Special forms charK 6= 2,3: y 2 = x 3 +ax+b, a,b ∈ K.

charK = 3: y 2 = x 3 +b2x 2 +b4x+b6, bi ∈ K.

charK = 2: Non-supersingular or ordinary

curve: y 2 +xy = x 3 +ax2 +b, a,b ∈ K. Supersingular

curve: y 2 +ay = x 3 +bx+c, a,b, c ∈ K.

The Elliptic-Curve Group Any (x, y) ∈ K 2 satisfying the equation of an elliptic curve E is called a K-rational point on E.

Example of Elliptic-Curve Arithmetic

E : y 2 = x 3 −5x+1 defined over F17.

Take the finite points P = (3,8) and Q = (10,13) on E.

Opposite: −P = (3,9), and −Q = (10,4).

Point addition The line L joining P and Q has slope λ ≡ 13−8 10−3 ≡ 8 (mod 17).

L has equation L : y = 8x+c. Since L passes through P, we have c = 1.

Substitute this in the equation for E to get (8x+1) 2 ≡ x 3 −5x+1 (mod 17), that is, x 3 +4x 2 +13x ≡ 0 (mod 17), that is, x(x−3)(x−10) ≡ 0 (mod 17).

The third point of intersection is (0,1), so P+Q = −(0,1) = (0,16). Point doubling The tangent T to E at P has slope 3×3 2−5 2×8 ≡ 12 (mod 17).

The equation for T is y = 12x+6. Substitute T in E to get x 3 +9x 2 +4x+16 ≡ 0 (mod 17), that is, (x−3) 2 (x−2) ≡ 0 (mod 17).

The third point of intersection is (2,13), so 2P = −(2,13) = (2,4).

Video Content / Details of website for further learning (if any):
https://cse.iitkgp.ac.in/~abhij/download/doc/ECC.pdf

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014
Page No: (285-293)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L-30

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **II - Symmetric Ciphers & Public Key Cryptography**

Date of Lecture:

Topic of Lecture: Elliptic curve cryptography.

Introduction : (Maximum 5 sentences)

- ✓ Elliptic Curve Arithmetic. The principal attraction of ECC, compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead.
- ✓ Most of the products and standards that use public-key cryptography for encryption and digital signatures use RSA.

Prerequisite knowledge for Complete understanding and learning of Topic:

- ➢ RSA Algorithm
- ➢ Diffie Hellman
- ➢ Public Key
- ➢ Private Key

Detailed content of the Lecture:

- ✓ Elliptic Curve Arithmetic. The principal attraction of ECC, compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead.
- ✓ Most of the products and standards that use public-key cryptography for encryption and digital signatures use RSA.

Elliptic Curves Let K be a field.

An elliptic curve E over K is defined by the Weierstrass equation:

E : y 2 +a1xy+a3y = x 3 +a2x 2 +a4x+a6, ai ∈ K.

The curve should be smooth (no singularities).

Special forms charK 6= 2,3: y 2 = x 3 +ax+b, a,b ∈ K.

charK = 3: y 2 = x 3 +b2x 2 +b4x+b6, bi ∈ K.

charK = 2: Non-super singular or ordinary

curve: y 2 +xy = x 3 +ax2 +b, a,b ∈ K. Super singular

curve: y 2 +ay = x 3 +bx+c, a,b, c ∈ K.

The Elliptic-Curve Group Any (x, y) ∈ K 2 satisfying the equation of an elliptic curve E is called a K-rational point on E.

Point at infinity:

- ➢ There is a single point at infinity on E, denoted by O.
- ➢ This point cannot be visualized in the two-dimensional (x, y) plane.
- ➢ The point exists in the projective plane.
- ➢ E(K) is the set of all finite K-rational points on E and the point at infinity.
- ➢ An additive group structure can be defined on E(K).
- ➢ O acts as the identity of the group

  Size of the Elliptic-Curve Group

  Let E be an elliptic curve defined over Fq = Fp n .

  Hasse's Theorem:

$|E(Fq)| = q+1-t$, where $-2 \sqrt{q}$ 6 t 6 $2 \sqrt{q}$. t is called the trace of Frobenius at q.

If t = 1, then E is called anomalous.

If p|t, then E is called super singular. If p6 |t, then E is called non-super singular or ordinary.

Let $\alpha,\beta \in C$ satisfy $1-tx+qx2 = (1-\alpha x)(1-\beta x)$.

Then,

$|E(Fq\ m\ )| = q\ m\ +1-(\alpha\ m\ +\beta\ m)$.

Note: E(Fq) is not necessarily cyclic.

Video Content / Details of website for further learning (if any):
https://cse.iitkgp.ac.in/~abhij/download/doc/ECC.pdf

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014
Page No: (293-296)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L

L-31

LECTURE HANDOUTS

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **III - Data Integrity Algorithms and Digital Signatures**

Date of Lecture:

Topic of Lecture: Hash Functions

Introduction : (Maximum 5 sentences)

- A variation on the message authentication code is the one way hash function. As with MAC, a hash function accepts a variable size message M as input and produces a fixed-size output, referred to as hash code H(M).
- Unlike a MAC, a hash code does not use a key but is a function only of the input message. The hash code is also referred to as a message digest or hash value.

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- Hash Functions
- MAC

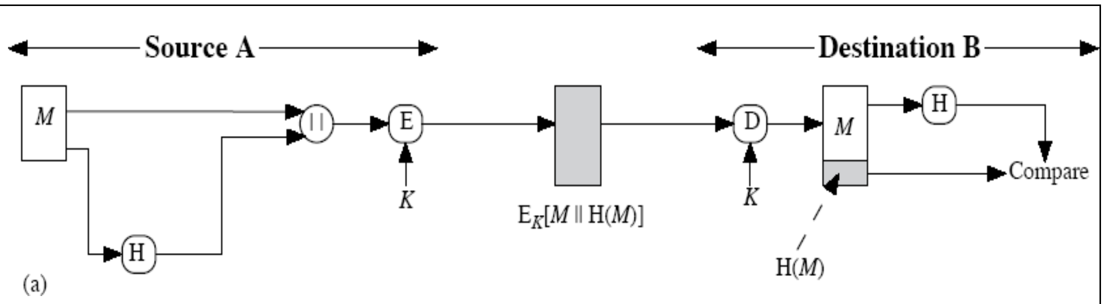
Detailed content of the Lecture:

HASH FUNCTIONS

- A variation on the message authentication code is the one way hash function. As with MAC, a hash function accepts a variable size message M as input and produces a fixed-size output, referred to as hash code H(M).
- Unlike a MAC, a hash code does not use a key but is a function only of the input message. The hash code is also referred to as a message digest or hash value.

There are varieties of ways in which a hash code can be used to provide message authentication, as follows:

- The message plus the hash code is encrypted using symmetric encryption. This is identical to that of internal error control strategy. Because encryption is applied to the entire message plus the hash code, confidentiality is also provided.



N Only the hash code is encrypted, using symmetric encryption. This reduces the processing burden for those applications that do not require confidentiality.

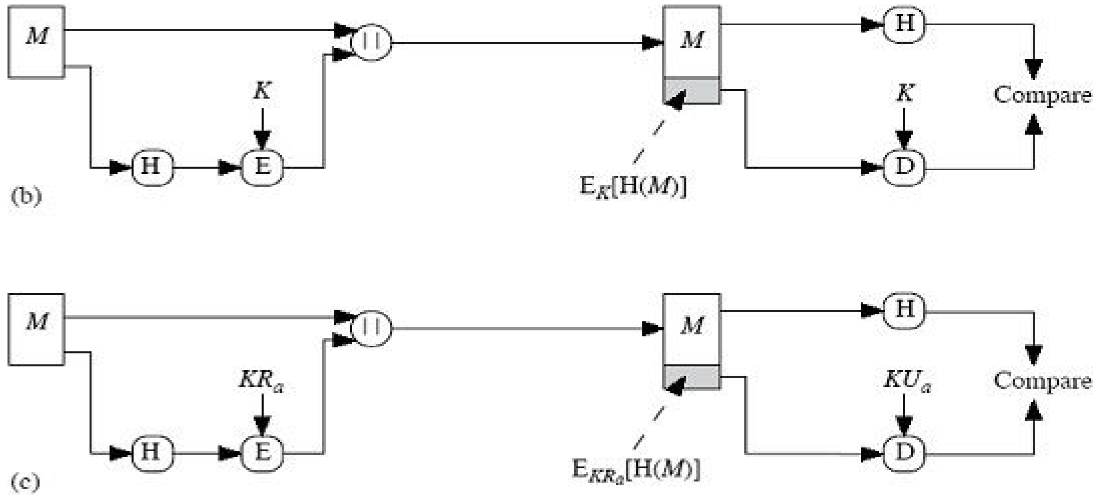
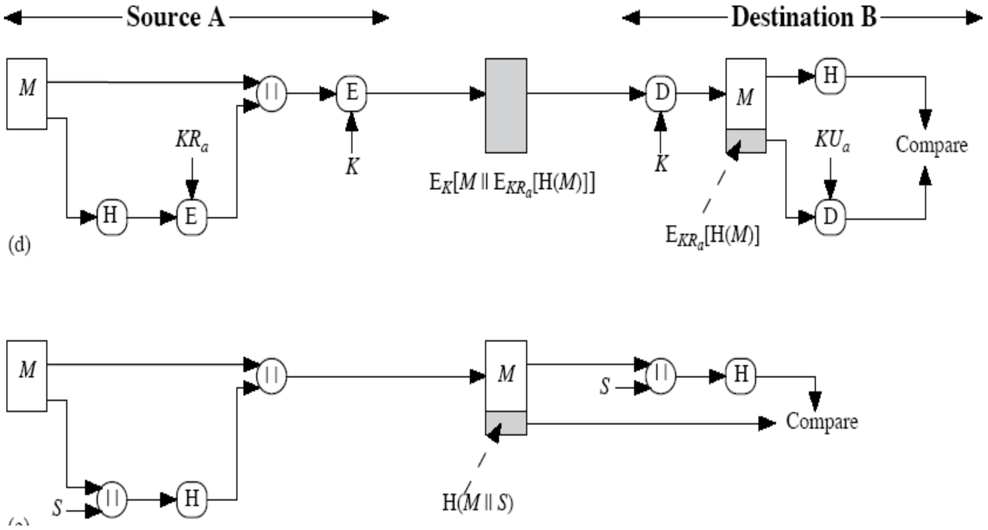


Fig.3.3.1: Basic Use of Hash Functions

c) Only the hash code is encrypted, using the public key encryption and using the sender‟s private key. It provides authentication plus the digital signature.

d) If confidentiality as well as digital signature is desired, then the message plus the public key encrypted hash code can be encrypted using a symmetric secret key.



e) This technique uses a hash function, but no encryption for message authentication. This technique assumes that the two communicating parties share a common secret value „S‟. The source computes the hash value over the concatenation of M and S and appends the resulting hash value to M.

f) Confidentiality can be added to the previous approach by encrypting the entire message plus the hash code.

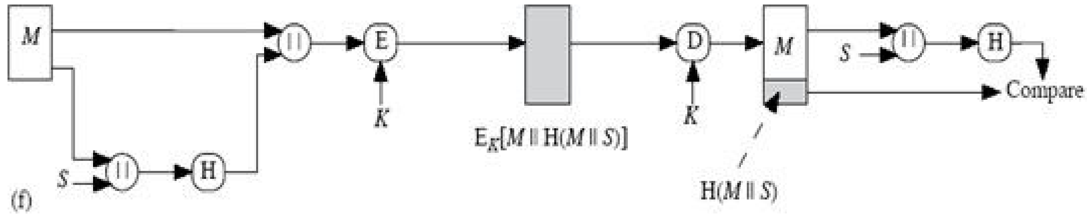


Fig3.3.2: Basic Use of Hash Functions

A hash value h is generated by a function H of the form

$$h = H(M)$$

where M is a variable-length message and H(M) is the fixed-length hash value. The hash value is appended to the message at the source at a time when the message is assumed orknown to be correct. The receiver authenticates that message by recomputing the hashvalue.

SIMPLE HASH FUNCTIONS

All hash functions operate using the following general principles. The input (message, file, etc.) is viewed as a sequence of n-bit blocks. The input is processed one block at a time in an iterative fashion to produce an n-bit hash function.

One of the simplest hash functions is the bit-by-bit exclusive-OR (XOR) of every block. This can be expressed as follows:

$$C_i = b_{i1} \quad b_{i1} \quad ... \quad b_{im} \oplus \quad \oplus \quad \oplus$$

where

C_i = ith bit of the hash code, 1 ≤i ≤n m = number of n-bit blocks in the input

b_{ij} = ith bit in jth block $\oplus$ = XOR operation Thus, the probability that a data error will result in an unchanged hash value is 2^n. With more predictably formatted data, the function is less effective. For example, in most normal text files, the high-order bit of each octet is always zero. So if a 128-bit hash value is used, instead of an effectiveness of 2^{128}, the hash function on this type of data has an effectiveness of 2^{112}.

Birthday Attacks

Suppose that a 64-bit hash code is used. One might think that this is quite secure. For example, if an encrypted hash code C is transmitted with the corresponding unencrypted message M, then an opponent would need to find an M' such that H(M') = H(M) to substitute another message and fool the receiver.

1. The opponent generates $2^{m/2}$ variations on the message, all of which convey essentially the same meaning. (fraudulent message
2. The two sets of messages are compared to find a pair of messages that produces the same hash code. The probability of success, by the birthday paradox, is greater than 0.5. If no match is found, additional valid and fraudulent messages are generated until a match is

made.

3. The opponent offers the valid variation to A for signature. This signature can then be attached to the fraudulent variation for transmission to the intended recipient. Because the two variations have the same hash code, they will produce the same signature; the opponent is assured of success even though the encryption key is not known.

Thus, if a 64-bit hash code is used, the level of effort required is only on the order of 2^{32} .

Block Chaining Techniques

Divide a message M into fixed-size blocks $M_1, M_2, \ldots,$ M_N and use a symmetric encryption system such as DES to compute the hash code G as follows:

H_o = initial

value Hi = EMi

[Hi-1]

Furthermore, another version of the birthday attack can be used even if the opponent has access to only one message and its valid signature and cannot obtain multiple signings.

Here is the scenario; we assume that the opponent intercepts a message with a signature in the form of an encrypted hash code and that the unencrypted hash code is m bits long:

1. Use the algorithm defined at the beginning of this subsection to calculate the unencrypted hash code G.
2. Construct any desired message in the form $Q_1, Q_2, \ldots, Q_{N2}$.
3. Compute for $H_i = EQ_i\,[H_{i-1}\,]$for $1 \leq i \leq (N-2)$.
4. Generate $2^{m/2}$ random blocks; for each block X, compute $E_X[H_{N-2}.]$ Generate an additional $2^{m/2}$ random blocks; for each block Y, compute $D_Y[G]$, where D is the decryption function corresponding to E.
5. Based on the birthday paradox, with high probability there will be an X and Y such that $E_X\,[H_{N-2}\,] = D_Y[\,G]$.
6. Form the message $Q_1, Q_2, \ldots, Q_{N-2}$, X, Y. This message has the hash code G and therefore can be used with the intercepted encrypted signature.

This form of attack is known as a **meet-in-the-middle attack**.

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html.

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014
Page No: (304,310- 312)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

L

LECTURE HANDOUTS

L-32

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **III - Data Integrity Algorithms and Digital Signatures**

Date of Lecture:

Topic of Lecture: Hash Function – Applications

Introduction : (Maximum 5 sentences)

- The hash function takes an input message and partitions it into L fixed-sized blocks of b bits each. If necessary, the final block is padded to b bits. The final block also includes the value of the total length of the input to the hash function.
- The inclusion of the length makes the job of the opponent more difficult. Either the opponent must find two messages of equal length that hash to the same value or two messages of differing lengths that, together with their length values, hash to the same value

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ HASH FUNCTION
- ✓ MAC
- ✓ CMAC

Detailed content of the Lecture:

Security of Hash Functions and Macs

Just as with symmetric and public-key encryption, we can group attacks on hash functions and MACs into two categories: brute-force attacks and cryptanalysis.

Brute-Force Attacks

The nature of brute-force attacks differs somewhat for hash functions and MACs.

Hash Functions

The strength of a hash function against brute-force attacks depends solely on the length of the hash code produced by the algorithm. Recall from our discussion of hash functions that there are three desirable properties:

- One-way: For any given code h, it is computationally infeasible to find x such that H(x) = h.
- Weak collision resistance: For any given block x, it is computationally infeasible to find y x with H(y) = H(x).
- Strong collision resistance: It is computationally infeasible to find any pair (x, y)

such that H(x) = H(y).

For a hash code of length n, the level of effort required, as we have seen is proportional to the following:

One way	$_2$n
Weak collision resistance	$_2$n
Strong collision resistance	$_2$n/2

Message Authentication Codes

A brute-force attack on a MAC is a more difficult undertaking because it requires known message-MAC pairs.. To attack a hash code, we can proceed in the following way. Given a fixed message x with n-bit hash code h = H(x), a brute-force method of finding a collision is to pick a random bit string y and check if H(y) = H(x). The attacker can do this repeatedly off line. To proceed, we need to state the desired security property of a MAC algorithm, which can be expressed as follows:

Computation resistance: Given one or more text-MAC pairs (x_i, $C_K[x_i]$), it is computationally infeasible to compute any text-MAC pair (x, C_K(x)) for any new input x $\neq x_i$.

To summarize, the level of effort for brute-force attack on a MAC algorithm can be expressed as min(2^k, 2^n). The assessment of strength is similar to that for symmetric encryption algorithms. It would appear reasonable to require that the key length and MAC length satisfy a relationship such as min(k, n) ≥N, where N is perhaps in the range of 128 bits.

Cryptanalysis

As with encryption algorithms, cryptanalytic attacks on hash functions and MAC algorithms seek to exploit some property of the algorithm to perform some attack other than an exhaustive search.

HASH FUNCTIONS

In recent years, there has been considerable effort, and some successes, in developing cryptanalytic attacks on hash functions. To understand these, we need to look at the overall structure of a typical secure hash function, and is the structure of most hash functions in use today, including SHA and Whirlpool.

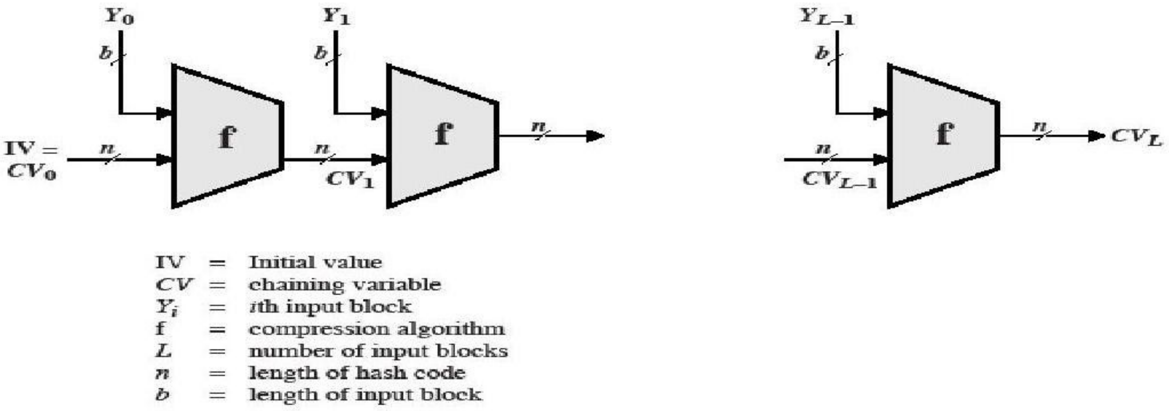


Fig.3.7.1: General Structure of Secure Hash Code

The hash function takes an input message and partitions it into L fixed-sized blocks of b bits each. If necessary, the final block is padded to b bits. The final block also includes the value of the total length of the input to the hash function. The inclusion of the length makes the job of the opponent more difficult. Either the opponent must find two messages of equal length that hash to the same value or two messages of differing lengths that, together with their length values, hash to the samevalue.

The hash algorithm involves repeated use of a **compression function**, f, that takes two inputs (an n-bit input from the previous step, called the chaining variable, and a b-bit block) and produces an n-bit output. At the start of hashing, the chaining variable has an initial value that is specified as part of the algorithm. The final value of the chaining variable is the hash value. Often, $b > n$; hence the term compression. The hash function can be summarized as follows:

$$CV_o = IV = \text{initial n-bit value}$$

$$CV_i = f(CV_{i-1}, Y_{i-1}) \; 1 \leq i \leq L$$

$$H(M) = CV_L$$

where the input to the hash function is a message M consisting of the blocks Y_o, Y_1,..., $Y_{L-1.}$ The structure can be used to produce a secure hash function to operate on a message of any length.

Message Authentication Codes

There is much more variety in the structure of MACs than in hash functions, so it is difficult to generalize about the cryptanalysis of MACs. Further, far less work has been done on developing such attacks.

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014
Page No: (305-310),(312-318)

Course Teacher

Verified by HOD

Estd. 2000

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L

L-33

LECTURE HANDOUTS

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **III - Data Integrity Algorithms and Digital Signatures**

Date of Lecture:

Topic of Lecture: Hash Functions – Requirements

Introduction : (Maximum 5 sentences)

- A variation on the message authentication code is the one way hash function. As with MAC, a hash function accepts a variable size message M as input and produces a fixed-size output, referred to as hash code H(M).
- Unlike a MAC, a hash code does not use a key but is a function only of the input message. The hash code is also referred to as a message digest or hash value.

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- Hash Functions
- MAC

Detailed content of the Lecture:

HASH FUNCTIONS

- A variation on the message authentication code is the one way hash function. As with MAC, a hash function accepts a variable size message M as input and produces a fixed-size output, referred to as hash code H(M).
- Unlike a MAC, a hash code does not use a key but is a function only of the input message. The hash code is also referred to as a message digest or hash value.

There are varieties of ways in which a hash code can be used to provide message authentication, as follows:

- The message plus the hash code is encrypted using symmetric encryption. This is identical to that of internal error control strategy.
- Because encryption is applied to the entire message plus the hash code, confidentiality is also provided.

Requirements for a Hash Function

1. H can be applied to a block of data of any size.
2. H produces a fixed-length output.
3. H(x) is relatively easy to compute for any given x, making both hardware and software

implementations practical.

4. For any given value h, it is computationally infeasible to find x such that H(x) = h. This is sometimes referred to in the literature as the one-way property.
5. For any given block x, it is computationally infeasible to find y, x such that H(y) = H(x). This is sometimes referred to as **weak collision resistance**.
6. It is computationally infeasible to find any pair (x, y) such that H(x) = H(y). This is sometimes referred to as **strong collision resistance**.

The first three properties are requirements for the practical application of a hash function to message authentication.

The fourth property, the one-way property, states that it is easy to generate a code given a message but virtually impossible to generate a message given a code.

The fifth property guarantees that an alternative message hashing to the same value as a given message cannot be found. This prevents forgery when an encrypted hash code is used (Figures b and c).

The sixth property refers to how resistant the hash function is to a type of attack known as the birthday attack, which we examine shortly.

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html.

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014
Page No: (304,310- 312)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L11

LECTURE HANDOUTS

L-34

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **III - Data Integrity Algorithms and Digital Signatures**

Date of Lecture:

Topic of Lecture: Secure Hash Algorithm (SHA)

Introduction : (Maximum 5 sentences)

- SHA originally designed by NIST & NSA in 1993 was revised in 1995 as SHA-1
- US standard for use with DSA signature scheme
  - ✓ standard is FIPS 180-1 1995, also Internet RFC3174
  - ✓ nb. the algorithm is SHA, the standard is SHS
- based on design of MD4 with key differences
- produces 160-bit hash values
- recent 2005 results on security of SHA-1 have raised concerns on its use in future applications

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- ✓ Hash fuction
- ✓ Cmac
- ✓ Mac
- ✓ SHA

Detailed content of the Lecture:

- SHA originally designed by NIST & NSA in 1993 was revised in 1995 as SHA-1
- US standard for use with DSA signature scheme
  - ✓ standard is FIPS 180-1 1995, also Internet RFC3174
  - ✓ nb. the algorithm is SHA, the standard is SHS
- based on design of MD4 with key differences
- produces 160-bit hash values
- recent 2005 results on security of SHA-1 have raised concerns on its use in

future applications

SECURE HASH ALGORITHM

- SHA originally designed by NIST & NSA in 1993 was revised in 1995 as SHA-1
- US standard for use with DSA signature scheme
  - ✓ standard is FIPS 180-1 1995, also Internet RFC3174
  - ✓ nb. the algorithm is SHA, the standard is SHS
- based on design of MD4 with key differences
- produces 160-bit hash values
- recent 2005 results on security of SHA-1 have raised concerns on its use in future applications

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: 319-329

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L-35

LECTURE HANDOUTS

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **III - Data Integrity Algorithms and Digital Signatures**

Date of Lecture:

Topic of Lecture: SHA- 512

Introduction : (Maximum 5 sentences)

- SHA originally designed by NIST & NSA in 1993 was revised in 1995 as SHA-1
- US standard for use with DSA signature scheme
  - ✓ standard is FIPS 180-1 1995, also Internet RFC3174
  - ✓ nb. the algorithm is SHA, the standard is SHS
- based on design of MD4 with key differences
- produces 160-bit hash values
- recent 2005 results on security of SHA-1 have raised concerns on its use in future applications

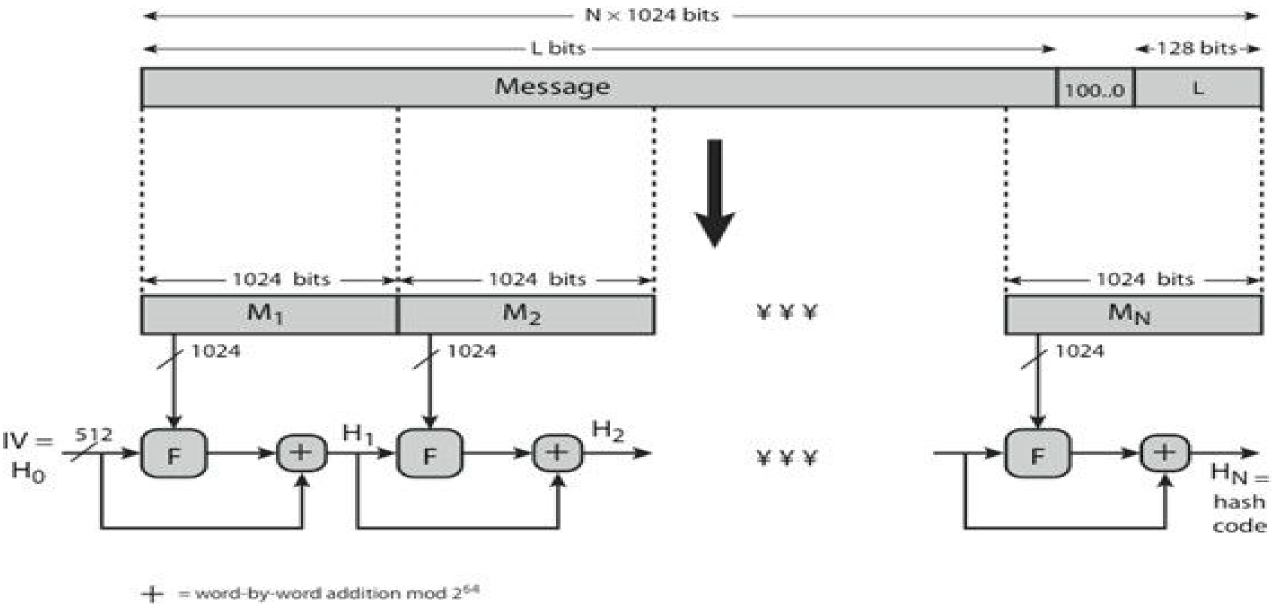
Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- ✓ Hash fuction
- ✓ Cmac
- ✓ Mac
- ✓ SHA

Detailed content of the Lecture:

- SHA originally designed by NIST & NSA in 1993 was revised in 1995 as SHA-1
- US standard for use with DSA signature scheme
  - ✓ standard is FIPS 180-1 1995, also Internet RFC3174
  - ✓ nb. the algorithm is SHA, the standard is SHS
- based on design of MD4 with key differences
- produces 160-bit hash values
- recent 2005 results on security of SHA-1 have raised concerns on its use in future applications

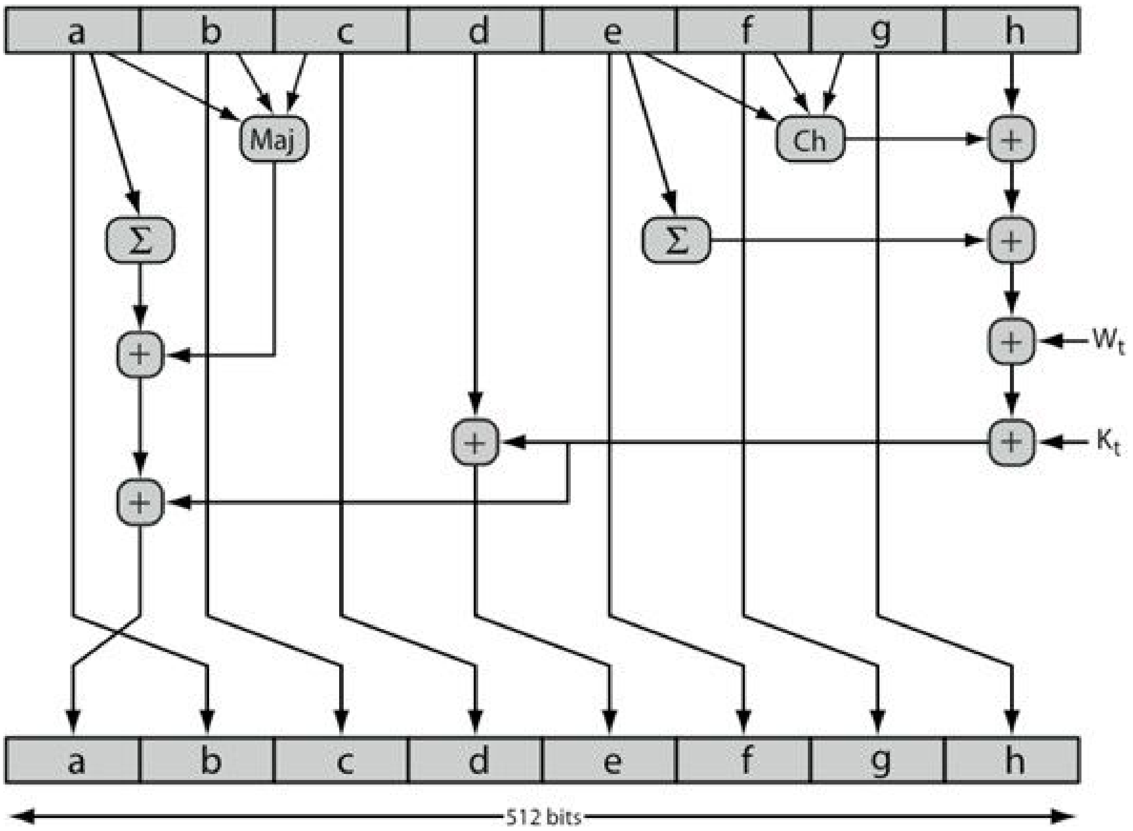
SHA-512 Overview



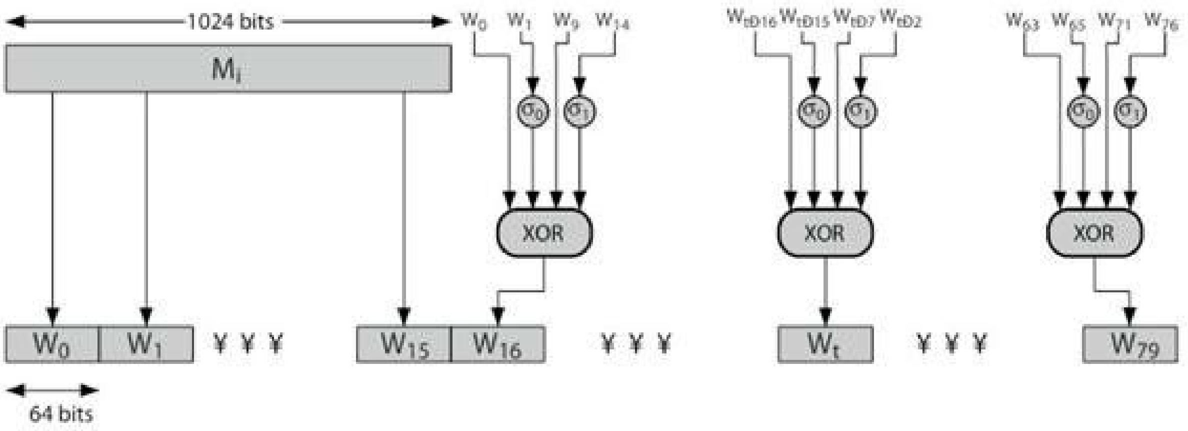
SHA-512 Compression Function

- heart of the algorithm
- processing message in 1024-bit blocks
- consists of 80 rounds
  - ✓ updating a 512-bit buffer
  - ✓ using a 64-bit value Wt derived from the current message block
  - ✓ and a round constant based on cube root of first 80 prime numbers

SHA-512 Round Function



SHA-512 –Individual Round Function


1024 bits
M_i
W_0 W_1 W_9 W_{14}
W_{tD16} W_{tD15} W_{tD7} W_{tD2}
W_{63} W_{65} W_{71} W_{76}
σ_0
σ_1
XOR
W_0
W_1
¥ ¥ ¥
W_{15}
W_{16}
W_t
W_{79}
64 bits

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (329-340)

Course Teacher

Verified by HOD

LECTURE HANDOUTS

L-36

CSE

III/V

Course Name with Code : Cryptography and Network Security/16CSD09

Course Teacher :

Unit : III - Data Integrity Algorithms and Digital Signatures

Date of Lecture:

Topic of Lecture: Message Authentication Codes(MAC)

Introduction : (Maximum 5 sentences)

- A brute-force attack on a MAC is a more difficult undertaking because it requires known message-MAC pairs.
- To attack a hash code, we can proceed in the following way. Given a fixed message x with n-bit hash code h = H(x), a brute-force method of finding a collision is to pick a random bit string y and check if H(y) = H(x).
- The attacker can do this repeatedly off line

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Hash fuction
- ✓ Cmac
- ✓ Mac
- ✓ SHA

Detailed content of the Lecture:

Message Authentication Codes

A brute-force attack on a MAC is a more difficult undertaking because it requires known message-MAC pairs.. To attack a hash code, we can proceed in the following way. Given a fixed message x with n-bit hash code h = H(x), a brute-force method of finding a collision is to pick a random bit string y and check if H(y) = H(x). The attacker can do this repeatedly off line. To proceed, we need to state the desired security property of a MAC algorithm, which can be expressed as follows:

- Computation resistance: Given one or more text-MAC pairs (x_i, $C_K[x_i]$), it is computationally infeasible to compute any text-MAC pair (x, C_K(x)) for any new input $x \neq x_i$.

In other words, the attacker would like to come up with the valid MAC code for a given message x. There are two lines of attack possible: Attack the key space and attack the MAC value. We examine each of these in turn.

To summarize, the level of effort for brute-force attack on a MAC algorithm can be expressed as min(2^k, 2^n). The assessment of strength is similar to that for symmetric encryption algorithms. It would appear reasonable to require that the key length and MAC length satisfy a relationship such as min(k, n) $\geq$N, where N is perhaps in the range of 128 bits.

Cryptanalysis

As with encryption algorithms, cryptanalytic attacks on hash functions and MAC algorithms seek to exploit some property of the algorithm to perform some attack other than an exhaustive search.

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (348-356)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

L-37

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **III - Data Integrity Algorithms and Digital Signatures**

Date of Lecture:

Topic of Lecture: MAC – Properties

Introduction : (Maximum 5 sentences)

- A brute-force attack on a MAC is a more difficult undertaking because it requires known message-MAC pairs.
- To attack a hash code, we can proceed in the following way. Given a fixed message x with n-bit hash code h = H(x), a brute-force method of finding a collision is to pick a random bit string y and check if H(y) = H(x).
- The attacker can do this repeatedly off line

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Hash fuction
- ✓ Cmac
- ✓ Mac
- ✓ SHA

Detailed content of the Lecture:

Message Authentication Codes

A brute-force attack on a MAC is a more difficult undertaking because it requires known message-MAC pairs.. To attack a hash code, we can proceed in the following way. Given a fixed message x with n-bit hash code h = H(x), a brute-force method of finding a collision is to pick a random bit string y and check if H(y) = H(x). The attacker can do this repeatedly off line. To proceed, we need to state the desired security property of a MAC algorithm, which can be expressed as follows:

Properties of MAC:

- **Establishment of Shared Secret.**
  - It can provide message authentication among pre-decided legitimate users who have shared key.
  - This requires establishment of shared secret prior to use of MAC.

- **Inability to Provide Non-Repudiation**
    - Non-repudiation is the assurance that a message originator cannot deny any previously sent messages and commitments or actions.
    - MAC technique does not provide a non-repudiation service. If the sender and receiver get involved in a dispute over message origination, MACs cannot provide a proof that a message was indeed sent by the sender.
    - Though no third party can compute the MAC, still sender could deny having sent the message and claim that the receiver forged it, as it is impossible to determine which of the two parties computed the MAC.

Both these limitations can be overcome by using the public key based digital signatures discussed in following section.

Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/cryptography/message_authentication.htm

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (348-356)

Course Teacher

Verified by HOD

LECTURE HANDOUTS

L-38

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **III - Data Integrity Algorithms and Digital Signatures**

Date of Lecture:

Topic of Lecture: MAC – Requirements

Introduction : (Maximum 5 sentences)

- A brute-force attack on a MAC is a more difficult undertaking because it requires known message-MAC pairs.
- To attack a hash code, we can proceed in the following way. Given a fixed message x with n-bit hash code h = H(x), a brute-force method of finding a collision is to pick a random bit string y and check if H(y) = H(x).
- The attacker can do this repeatedly off line

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Hash fuction
- ✓ Cmac
- ✓ Mac
- ✓ SHA

Detailed content of the Lecture:

Message Authentication Codes

A brute-force attack on a MAC is a more difficult undertaking because it requires known message-MAC pairs.. To attack a hash code, we can proceed in the following way. Given a fixed message x with n-bit hash code h = H(x), a brute-force method of finding a collision is to pick a random bit string y and check if H(y) = H(x). The attacker can do this repeatedly off line. To proceed, we need to state the desired security property of a MAC algorithm, which can be expressed as follows:

Requirements of MAC:

A MAC, also known as a cryptographic checksum, is generated by a function C of the form.

T = MAC(K, M)

Where M is a variable-length **message**, K is a secret **key** shared only by sender and receiver, and MAC(K, M) is the fixed-length authenticator, sometimes called a tag.

- **Disclosure:** Release of message contents to any person or process not possessing the appropriate cryptographic key.

- **Traffic analysis:** Discovery of the pattern of traffic between parties. ...
- **Masquerade:** Insertion of messages into the network from a fraudulent source.
- **Content modification:** Changes to the contents of a message, including insertion, deletion, transposition, and modification.
- **Sequence modification:** Any modification to a sequence of messages between parties, including insertion, deletion, and reordering.
- **Timing modification:** Delay or replay of messages. In a connection-oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In a connectionless application, an individual message (e.g., datagram) could be delayed or replayed.
- **Source repudiation:** Denial of transmission of message by source.
- **Destination repudiation**: Denial of receipt of message by destination.

Measures to deal with the first two attacks are in the realm of message confidentiality and are dealt with in Part One. Measures to deal with items 3 through 6 in the foregoing list are generally regarded as message authentication. Mechanisms for dealing specifically with item 7 come under the heading of digital signatures. Generally, a digital signature technique will also counter some or all of the attacks listed under items 3 through 6. Dealing with item 8 may require a combination of the use of digital signatures and a protocol designed to counter this attack.

Video Content / Details of website for further learning (if any):
https://flylib.com/books/en/3.190.1.97/1/

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (348-356)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

L-39

Course Name with Code : Cryptography and Network Security/16CSD09

Course Teacher :

Unit : III - Data Integrity Algorithms and Digital Signatures

Date of Lecture:

Topic of Lecture: MACs based on Hash Functions: HMAC

Introduction : (Maximum 5 sentences)

- **HMAC algorithm** stands for Hashed or Hash based Message Authentication Code. It is a result of work done on developing a MAC derived from cryptographic hash functions. HMAC is a great resistant towards cryptanalysis attacks as it uses the Hashing concept twice.
- HMAC consists of twin benefits of Hashing and MAC, and thus is more secure than any other authentication codes. RFC 2104 has issued HMAC, and HMAC has been made compulsory to implement in IP security. The FIPS 198 NIST standard has also issued HMAC.

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Hash fuction
- ✓ Cmac
- ✓ Mac
- ✓ SHA

Detailed content of the Lecture:

HMAC algorithm stands for Hashed or Hash based Message Authentication Code. It is a result of work done on developing a MAC derived from cryptographic hash functions. HMAC is a great resistant towards cryptanalysis attacks as it uses the Hashing concept twice.

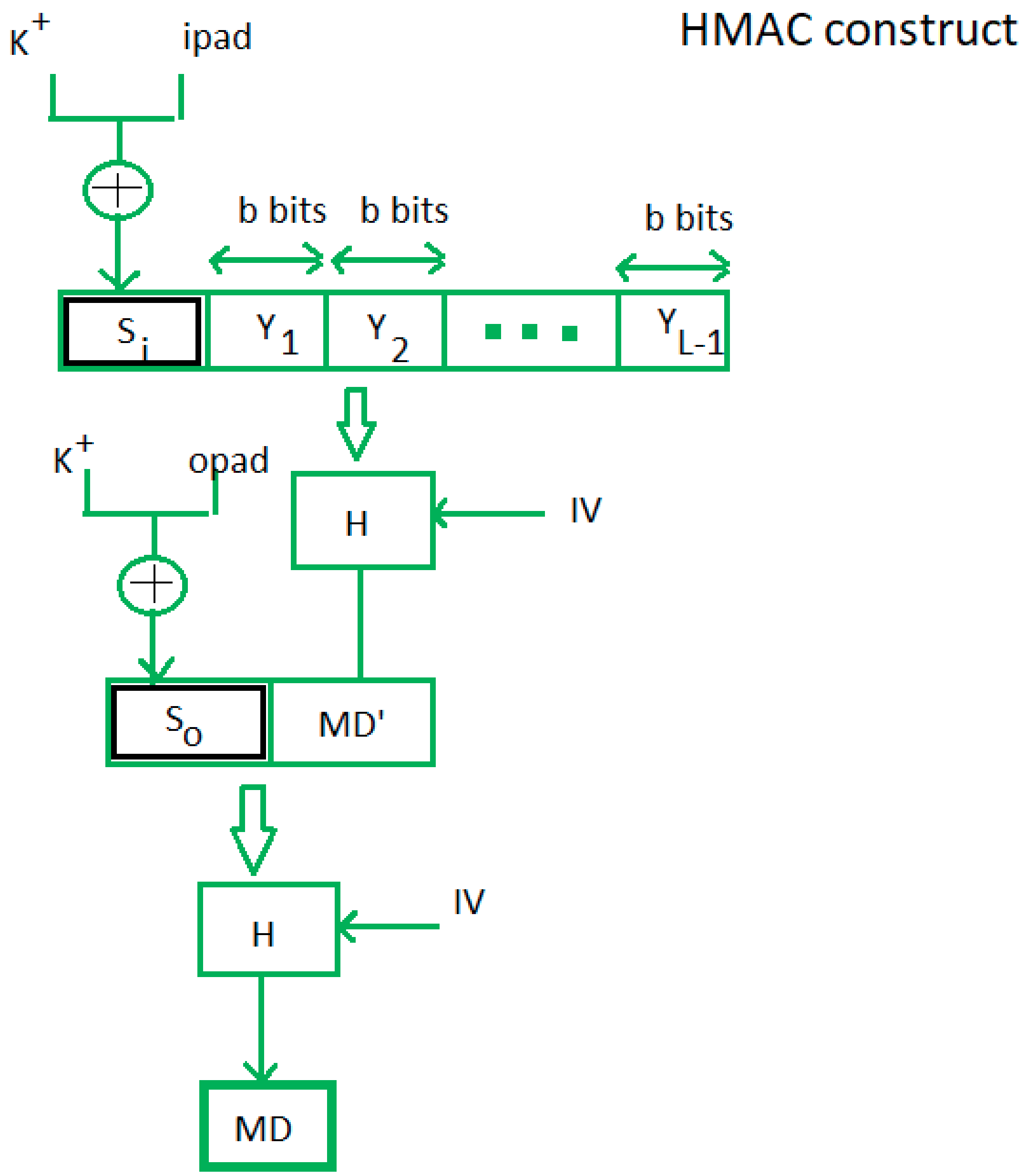
HMAC consists of twin benefits of Hashing and MAC, and thus is more secure than any other authentication codes. RFC 2104 has issued HMAC, and HMAC has been made compulsory to implement in IP security. The FIPS 198 NIST standard has also issued HMAC.

HMAC algorithm

The working of HMAC starts with taking a message M containing blocks of length *b* bits. An input signature is padded to the left of the message and the whole is given as input to a hash function which gives us a temporary message digest MD'.

MD' again is appended to an output signature and the whole is applied a hash function again, the result is our final message digest MD.

Here is a simple structure of HMAC:



Here, H stands for Hashing function,

M is original message

Si and So are input and output signatures respectively,

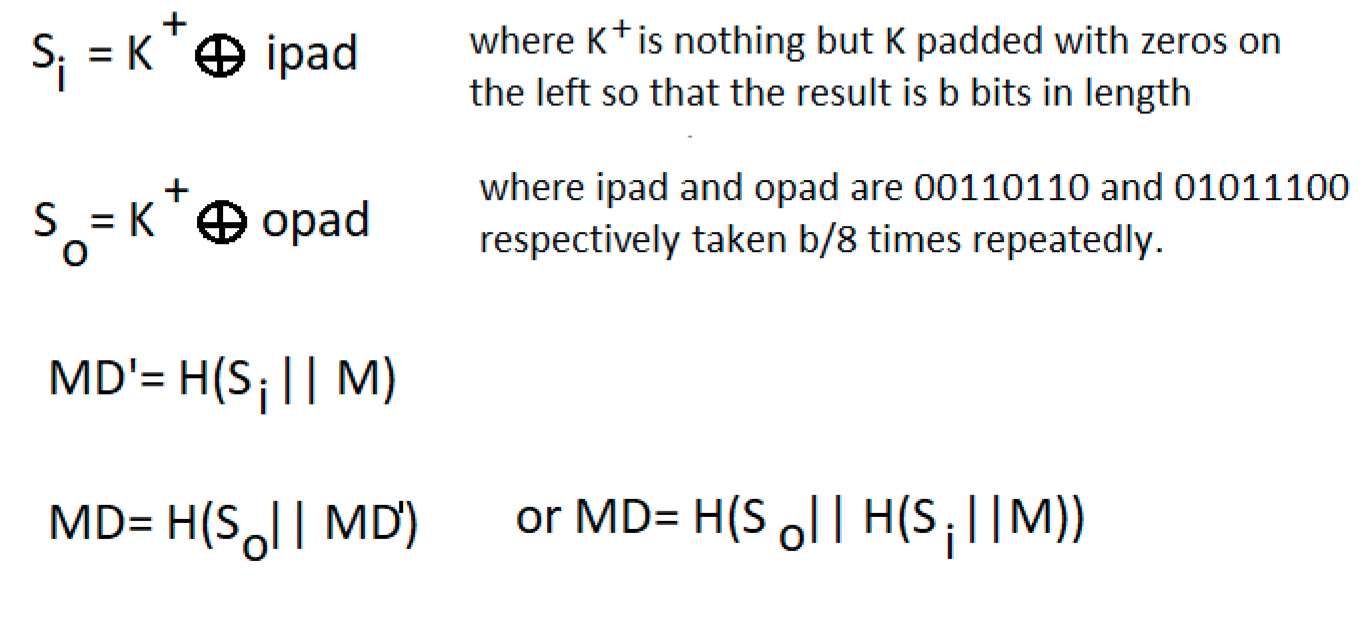
Yi is the ith block in original message M, where i ranges from [1, L)

L = the count of blocks in M

K is the secret key used for hashing

IV is an initial vector (some constant)

The generation of input signature and output signature *Si* and *So* respectively.



$S_i = K^+ \oplus \text{ipad}$ where K^+ is nothing but K padded with zeros on the left so that the result is b bits in length

$S_o = K^+ \oplus \text{opad}$ where ipad and opad are 00110110 and 01011100 respectively taken b/8 times repeatedly.

$MD' = H(S_i \,||\, M)$

$MD = H(S_o \,||\, MD')$ or $MD = H(S_o \,||\, H(S_i \,||\, M))$

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (360-364)

Course Teacher

Verified by HOD

LECTURE HANDOUTS

L-40

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **III - Data Integrity Algorithms and Digital Signatures**

Date of Lecture:

Topic of Lecture: CMAC

Introduction : (Maximum 5 sentences)

- **CMAC** (Cipher-based Message Authentication Code) is a block cipher-based message authentication code algorithm.
- It may be used to provide assurance of the authenticity and, hence, the integrity of binary data. ... The OMAC algorithm reduces the amount of key material required for XCBC.

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Hash fuction
- ✓ Cmac
- ✓ Mac
- ✓ SHA

Detailed content of the Lecture:

CMAC (Cipher-based Message Authentication Code) is a block cipher-based message authentication code algorithm. It may be used to provide assurance of the authenticity and, hence, the integrity of binary data. ... The OMAC algorithm reduces the amount of key material required for XCBC

- The Data Authentication Algorithm defined in FIPS PUB 113, also known as the CBC-MAC (cipher block chaining message authentication code), is described in Chapter 11. This cipher-based MAC has been widely adopted in government and industry.
- [BELL00] demonstrated that this MAC is secure under a reasonable set of security criteria, with the following restriction. Only messages of one fixed length of mn bits are processed, where n is the cipher block size and m is a fixed positive integer.
- As a simple example, notice that given the CBC MAC of a one-block message X, say T = MAC(K, X), the adversary immediately knows the CBC MAC for the two-block message X||(X ⊕ T.

Black and Rogaway demonstrated that this limitation could be overcome using three keys: one key of length k to be used at each step of the cipher block chaining and two keys of length n, where k is the key length and n is the cipher block length.

- This proposed construction was refined by Iwata and Kurosawa so that the two n-bit keys could be derived from the encryption key, rather than being provided separately .
- This refinement has been adopted by NIST cipher-based message authentication code (CMAC) mode of operation, for use with AES and triple DES. It is specified in NIST Special Publication

800-38B.

First, let us consider the operation of CMAC when the message is an integer multiple n of the cipher block length b. For AES, b = 128 and for triple DES, b = 64. The message is divided into n blocks, M_1, M_2,...,M_n. The algorithm makes use of a k-bit encryption key K and an n-bit constant K_1. For AES, the key size k is 128, 192, or 256 bits; for triple DES, the key size is 112 or 168 bits.

C= E(K,M_1)

1

C= E(K,[M_2 ⊕ =

2 E(K,[M_3

C_3 ⊕

.

.

.

C= =

n E(K,[M_n ⊕ n1 MSB$_{Tlen}$(C

⊕ n)

T

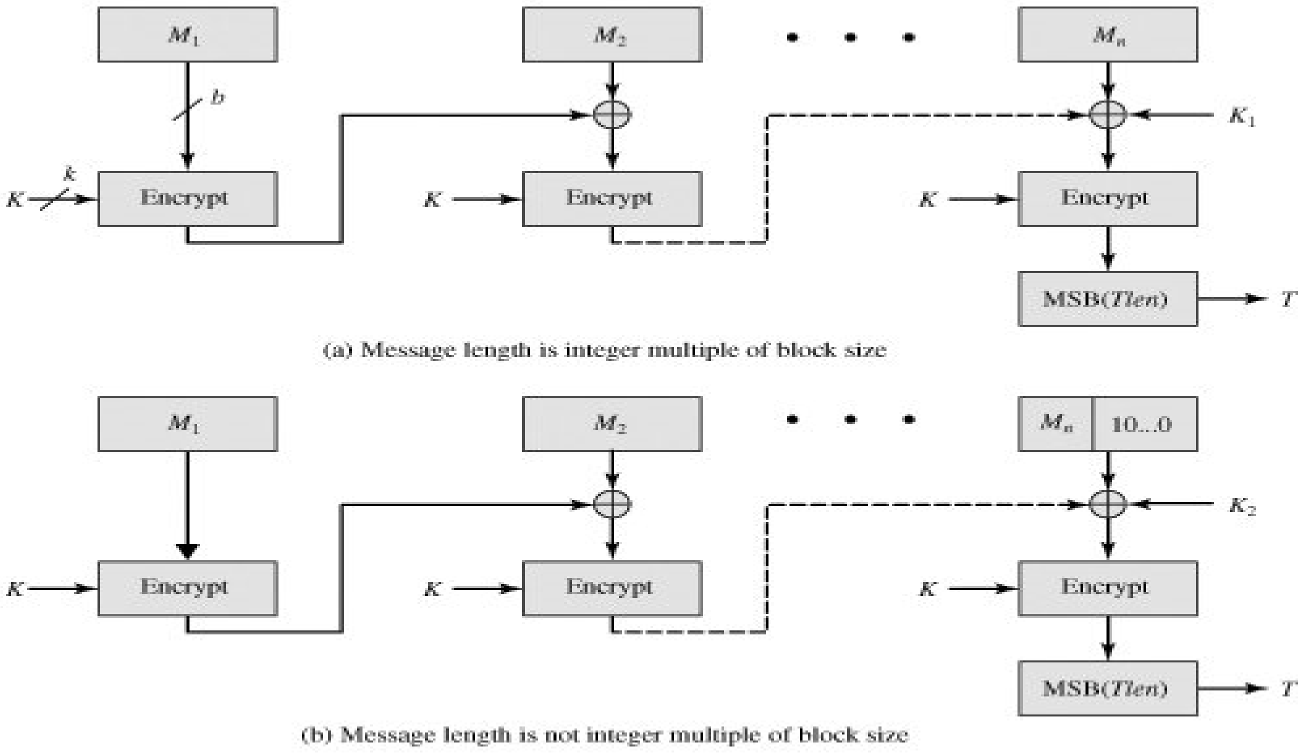
Where

T = message authentication code, also referred to as the tag

Tlen = bit length of T

MSB$_s$(X) = the s leftmost bits of the bit string X

Figure 12.12. Cipher-Based Message Authentication Code (CMAC)



(a) Message length is integer multiple of block size

(b) Message length is not integer multiple of block size

If the message is not an integer multiple of the cipher block length, then the final block is padded to the right (least significant bits) with a 1 and as many 0s as necessary so that the final block is also of length b. The CMAC operation then proceeds as before, except that a different n-bit key K_2 is used instead of K_1.

The two n-bit keys are derived from the k-bit encryption key as follows:

$L = E(K, 0^n)$
$K_1 = L \cdot x$
$K_2 = L \cdot x^2 =$
$(L \cdot x) \cdot x$

where multiplication (·) is done in the finite field (2^n) and x and x^2 are first and second order polynomials that are elements of $GF(2^n)$ Thus the binary representation of x consists of n - 2 zeros followed by 10; the binary representation of x^2 consists of n - 3 zeros followed by 100.

The finite field is defined with respect to an irreducible polynomial that is lexicographically first among all such polynomials with the minimum possible number of nonzero terms. For the two approved block sizes, the polynomials are and $x^{64} + x^4 + x^3 + x + 1$ and $x^{128} + x^7 + x^2 + x + 1$.

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014 Page No: (365-367)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

DESIGNING YOUR FUTURE
Estd. 2000

IQAC

LECTURE HANDOUTS

L-41

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **III - Data Integrity Algorithms and Digital Signatures**

Date of Lecture:

Topic of Lecture: MD5

Introduction : (Maximum 5 sentences)

- The hash algorithm **MD5** is widely used to check the integrity of messages.
- **MD5** divides the message into blocks of 512 bits and creates a 128 bit digest(typically, 32 Hexadecimal digits).

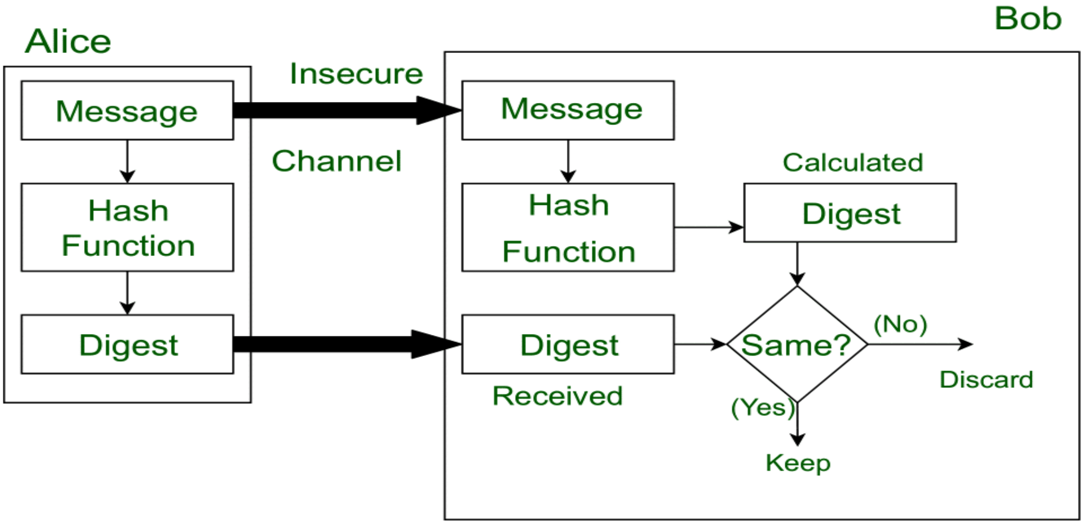
Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Hash function
- ✓ Cmac
- ✓ Mac
- ✓ SHA

Detailed content of the Lecture:

The hash algorithm **MD5** is widely used to check the integrity of messages. **MD5** divides the message into blocks of 512 bits and creates a 128 bit digest(typically, 32 Hexadecimal digits). ... In response to the insecurities of **MD5** hash algorithms, the **Secure** Hash Algorithm (SHA) was invented.

- **Message Digest** is used to ensure the integrity of a message transmitted over an insecure channel (where the content of the message can be changed).
- The message is passed through a Cryptographic hash function. This function creates a compressed image of the message called **Digest**.
- Lets assume, Alice sent a message and digest pair to Bob. To check the integrity of the message Bob runs the cryptographic hash function on the received message and gets a new digest.
- Now, Bob will compare the new digest and the digest sent by Alice. If, both are same then Bob is sure that the original message is not changed.



- Most importantly, the digest should be unchanged during the transmission.
- The cryptographic hash function is a one way function, that is, a function which is practically infeasible to invert. This cryptographic hash function takes a message of variable length as input and creates a **digest / hash / fingerprint** of fixed length, which is used to verify the integrity of the message.
- Message digest ensures the integrity of the document. To provide authenticity of the message, digest is encrypted with sender's private key. Now this digest is called digital signature, which can be only decrypted by the receiver who has sender's public key. Now the receiver can authenticate the sender and also verify the integrity of the sent message.

Message digest algorithm characteristics

Message digests, also known as hash functions, are one-way functions; they accept a message of any size as input, and produce as output a fixed-length message digest. MD5 is the third message digest algorithm created by Rivest. All three (the others are MD2 and MD4) have similar structures, but MD2 was optimized for 8-bit machines, in comparison with the two later formulas, which are optimized for 32-bit machines. The MD5 algorithm is an extension of MD4, which the critical review found to be fast, but possibly not absolutely secure. In comparison, MD5 is not quite as fast as the MD4 algorithm, but offered much more assurance of data security.
Video Content / Details of website for further learning (if any): WilliamStallings.com/Crypto/Crypto4e.html
Important Books/Journals for further learning including the page nos.: **Book:** Web reference

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

DESIGNING YOUR FUTURE
Estd. 2000

IQAC

LECTURE HANDOUTS

L-42

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **III - Data Integrity Algorithms and Digital Signatures**

Date of Lecture:

Topic of Lecture: MD4 VS MD5
Introduction : (Maximum 5 sentences) • The significant differences between **MD4** and **MD5** are the following: **MD5** has four rounds, whereas **MD4** has only three. . • The hash algorithm **MD5** is widely used to check the integrity of messages. • **MD5** divides the message into blocks of 512 bits and creates a 128 bit digest(typically, 32 Hexadecimal digits).

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Hash function
- ✓ Cmac
- ✓ Mac
- ✓ SHA

Detailed content of the Lecture:

The hash algorithm **MD5** is widely used to check the integrity of messages. **MD5** divides the message into blocks of 512 bits and creates a 128 bit digest(typically, 32 Hexadecimal digits). ... In response to the insecurities of **MD5** hash algorithms, the **Secure** Hash Algorithm (SHA) was invented.

The significant differences between **MD4** and **MD5** are the following: **MD5** has four rounds, whereas **MD4** has only three. ...

Each step of **MD5** has a unique additive constant, T[i], whereas each round of **MD4** uses a fixed constant. The function G in the second round of **MD5** is less symmetric than the G function in **MD4**.

MD4 and MD5 are the initial members of the **MD4** type hash functions. They take variable length input messages and hash them to fixed-length outputs.

Both operate on 512-bit message blocks divided into 32-bit words and produce a message digest of 128 bits.

The following are the differences between MD4 and MD5:

1. A fourth round has been added.
2. Each step now has a unique additive constant.
3. The function g in round 2 was changed from (XY v XZ v YZ) to (XZ v Y not(Z)) to make g less symmetric.
4. Each step now adds in the result of the previous step. This promotes a faster "avalanche effect".
5. The order in which input words are accessed in rounds 2 and 3 is changed, to make these patterns less like each other.
6. The shift amounts in each round have been approximately optimized, to yield a faster "avalanche effect." The shifts in different rounds are distinct.

Video Content / Details of website for further learning (if any):
https://www.freesoft.org/CIE/RFC/1321/10.htm

Important Books/Journals for further learning including the page nos.:
Book: Web reference

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

L-43

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **III - Data Integrity Algorithms and Digital Signatures**

Date of Lecture:

Topic of Lecture: Digital signatures-Digital signature Standard(DSS)

Introduction : (Maximum 5 sentences)

- have looked at message authentication- but does not address issues of lack of trust
- digital signatures provide the ability to:
  - ✓ verify author, date & time of signature
  - ✓ authenticate message contents
  - ✓ be verified by third parties to resolve disputes

- hence include authentication function with additional capabilities

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Hash fuction
- ✓ Cmac
- ✓ Mac
- ✓ SHA

Detailed content of the Lecture:

DIGITAL SIGNATURES

- have looked at message authentication- but does not address issues of lack of trust
- digital signatures provide the ability to:
  - ✓ verify author, date & time of signature
  - ✓ authenticate message contents
  - ✓ be verified by third parties to resolve disputes
- hence include authentication function with additional capabilities

DIRECT DIGITAL SIGNATURES

- involve only sender & receiver
- assumed receiver has sender‟s public-key
- digital signature made by sender signing entire message or hash with private-key
- can encrypt using receivers public-key
- important that sign first then encrypt message & signature
- security depends on sender‟s private-key

Arbitrated Digital Signatures

- involves use of arbiter A
  - ✓ validates any signed message then dated and sent to recipient
- requires suitable level of trust in arbiter
- can be implemented with either private or public-key algorithms
- arbiter may or may not see message

Authentication Protocols

- used to convince parties of each others identity and to exchange session keys
- may be one-way or mutual
- key issues are
  - ✓ confidentiality – to protect session keys
  - ✓ timeliness – to prevent replay attacks
- published protocols are often found to have flaws and need to be modified

Replay Attacks

- where a valid signed message is copied and later resent

- ✓ simple replay
- ✓ repetition that can be logged
- ✓ repetition that cannot be detected
- ✓ backward replay without modification

- countermeasures include
  - ✓ use of sequence numbers (generally impractical)
  - ✓ timestamps (needs synchronized clocks)
  - ✓ challenge/response (using unique nonce)

Using Symmetric Encryption

- as discussed previously can use a twolevel hierarchy of keys
- usually with a trusted Key Distribution Center (KDC)
  - ✓ each party shares own master key with KDC
  - ✓ KDC generates session keys used for connections between parties
  - ✓ master keys used to distribute these to them
- can refine use of KDC but can"t have final exchange of nonces, vis:
  - ✓ A->KDC: IDA || IDB || N1
  - ✓ KDC -> A: EKa [Ks || IDB || N1 || EKb [Ks||IDA]]
  - ✓ A -> B: EKb [Ks||IDA] || EKs [M]
- does not protect against replays
  - ✓ could rely on timestamp in message, though email delays make this problematic

Using Public-Key Encryption

- have a range of approaches based on the use of public-key encryption
- need to ensure have correct public keys for other parties
- using a central Authentication Server (AS)
- various protocols exist using timestamps or nonces
- if confidentiality is major concern, can use:

  A->B: EPUb [Ks] || EKs [M]
  - ✓ has encrypted session key, encrypted message
- if authentication needed use a digital signature with a digital

  certificate: A->B: M || EPRa [H(M)] || EPRas
  [T||IDA||PUa]
  - ✓ with message, signature, certificate

DIGITAL SIGNATURE STANDARD (DSS)

- US Govt approved signature scheme
- designed by NIST & NSA in early 90's
- published as FIPS-186 in 1991
- revised in 1993, 1996 & then 2000

- uses the SHA hash algorithm
- DSS is the standard, DSA is the algorithm
- FIPS 186-2 (2000) includes alternative RSA & elliptic curve signature variants

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (389-392),(395-398)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

DESIGNING YOUR FUTURE
Estd. 2000

LECTURE HANDOUTS

L-44

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **III - Data Integrity Algorithms and Digital Signatures**

Date of Lecture:

Topic of Lecture: Digital signatures Algorithms

Introduction : (Maximum 5 sentences)

- have looked at message authentication- but does not address issues of lack of trust
- digital signatures provide the ability to:
  - ✓ verify author, date & time of signature
  - ✓ authenticate message contents

- ✓ be verified by third parties to resolve disputes
- hence include authentication function with additional capabilities

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Hash fuction
- ✓ Cmac
- ✓ Mac
- ✓ SHA

Detailed content of the Lecture:

DIGITAL SIGNATURES

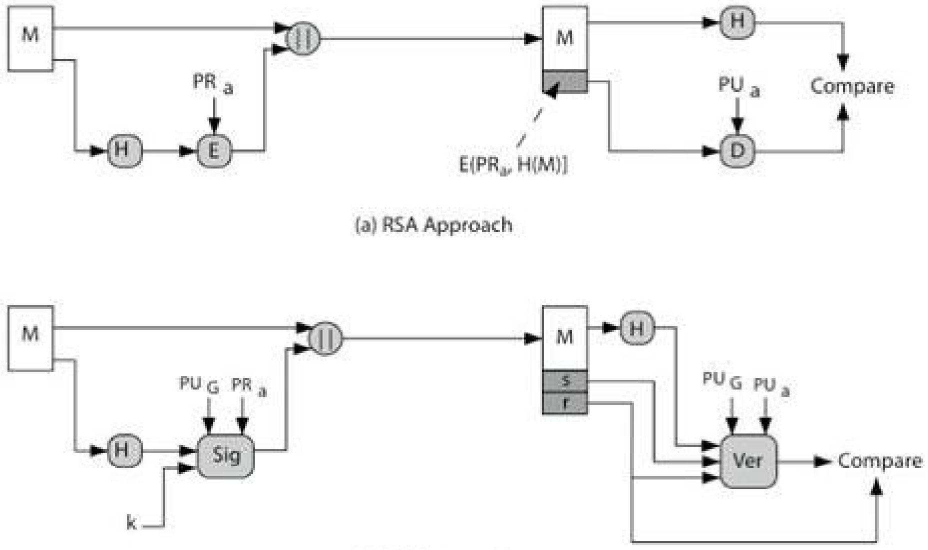
- have looked at message authentication- but does not address issues of lack of trust
- digital signatures provide the ability to:
  - ✓ verify author, date & time of signature
  - ✓ authenticate message contents
  - ✓ be verified by third parties to resolve disputes
- hence include authentication function with additional capabilities

Digital Signature Properties

- must depend on the message signed
- must use information unique to sender-to prevent both forgery and denial
- must be relatively easy to produce
- must be relatively easy to recognize & verify
- be computationally infeasible to forge
  - ✓ with new message for existing digital signature
  - ✓ with fraudulent digital signature for given message
- be practical save digital signature in storage

DIGITAL SIGNATURE ALGORITHM (DSA)

- creates a 320 bit signature
- with 512-1024 bit security
- smaller and faster than RSA
- a digital signature scheme only
- security depends on difficulty of computing discrete logarithms
- variant of ElGamal & Schnorr schemes



(a) RSA Approach

(b) DSS Approach

DSA Key Generation

- have shared global public key values (p,q,g):
- choose q, a 160 bit
- choose a large prime p = 2L
  - ✓ where L= 512 to 1024 bits and is a multiple of 64 and q is a prime factor of (p-1)
- choose g = h(p-1)/q
  - ✓ where h<p-1, h(pp-11)//q (mod p) > 1
- users choose private & compute public key:
  - ✓ choose x<q
  - ✓ compute y = gx (mod p)

DSA Signature Creation

- to sign a message M the sender:
  - ✓ generates a random signature key k, k<q
  - ✓ nb. k must be random, be destroyed after use, and never be reused
- then computes signature pair:

  r = (gk(mod p))(mod q)

  s = (k-1.H(M)+ x.r)(mod q)
- sends signature (r,s) with message M

  DSA Signature Verification
- having received M & signature (r,s)
- to verify a signature, recipient

  computes: w = s-1(mod q)

  u1= (H(M).w)(mod q)

  u2= (r.w)(mod q)

  v = (gu1.yu2(mod p)) (mod q)
- if v=r then signature is verified

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (389-392),(395-398)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L-45

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **III - Data Integrity Algorithms and Digital Signatures**

Date of Lecture:

Topic of Lecture: Digital signature-Example

Introduction : (Maximum 5 sentences)

- have looked at message authentication- but does not address issues of lack of trust
- digital signatures provide the ability to:
  - ✓ verify author, date & time of signature
  - ✓ authenticate message contents
  - ✓ be verified by third parties to resolve disputes
- hence include authentication function with additional capabilities

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Hash fuction
- ✓ Cmac
- ✓ Mac
- ✓ SHA

Detailed content of the Lecture:

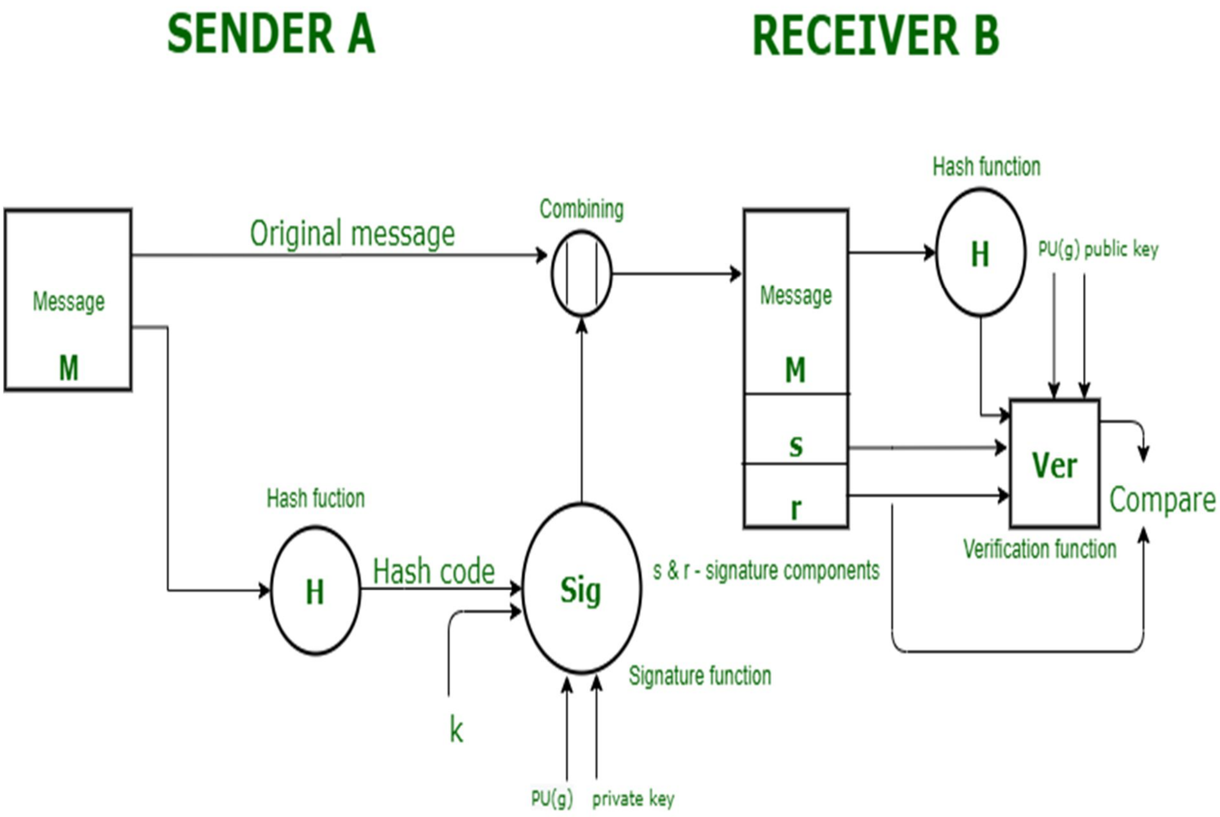
DIGITAL SIGNATURES

- have looked at message authentication- but does not address issues of lack of trust
- digital signatures provide the ability to:
  - ✓ verify author, date & time of signature
  - ✓ authenticate message contents
  - ✓ be verified by third parties to resolve disputes
- hence include authentication function with additional capabilities

Digital Signature Properties

- must depend on the message signed
- must use information unique to sender-to prevent both forgery and denial
- must be relatively easy to produce
- must be relatively easy to recognize & verify
- be computationally infeasible to forge
  - ✓ with new message for existing digital signature
  - ✓ with fraudulent digital signature for given message

- be practical save digital signature in storage



Sender Side :

In DSS Approach, a hash code is generated out of the message and following inputs are given to the signature function –

1. The hash code.
2. The random number 'k' generated for that particular signature.
3. The private key of the sender i.e., PR(a).
4. A global public key(which is a set of parameters for the communicating principles) i.e., PU(g).

These input to the function will provide us with the output signature containing two components – 's' and 'r'. Therefore, the original message concatenated with the signature is sent to the receiver.

Receiver Side :

At the receiver end, verification of the sender is done. The hash code of the sent message is generated. There is a verification function which takes the following inputs –

1. The hash code generated by the receiver.
2. Signature components 's' and 'r'.
3. Public key of the sender.
4. Global public key.

The output of the verification function is compared with the signature component 'r'. Both the values will

match if the sent signature is valid because only the sender with the help of it private key can generate a valid signature.
Video Content / Details of website for further learning (if any): https://www.geeksforgeeks.org/digital-signature-standard-dss/
Important Books/Journals for further learning including the page nos.: **Book:** William Stallings, Cryptography and Network Security, Prentice Hall, 2014 Page No: (389-392),(395-398)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L-46

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **IV - Authentication, Email & Web Security**

Date of Lecture:

Topic of Lecture: Authentication applications

Introduction : (Maximum 5 sentences)

- An alternative is to use an authentication server (AS) that knows the passwords of all users and stores these in a centralized database.
- In addition, the AS shares a unique secret key with each server.

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- Kerberos
- X.509

Detailed content of the Lecture:

A Simple Authentication Dialogue

In an unprotected network environment, any client can apply to any server for service. The obvious security risk is that of impersonation. To counter this threat, servers must be able to confirm the identities of clients who request service. But in an open environment, this places a substantial burden on each server.

An alternative is to use an authentication server (AS) that knows the passwords of all users and stores these in a centralized database. In addition, the AS shares a unique secret key with each server.

The simple authentication dialogue is as follows:

- C >> AS: IDc||Pc||IDv
- AS >> C: Ticket
- C >> V: IDc||Ticket

Ticket= EKv(IDc||ADc||IDv)

C: Client,

AS: Authentication Server, V: Server,

IDv : ID of the server, IDc : ID of the client,

Pc:Password of the client, ADc: Address of

client, Kv: secret key shared by AS and V, ||:

concatenation.

A More Secure Authentication Dialogue

There are two major problems associated with the previous approach:

- Plaintext transmission of the password.
- Each time a user has to enter the password.

To solve these problems, we introduce a scheme for avoiding plaintext passwords, and anew server, known as ticket granting server (TGS). The hypothetical scenario is as follows: **Once per user logon session:**

- C >> AS: IDc||IDtgs
- AS >> C: Ek_c ($Ticket_{tgs}$)

Once per type of service:

- C >> TGS: IDc||IDv||$Ticket_{tgs}$
- TGS >> C: $ticket_v$

Once per service session:

5. C >> V: IDc||$ticket_v$

$Ticket_{tgs}$= Ek_{tgs}(IDc||ADc||IDtgs||TS1||Lifetime1) $Ticket_v$= Ek_v(IDc||ADc||IDv||TS2||Lifetime2)

C: Client, AS: Authentication Server, V: Server, IDc : ID of the client, Pc:Password of the client, ADc: Address of client, IDv : ID of the server, Kv: secret key shared by AS and V, ||: concatenation, IDtgs: ID of the TGS server, TS1, TS2: time stamps, lifetime: lifetime of the ticket.

- The new service, TGS, issues tickets to users who have been authenticated to AS. Thus, the user first requests a ticket-granting ticket ($Ticket_{tgs}$) from the AS.
- The client module in the user workstation saves this ticket. Each time the user requires access to a new service, the client applies to the TGS, using the ticket to authenticate itself. The TGS then grants a ticket for the particular service.
- The client saves each service-granting ticket and uses it to authenticate its user to a server each time a particular service is requested. Let us look at the details of this scheme:
- The client requests a ticket-granting ticket on behalf of the user by sending its user's ID and password to the AS, together with the TGS ID, indicating a request to use the TGS service.
- The AS responds with a ticket that is encrypted with a key that is derived from the user's password.

When this response arrives at the client, the client prompts the user for his or her password, generates the key, and attempts to decrypt the incoming message.

- If the correct password is supplied, the ticket is successfully recovered.
- Because only the correct user should know the password, only the correct user can recover the ticket. Thus, we have used the password to obtain credentials from Kerberos without having to transmit the password in plaintext.

Now that the client has a ticket-granting ticket, access to any server can be obtained with steps 3 and 4:

- The client requests a service-granting ticket on behalf of the user. For this purpose, the client transmits a message to the TGS containing the user's ID, the ID of the desired service, and the ticket-granting ticket.
- The TGS decrypts the incoming ticket and verifies the success of the decryption by the presence of its ID. It checks to make sure that the lifetime has not expired.
- Then it compares the user ID and network address with the incoming information to authenticate the user. If the user is permitted access to the server V, the TGS issues a ticket to grant access to the requested service.

The service-granting ticket has the same structure as the ticket-granting ticket. Indeed, because the TGS is a server, we would expect that the same elements are needed to authenticate a client to the TGS and to authenticate a client to an application server. Again, the ticket contains a timestamp and lifetime. If the user wants access to the same service at a later time, the client can simply use the previously acquired service-granting ticket and need not bother the user for a password. Note that the ticket is encrypted with a secret key (K_V) known only to the TGS and the server, preventing alteration.

Finally, with a particular service-granting ticket, the client can gain access to the corresponding service with step 5:

e) The client requests access to a service on behalf of the user. For this purpose, the client transmits a message to the server containing the user's ID and the service-granting ticket. The server authenticates by using the contents of the ticket.

This new scenario satisfies the two requirements of only one password query per user session and protection of the user password.

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html.

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (447-450),(454-471)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS **L-47**

CSE **III/V**

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **IV - Authentication, Email & Web Security**

Date of Lecture:

Topic of Lecture: Kerberos Version 4

Introduction : (Maximum 5 sentences)

- Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users.
- Kerberos relies exclusively on conventional encryption, making no use of public-key encryption.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Kerberos
- X.509

Detailed content of the Lecture:

KERBEROS

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. Kerberos relies exclusively on conventional encryption, making no use of public-key encryption.

The following are the requirements for Kerberos:

- **Secure:** A network eavesdropper should not be able to obtain the necessary information to impersonate a user. More generally, Kerberos should be strong enough that a potential opponent does not find it to be the weak link.
- **Reliable:** For all services that rely on Kerberos for access control, lack of availability of the Kerberos service means lack of availability of the supported services. Hence, Kerberos should be highly reliable and should employ a distributed server architecture, with one system able to back up another.
- **Transparent:** Ideally, the user should not be aware that authentication is taking place, beyond the requirement to enter a password.
- **Scalable:** The system should be capable of supporting large numbers of clients and servers. This suggests a modular, distributed architecture.

Kerbero V4 Authentication Dialogue Message Exchange

Two additional problems remain in the more secure authentication dialogue:

- Lifetime associated with the ticket granting ticket. If the lifetime is very short, then the user will be repeatedly asked for a password. If the lifetime is long, then the opponent has the greater opportunity for replay.
- Requirement for the servers to authenticate themselves to users.

The actual Kerberos protocol version 4 is as follows :

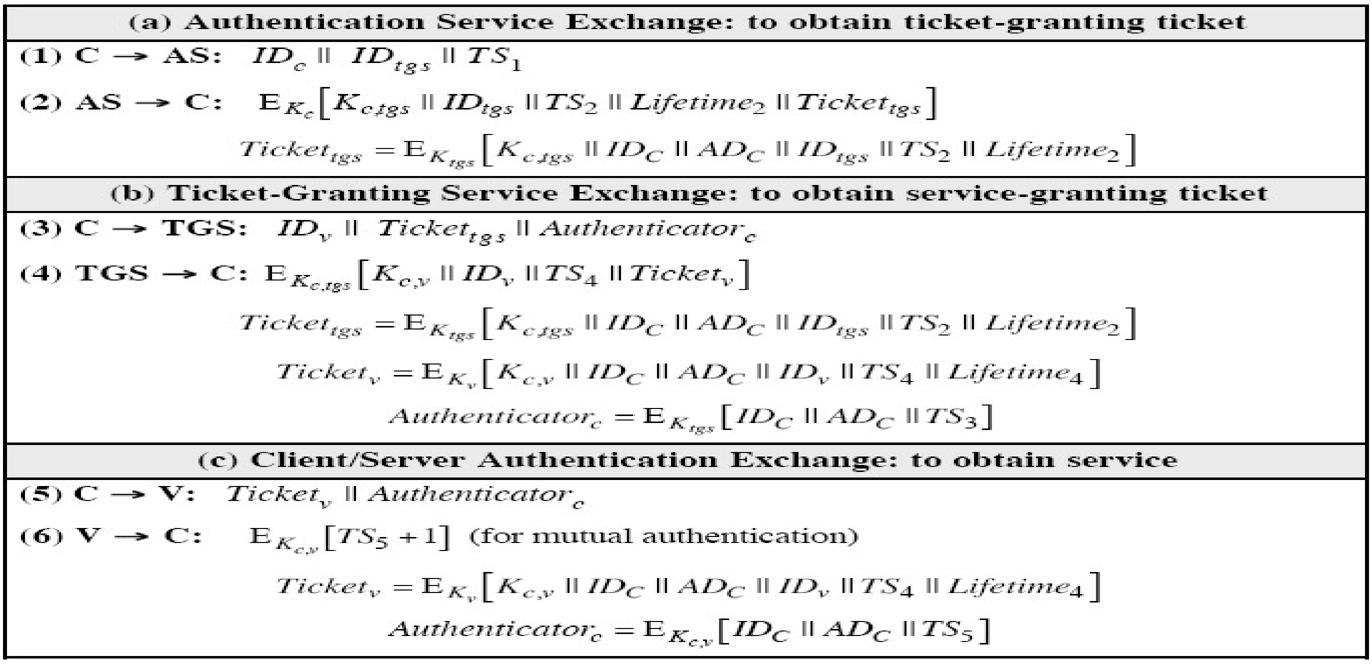
a basic third-party authentication scheme

have an Authentication Server (AS)

- users initially negotiate with AS to identify self
- AS provides a non-corruptible authentication credential (ticket granting ticket TGT)

have a Ticket Granting server (TGS)

- users subsequently request access to other services from TGS on basis of users TGT



(a) Authentication Service Exchange: to obtain ticket-granting ticket

(1) C → AS: $ID_c \parallel ID_{tgs} \parallel TS_1$

(2) AS → C: $\mathrm{E}_{K_c}[K_{c,tgs} \parallel ID_{tgs} \parallel TS_2 \parallel Lifetime_2 \parallel Ticket_{tgs}]$

$$Ticket_{tgs} = \mathrm{E}_{K_{tgs}}[K_{c,tgs} \parallel ID_C \parallel AD_C \parallel ID_{tgs} \parallel TS_2 \parallel Lifetime_2]$$

(b) Ticket-Granting Service Exchange: to obtain service-granting ticket

(3) C → TGS: $ID_v \parallel Ticket_{tgs} \parallel Authenticator_c$

(4) TGS → C: $\mathrm{E}_{K_{c,tgs}}[K_{c,v} \parallel ID_v \parallel TS_4 \parallel Ticket_v]$

$$Ticket_{tgs} = \mathrm{E}_{K_{tgs}}[K_{c,tgs} \parallel ID_C \parallel AD_C \parallel ID_{tgs} \parallel TS_2 \parallel Lifetime_2]$$

$$Ticket_v = \mathrm{E}_{K_v}[K_{c,v} \parallel ID_C \parallel AD_C \parallel ID_v \parallel TS_4 \parallel Lifetime_4]$$

$$Authenticator_c = \mathrm{E}_{K_{tgs}}[ID_C \parallel AD_C \parallel TS_3]$$

(c) Client/Server Authentication Exchange: to obtain service

(5) C → V: $Ticket_v \parallel Authenticator_c$

(6) V → C: $\mathrm{E}_{K_{c,v}}[TS_5 + 1]$ (for mutual authentication)

$$Ticket_v = \mathrm{E}_{K_v}[K_{c,v} \parallel ID_C \parallel AD_C \parallel ID_v \parallel TS_4 \parallel Lifetime_4]$$

$$Authenticator_c = \mathrm{E}_{K_{c,v}}[ID_C \parallel AD_C \parallel TS_5]$$

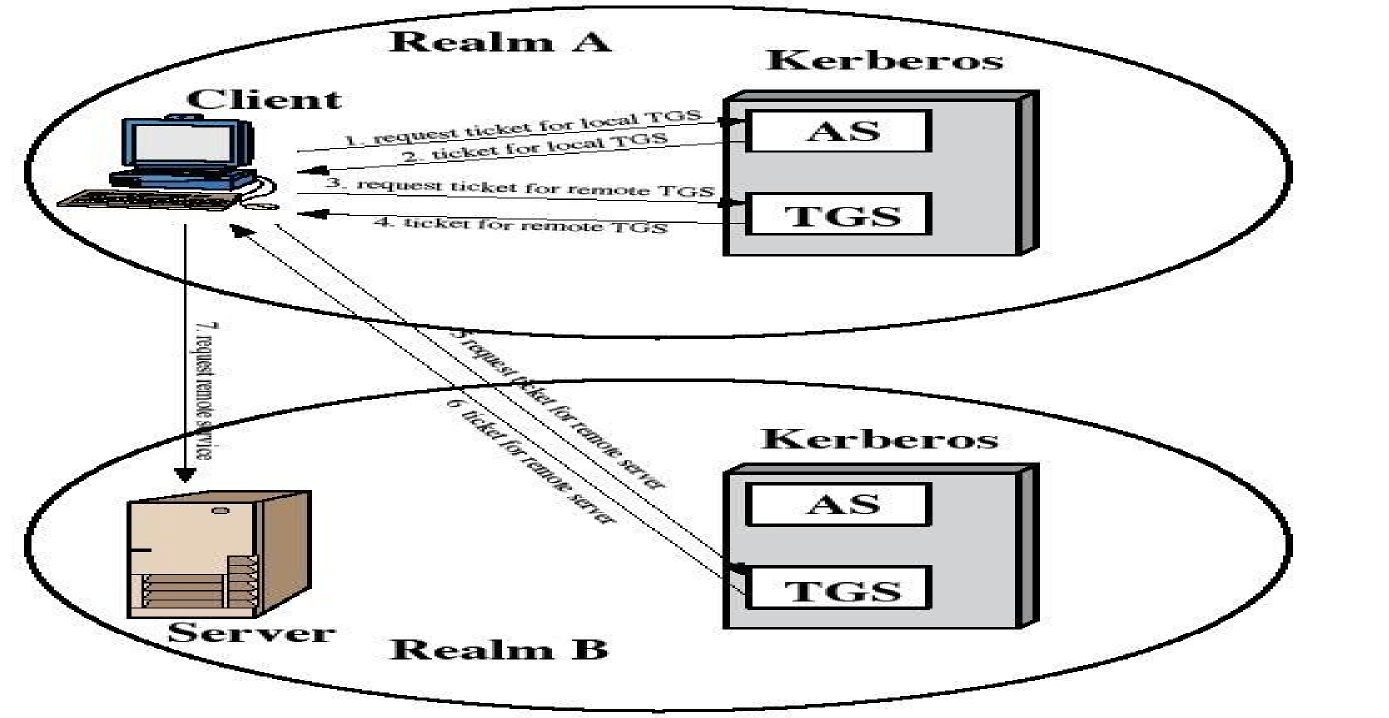
Kerberos Realms and Multiple Kerberi

A full-service Kerberos environment consisting of a Kerberos server, a number of clients, and a number of application servers requires the following:

- The Kerberos server must have the user ID and hashed passwords of all participating users in its database. All users are registered with the Kerberos server.
- The Kerberos server must share a secret key with each server. All servers are registered with the Kerberos server.

Such an environment is referred to as a Kerberos realm.

The concept of realm can be explained as follows.



Realm A
Kerberos
Client
AS
TGS
1. request ticket for local TGS
2. ticket for local TGS
3. request ticket for remote TGS
4. ticket for remote TGS
7. request remote service
5 request ticket for remote server
6 ticket for remote server
Kerberos
AS
TGS
Server
Realm B

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html.

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (447-450),(454-471)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

L-48

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **IV - Authentication, Email & Web Security**

Date of Lecture:

Topic of Lecture: Kerberos -X.509

Introduction : (Maximum 5 sentences)

- Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users.
- Kerberos relies exclusively on conventional encryption, making no use of public-key encryption.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Kerberos
- X.509

Detailed content of the Lecture:

KERBEROS

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. Kerberos relies exclusively on conventional encryption, making no use of public-key encryption.

The following are the requirements for Kerberos:

- **Secure:** A network eavesdropper should not be able to obtain the necessary information to impersonate a user. More generally, Kerberos should be strong enough that a potential opponent does not find it to be the weak link.
- **Reliable:** For all services that rely on Kerberos for access control, lack of availability of the Kerberos service means lack of availability of the supported services. Hence, Kerberos should be highly reliable and should employ a distributed server architecture, with one system able to back up another.
- **Transparent:** Ideally, the user should not be aware that authentication is taking place, beyond the requirement to enter a password.
- **Scalable:** The system should be capable of supporting large numbers of clients and servers. This suggests a modular, distributed architecture.

To support these requirements, the overall scheme of Kerberos is that of a trusted third- party authentication service that uses a protocol based on that proposed by Needham and Schroeder [NEED78] It is trusted in the sense that clients and servers trust Kerberos to mediate their mutual authentication. Assuming the Kerberos protocol is well designed, then the authentication service is secure if the Kerberos server itself is secure.

X.509 Certificates

Overview:

- issued by a Certification Authority (CA), containing:
  - version (1, 2, or 3)
  - serial number (unique within CA) identifying certificate
  - signature algorithm identifier
  - issuer X.500 name (CA)
  - period of validity (from - to dates)
  - subject X.500 name (name of owner)
  - subject public-key info (algorithm, parameters, key)
  - issuer unique identifier (v2+)
  - subject unique identifier (v2+)
  - extension fields (v3)
  - signature (of hash of all fields in certificate)
- notation CA<<A>> denotes certificate for A signed by CA

X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. The directory may serve as a repository of public-key certificates. Each certificate contains the public key of a user and is signed with the private key of a trusted certification authority. In addition, X.509 defines alternative authentication protocols based on the use of public-key certificates.

Signature algorithm identifier:

The algorithm used to sign the certificate, together with any associated parameters. Because this information is repeated in the Signature field at the end of the certificate, this field has little, if any, utility.

Issuer name:
X.500 name of the CA that created and signed this certificate.

Period of validity:
Consists of two dates: the first and last on which the certificate is valid.

name:
The name of the user to whom this certificate refers. That is, this certificate certifies the public key of the subject who holds the corresponding private key.

Subject's public-key information:
The public key of the subject, plus an identifier of the algorithm for which this key is to be used, together with any associated parameters.

Issuer unique identifier:
An optional bit string field used to identify uniquely the issuing CA in the event the X.500 name has been reused for different entities.

Subject unique identifier:
An optional bit string field used to identify uniquely the subject in the event the X.500 name has been reused for different entities.

Extensions:

A set of one or more extension fields. Extensions were added in version 3 and are discussed later in this section.

Signature:

Covers all of the other fields of the certificate; it contains the hash code of the other fields, encrypted with the CA's private key. This field includes the signature algorithm identifier.

The standard uses the following notation to define a certificate:

CA<<A>> = CA {V, SN, AI, CA, T_A, A, Ap}

Where, Y <<X>> = the certificate of user X issued by certification authority Y

Y {I} = the signing of I by Y. It consists of I with an encrypted hash code appended The CA signs the certificate with its private key. If the corresponding public key is known to a user, then that user can verify that a certificate signed by the CA is valid.

Certificates

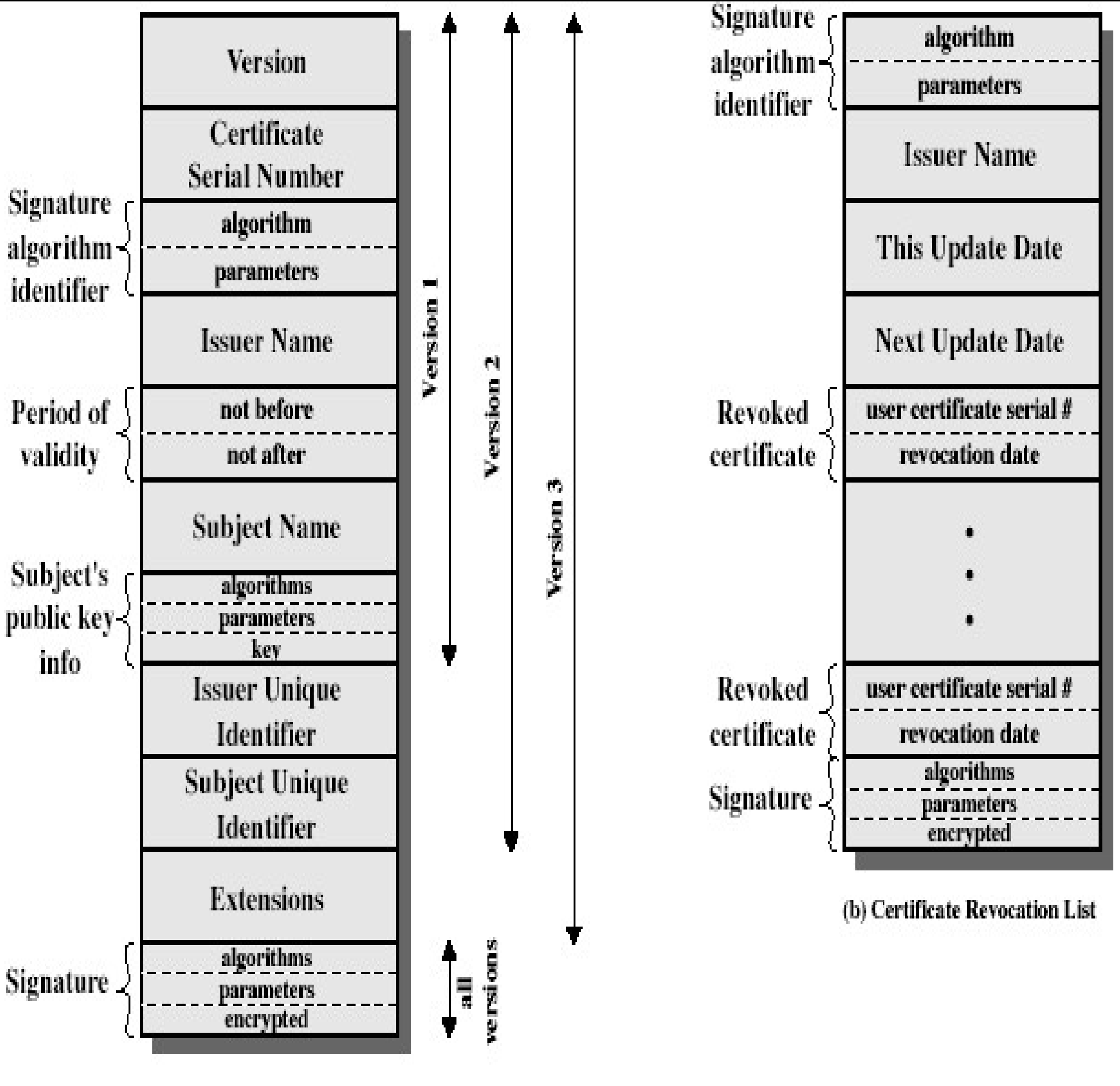
The heart of the X.509 scheme is the public-key certificate associated with each user. These user certificates are assumed to be created by some trusted certification authority (CA) and placed in the directory by the CA or by the user.

Version:

Differentiates among successive versions of the certificate format; the default is version 1. If the Issuer Unique Identifier or Subject Unique Identifier are present, the value must be version 2. If one or more extensions are present, the version must be version 3.

Serial number:

An integer value, unique within the issuing CA, that is unambiguously associated with this certificate.



(a) X.509 Certificate

(b) Certificate Revocation List

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html.

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (447-450),(454-471)

Course Teacher

Verified by HOD

LECTURE HANDOUTS

L-49

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **IV - Authentication, Email & Web Security**

Date of Lecture:

Topic of Lecture: Electronic Mail security: Pretty Good Privacy(PGP)

Introduction : (Maximum 5 sentences)

- Select the best available cryptographic algorithms as building blocks.
- Integrate these algorithms into a general purpose application that is independent of operating system and processor and that is based on a small set of easy-to-use commands.
- Make the package and its documentation, including the source code, freely available via the internet, bulletin boards and commercial networks.
- Enter into an agreement with a company to provide a fully compatible, low cost commercial version of PGP.

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Authentication applications
- ✓ Kerberos -X.509

Detailed content of the Lecture:

PRETTY GOOD PRIVACY (PGP)

PGP provides the confidentiality and authentication service that can be used for electronic mail and file storage applications**.**

The steps involved in PGP are:

- Select the best available cryptographic algorithms as building blocks.
- Integrate these algorithms into a general purpose application that is independent of operating system and processor and that is based on a small set of easy-to-use commands.
- Make the package and its documentation, including the source code, freely available via the internet, bulletin boards and commercial networks.
- Enter into an agreement with a company to provide a fully compatible, low cost commercial version of PGP.

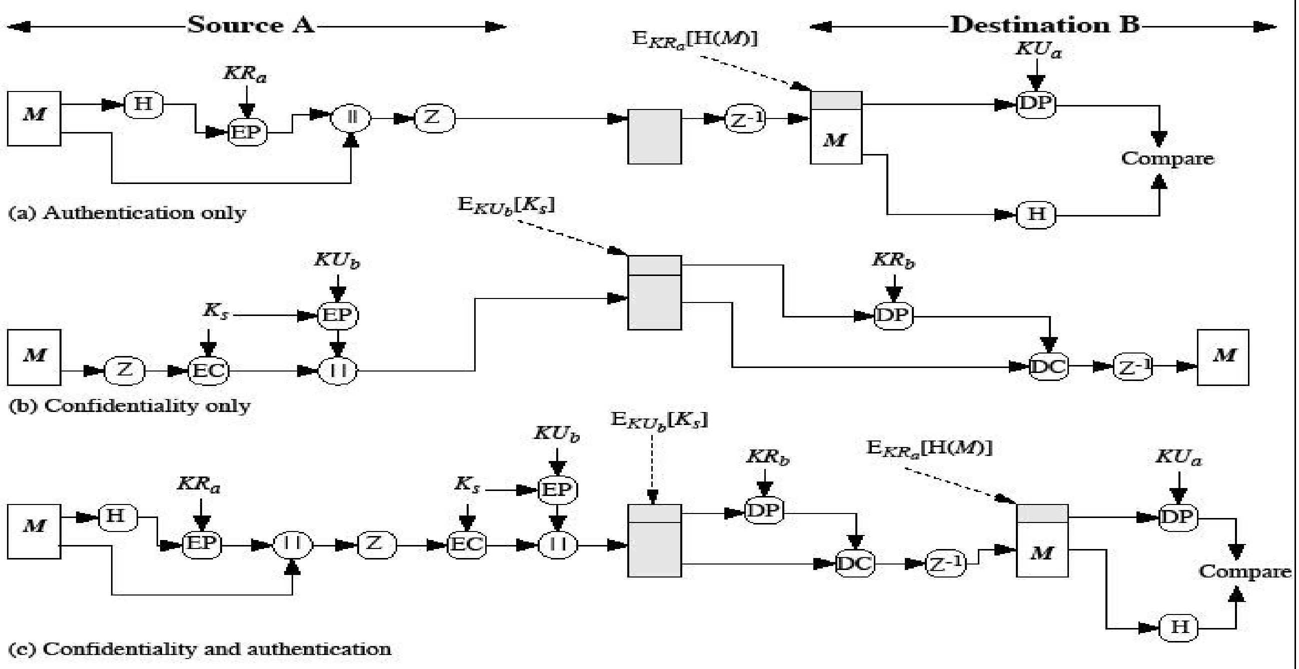
PGP has grown explosively and is now widely used. A number of reasons can be cited for this growth.

- It is available free worldwide in versions that run on a variety of platform.
- It is based on algorithms that have survived extensive public review and are considered extremely secure.

e.g., RSA, DSS and Diffie Hellman for public key encryption CAST-128, IDEA and 3DES for conventional encryption SHA-1 for hash coding.

- It has a wide range of applicability.

- It was not developed by, nor it is controlled by, any governmental or standards organization.



(a) Authentication only

(b) Confidentiality only

(c) Confidentiality and authentication

Confidentiality and authentication

Fig.4.5.1.1:PGP Cryptographic Functions

Operational description

The actual operation of PGP consists of five services: authentication, confidentiality, compression, e-mail compatibility and segmentation.

1. Authentication

   The sequence for authentication is as follows:

   - The sender creates the message
   - SHA-1 is used to generate a 160-bit hash code of the message
   - The hash code is encrypted with RSA using the sender‟s private key and the result is prepended to the message
   - The receiver uses RSA with the sender‟s public key to decrypt and recover the hash code.
   - The receiver generates a new hash code for the message and compares it with the decrypted hash code. If the two match, the message is accepted as authentic.

2. Confidentiality

Confidentiality is provided by encrypting messages to be transmitted or to be stored locally as files. In both cases, the conventional encryption algorithm CAST-128 may be used. The 64-bit cipher feedback (CFB) mode is used.

In PGP, each conventional key is used only once. That is, a new key is generated as a random 128-bit number for each message. Thus although this is referred to as **a session key**, it is in reality a **one time key**. To protect the key, it is encrypted with the receiver‟s public key.

The sequence for confidentiality is as follows:

- The sender generates a message and a random 128-bit number to be used as a session key for this message only.
- The message is encrypted using CAST-128 with the session key.
- The session key is encrypted with RSA, using the receiver‟s public key and is prepended to the

message.

- The receiver uses RSA with its private key to decrypt and recover the session key.
- The session key is used to decrypt the message.

Here both services may be used for the same message. First, a signature is generated for the plaintext message and prepended to the message. Then the plaintext plus the signature is encrypted using CAST-128 and the session key is encrypted using RSA.

3. Compression

As a default, PGP compresses the message after applying the signature but before encryption. This has the benefit of saving space for both e-mail transmission and for file storage.

The signature is generated before compression for two reasons:

- It is preferable to sign an uncompressed message so that one can store only the uncompressed message together with the signature for future verification. If one signed a compressed document, then it would be necessary either to store a compressed version of the message for later verification or to recompress the message when verification is required.
- Even if one were willing to generate dynamically a recompressed message fro verification, PGP“s compression algorithm presents a difficulty. The algorithm is not deterministic; various implementations of the algorithm achieve different tradeoffs in running speed versus compression ratio and as a result, produce different compression forms.

Message encryption is applied after compression to strengthen cryptographic security. Because the compressed message has less redundancy than the original plaintext, cryptanalysis is more difficult. The compression algorithm used is ZIP.

4. e-mail compatibility

Many electronic mail systems only permit the use of blocks consisting of ASCII texts.
To accommodate this restriction, PGP provides the service of
converting the raw 8-bit binary stream to a stream of printable ASCII characters. The scheme used for this purpose is **radix-64 conversion**. Each group of three octets of binary data is mapped into four ASCII characters.
e.g., consider the 24-bit (3 octets) raw text sequence 00100011 01011100 10010001, we can express this input in block of 6-bits to produce 4 ASCII characters.

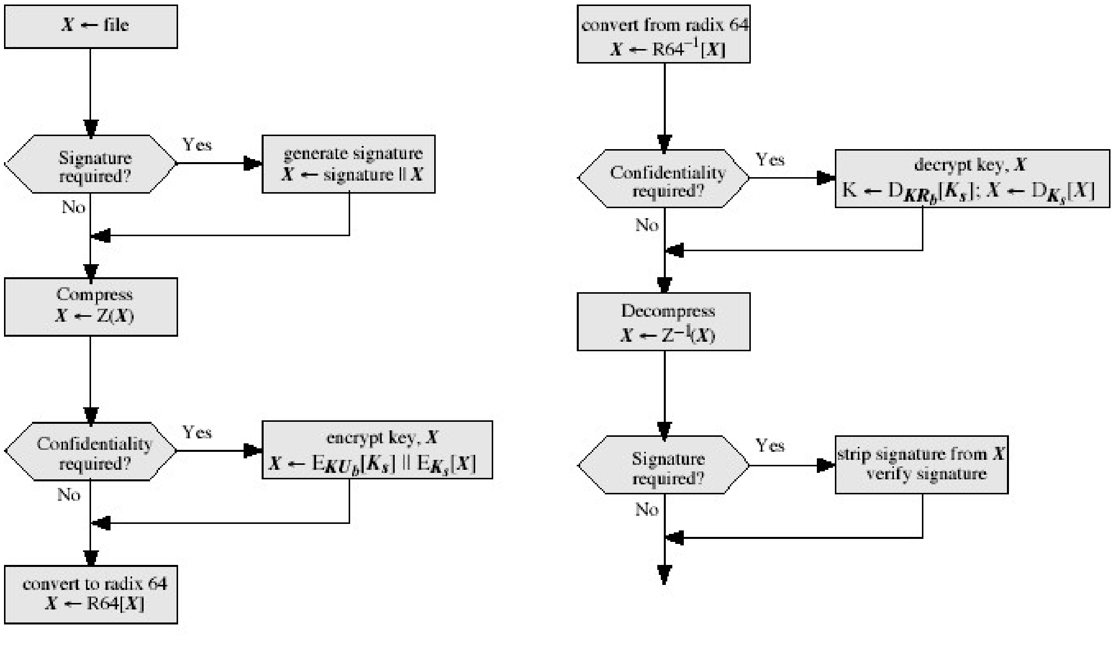
001000	110101	110010	010001
I	L	Y	R => corresponding ASCII Characters

1. Segmentation and reassembly

E-mail facilities often are restricted to a maximum length. E.g., many of the facilities accessible through the internet impose a maximum length of 50,000 octets. Any message longer than that must be broken up into smaller segments, each of which is mailed separately.

To accommodate this restriction, PGP automatically subdivides a message that is too large into segments that are small enough to send via e-mail. The segmentation is done after all the other processing, including the radix-64 conversion. At the receiving end, PGP must strip off all e-mail headers and reassemble the entire original block before performing the other steps.

PGP Operation Summary:



X ← file
Signature required?
Yes
generate signature X ← signature || X
No
Compress X ← Z(X)
Confidentiality required?
Yes
encrypt key, X X ← E_{KU_b}[K_s] || E_{K_s}[X]
No
convert to radix 64 X ← R64[X]
convert from radix 64 X ← R64^{-1}[X]
Confidentiality required?
Yes
decrypt key, X K ← D_{KR_b}[K_s]; X ← D_{K_s}[X]
No
Decompress X ← Z^{-1}(X)
Signature required?
Yes
strip signature from X verify signature
No

(a) Generic Transmission Diagram (from A)

(b) Generic Reception Diagram (to B)

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014
Page No: (565-572)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L-50

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **IV - Authentication, Email & Web Security**

Date of Lecture:

Topic of Lecture: Pretty Good Privacy(PGP) – Keys

Introduction : (Maximum 5 sentences)

- Select the best available cryptographic algorithms as building blocks.
- Integrate these algorithms into a general purpose application that is independent of operating system and processor and that is based on a small set of easy-to-use commands.
- Make the package and its documentation, including the source code, freely available via the internet, bulletin boards and commercial networks.
- Enter into an agreement with a company to provide a fully compatible, low cost commercial version of PGP.

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Authentication applications
- ✓ Kerberos -X.509

Detailed content of the Lecture:

PRETTY GOOD PRIVACY (PGP)

PGP provides the confidentiality and authentication service that can be used for electronic mail and file storage applications**.**

The steps involved in PGP are:

- Select the best available cryptographic algorithms as building blocks.
- Integrate these algorithms into a general purpose application that is independent of operating system and processor and that is based on a small set of easy-to-use commands.
- Make the package and its documentation, including the source code, freely available via the internet, bulletin boards and commercial networks.
- Enter into an agreement with a company to provide a fully compatible, low cost commercial version of PGP.

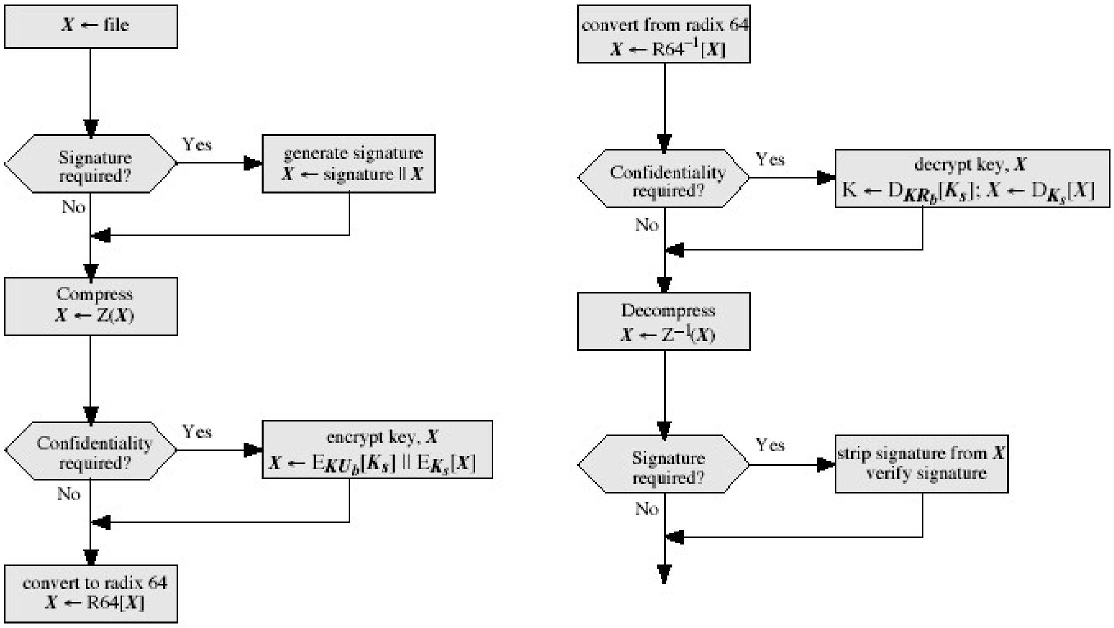
PGP has grown explosively and is now widely used. A number of reasons can be cited for this growth.

- It is available free worldwide in versions that run on a variety of platform.
- It is based on algorithms that have survived extensive public review and are considered extremely secure.

e.g., RSA, DSS and Diffie Hellman for public key encryption CAST-128, IDEA and 3DES for conventional encryption SHA-1 for hash coding.

- It has a wide range of applicability.
- It was not developed by, nor it is controlled by, any governmental or standards organization.

PGP Operation Summary:



(a) Generic Transmission Diagram (from A)

(b) Generic Reception Diagram (to B)

Cryptographic keys and key rings

Three separate requirements can be identified with respect to these keys:

- A means of generating unpredictable session keys is needed.
- It must allow a user to have multiple public key/private key pairs.
- Each PGP entity must maintain a file of its own public/private key pairs as well as a file of public keys of correspondents.

We now examine each of the requirements in turn.

1. Session key generation

Each session key is associated with a single message and is used only for the purpose of encryption and decryption of that message. Random 128-bit numbers are generated using CAST-128 itself. The input to the random number generator consists of a 128-bit key and two 64-bit blocks that are treated as plaintext to be encrypted. Using cipher feedback mode, the CAST-128 produces two 64-bit cipher text blocks, which are concatenated to form the 128-bit session key. The plaintext input to CAST-128 is itself derived from a stream of 128-bit randomized numbers. These numbers are based on the keystroke input from the user.

2. Key identifiers

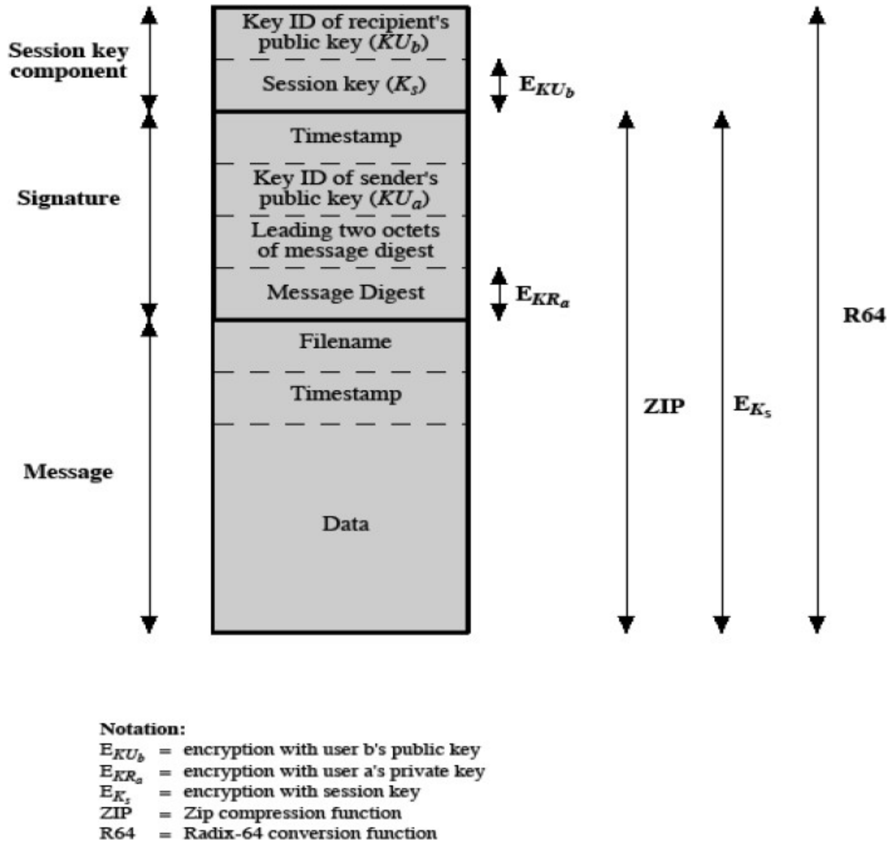
If multiple public/private key pair are used, then how does the recipient know which of the public keys was used to encrypt the session key? One simple solution would be to transmit the public key with the message but, it is unnecessary wasteful of space. Another solution would be to associate an identifier with each public key that is unique at least within each user.

The solution adopted by PGP is to assign a key ID to each public key that is, with very high probability, unique within a user ID. The key ID associated with each public key consists of its least significant 64 bits. i.e., the key ID of public key KU_a is

$$(KU_a \bmod 2^{64}).$$

A message consists of three components.

- **Message component** – includes actual data to be transmitted, as well as the filename and a timestamp that specifies the time of creation.
- **Signature component** – includes the following
  - Timestamp – time at which the signature was made.
  - Message digest – hash code.
  - Two octets of message digest – to enable the recipient to determine if the correct public key was used to decrypt the message.
  - Key ID of sender‟s public key – identifies the public key
- **Session key component** – includes session key and the identifier of the recipient public key.


Session key component
Signature
Message
Key ID of recipient's public key (KU_b)
Session key (K_s)
Timestamp
Key ID of sender's public key (KU_a)
Leading two octets of message digest
Message Digest
Filename
Timestamp
Data
E_{KU_b}
E_{KR_a}
ZIP
E_{K_s}
R64
Notation:
E_{KU_b} = encryption with user b's public key
E_{KR_a} = encryption with user a's private key
E_{K_s} = encryption with session key
ZIP = Zip compression function
R64 = Radix-64 conversion function

3.Key rings

PGP provides a pair of data structures at each node, one to store the public/private key pair owned by that node and one to store the public keys of the other users known at that node. These data structures are referred to as private key ring and public key ring.

The general structures of the private and public key rings are shown below:

Timestamp – the date/time when this entry was made.

Key ID – the least significant bits of the public key.

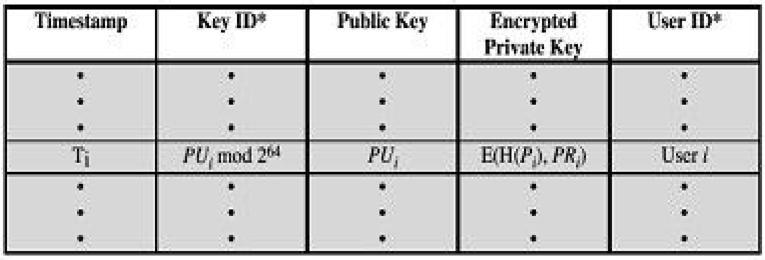
Public key – public key portion of the pair.

Private key – private key portion of the pair.

User ID – the owner of the key.

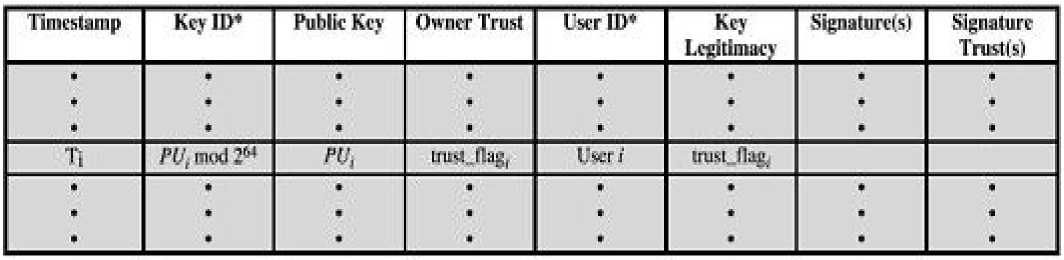
Key legitimacy field – indicates the extent to which PGP will trust that this is a valid public key for this user.

Private Key Ring



Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
• • •	• • •	• • •	• • •	• • •
T_i	PU_i mod 2^{64}	PU_i	$E(H(P_i), PR_i)$	User i
• • •	• • •	• • •	• • •	• • •

Public Key Ring



Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •
T_i	PU_i mod 2^{64}	PU_i	trust_flag$_i$	User i	trust_flag$_i$		
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

* = field used to index table

Signature trust field – indicates the degree to which this PGP user trusts the signer to certify public key.

Owner trust field – indicates the degree to which this public key is trusted to sign other public key certificates.

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014
Page No: (565-572)

Course Teacher

Verified by HOD

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **IV - Authentication, Email & Web Security**

Date of Lecture:

Topic of Lecture: PGP – Message Generation, Reception

Introduction : (Maximum 5 sentences)

- Select the best available cryptographic algorithms as building blocks.
- Integrate these algorithms into a general purpose application that is independent of operating system and processor and that is based on a small set of easy-to-use commands.
- Make the package and its documentation, including the source code, freely available via the internet, bulletin boards and commercial networks.
- Enter into an agreement with a company to provide a fully compatible, low cost commercial version of PGP.

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Authentication applications
- ✓ Kerberos -X.509

Detailed content of the Lecture:

PRETTY GOOD PRIVACY (PGP)

PGP provides the confidentiality and authentication service that can be used for electronic mail and file storage applications**.**

The steps involved in PGP are:

- Select the best available cryptographic algorithms as building blocks.
- Integrate these algorithms into a general purpose application that is independent of operating system and processor and that is based on a small set of easy-to-use commands.
- Make the package and its documentation, including the source code, freely available via the internet, bulletin boards and commercial networks.
- Enter into an agreement with a company to provide a fully compatible, low cost commercial version of PGP.

PGP has grown explosively and is now widely used. A number of reasons can be cited for this growth.

- It is available free worldwide in versions that run on a variety of platform.
- It is based on algorithms that have survived extensive public review and are considered extremely secure.

e.g., RSA, DSS and Diffie Hellman for public key encryption CAST-128, IDEA and 3DES for conventional encryption SHA-1 for hash coding.

- It has a wide range of applicability.
- It was not developed by, nor it is controlled by, any governmental or standards organization.

PGP message generation

First consider message transmission and assume that the message is to be both signed and encrypted. The sending PGP entity performs the following steps:

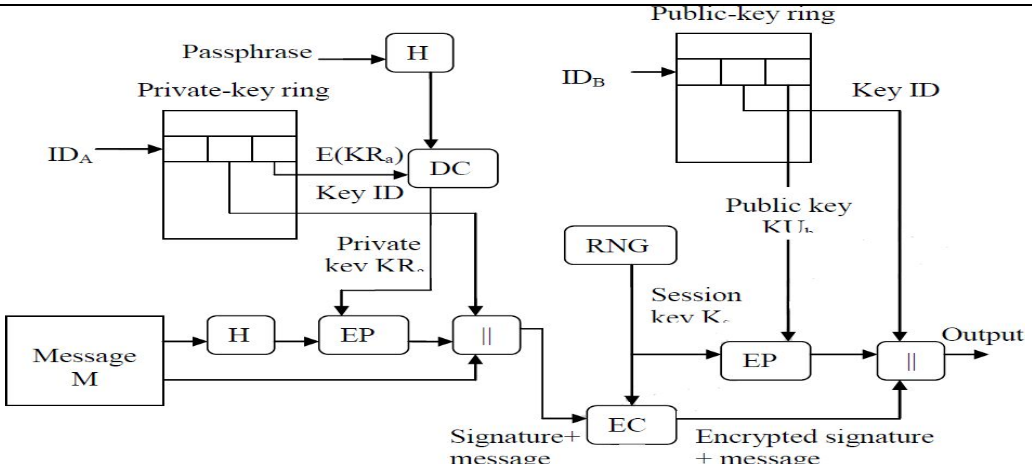


Figure 4.5.3.1: PGP message generation

1. **Signing the message**
   - PGP retrieves the sender‟s private key from the private key ring using user ID as an index. If user ID was not provided, the first private key from the ring is retrieved.
   - PGP prompts the user for the passpharse (password) to recover the unencrypted private key.
   - The signature component of the message is constructed.
2. Encrypting the message
   - PGP generates a session key and encrypts the message.
   - PGP retrieves the recipient‟s public key from the public key ring using user ID as index.
   - The session key component of the message is constructed.

The receiving PGP entity performs the following steps

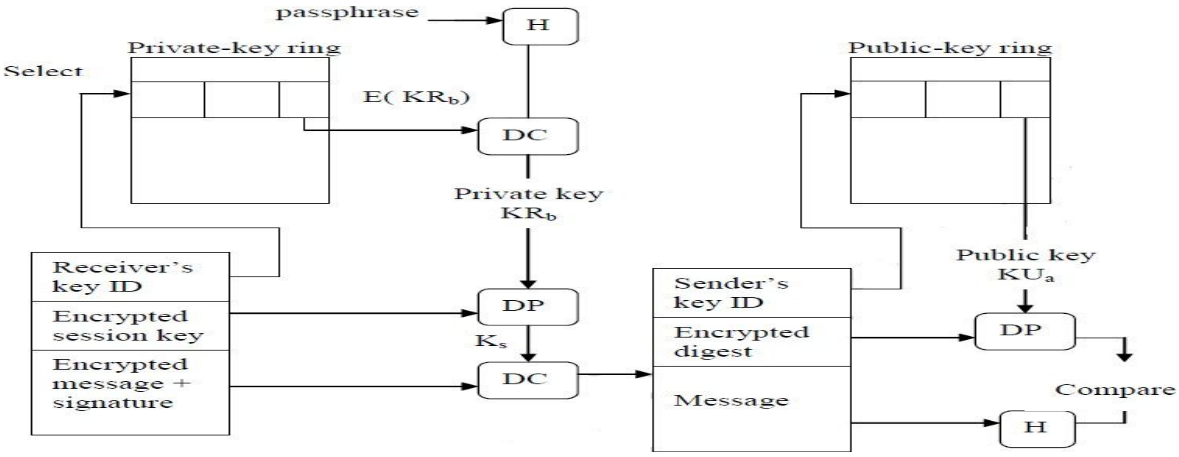


Figure: PGP message reception

1. **Decrypting the message**
   - PGP retrieves the receiver‟s private key from the private key ring, using the key ID field in the session key component of the message as an index.
   - PGP prompts the user for the passpharse (password) to recover the unencrypted private key.
   - PGP then recovers the session key and decrypts the message.
2. **Authenticating the message**
   - PGP retrieves the sender‟s public key from the public key ring, using the key ID field in the signature key component of the message as an index.

- PGP recovers the transmitted message digest.
- PGP computes the message digest for the received message and compares it to the transmitted message digest to authenticate.

Public-Key Management

This whole business of protecting public keys from tampering is the single most difficult problem in practical public key applications. PGP provides a structure for solving this problem, with several suggested options that may be used.

Approaches to Public-Key Management

The essence of the problem is this: User A must build up a public-key ring containing the public keys of other users to interoperate with them using PGP. Suppose that A's key ring contains a public key attributed to B but that the key is, in fact, owned by C. This could happen if, for example, A got the key from a bulletin board system (BBS) that was used by B to post the public key but that has been compromised by C. The result is that two threats now exist. First, C can send messages to A and forge B's signature, so that A will accept the message as coming from B. Second, any encrypted message from A to B can be read by C.

The following are some approaches that could be used:

1. Physically get the key from B. B could store her public key (PU_b) on a floppy disk and hand it to A..
2. Verify a key by telephone. If A can recognize B on the phone, A could call B and ask her to dictate the key, in radix-64 format, over the phone.
3. Obtain B's public key from a mutual trusted individual D. For this purpose, the introducer, D, creates a signed certificate. The certificate includes B's public key, the time of creation of the key, and a validity period for the key.
4. Obtain B's public key from a trusted certifying authority. Again, a public key certificate is created and signed by the authority. A could then access the authority, providing a user name and receiving a signed certificate.

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014
Page No: (565-572)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L-52

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **IV - Authentication, Email & Web Security**

Date of Lecture:

Topic of Lecture: S/MIME

Introduction : (Maximum 5 sentences)

S/MIME (Secure/Multipurpose Internet Mail Extension) is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security. S/MIME is defined in a number of documents, most importantly RFCs 3369, 3370, 3850 and 3851.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- ✓ Electronic Mail security
- ✓ Pretty Good Privacy(PGP)

Detailed content of the Lecture:

S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extension) is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security. S/MIME is defined in a number of documents, most importantly RFCs 3369, 3370, 3850 and 3851.

Multipurpose Internet Mail Extensions

MIME is an extension to the RFC 822 framework that is intended to address some of the problems and limitations of the use of SMTP (Simple Mail Transfer Protocol) or some other mail transfer protocol and RFC 822 for electronic mail. Following are the limitations of SMTP/822 scheme:

1. SMTP cannot transmit executable files or other binary objects.
2. SMTP cannot transmit text data that includes national language characters because these are represented by 8-bit codes with values of 128 decimal or higher, and SMTP is limited to 7-bit ASCII.
3. SMTP servers may reject mail message over a certain size.
4. SMTP gateways that translate between ASCII and the character code EBCDIC do not use a consistent set of mappings, resulting in translation problems.
5. SMTP gateways to X.400 electronic mail networks cannot handle nontextual data included in X.400 messages.
6. Some SMTP implementations do not adhere completely to the SMTP standards defined in RFC 821. Common problems include:

- Deletion, addition, or reordering of carriage return and linefeed
- Truncating or wrapping lines longer than 76 characters
- Removal of trailing white space (tab and space characters)
- Padding of lines in a message to the same length
- Conversion of tab characters into multiple space characters

Overview

The MIME specification includes the following elements:

1. **Five new message header** fields are defined, which may be included in an RFC 822 header. These fields provide information about the body of the message.
2. **A number of content formats** are defined, thus standardizing representations that support multimedia electronic mail.
3. **Transfer encodings** are defined that enable the conversion of any content format into a form that is protected from alteration by the mail system.

In this subsection, we introduce the five message header fields. The next two subsections deal with content formats and transfer encodings.

The five header fields defined in MIME are as follows:

- **MIME-Version**: Must have the parameter value 1.0. This field indicates that the message conforms to RFCs 2045 and 2046.
- **Content-Type**: Describes the data contained in the body with sufficient detail
- **Content-Transfer-Encoding**: Indicates the type of transformation that has been used to represent the body of the message in a way that is acceptable for mail transport.
- **Content-ID:** Used to identify MIME entities uniquely in multiple contexts.
- **Content-Description**: A text description of the object with the body; this is useful when the object is not readable (e.g., audio data).

MIME Content Types

The bulk of the MIME specification is concerned with the definition of a variety of content types. This reflects the need to provide standardized ways of dealing with a wide variety of information representations in a multimedia environment.

Below lists the content types specified in RFC 2046. There are seven different major types of content and a total of 15 subtypes

MIME Content Types (This item is displayed on page 461 in the print version)

Type	**Subtype**	**Description**
Text	Plain	Unformatted text; may be ASCII or ISO 8859.
	Enriched	Provides greater format flexibility.
Multipart	Mixed	The different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message.
	Parallel	Differs from Mixed only in that no order is defined for delivering the parts to the receiver.

	Alternative	The different parts are alternative versions of the same information. They are ordered in increasing faithfulness to the original, and the recipient's mail system should display the "best" version to the user.
	Digest	Similar to Mixed, but the default type/subtype of each part is message/rfc822.
Message	rfc822	The body is itself an encapsulated message that conforms to RFC 822.
	Partial	Used to allow fragmentation of large mail items, in a way that is transparent to the recipient.
	External-body	Contains a pointer to an object that exists elsewhere.
Image	jpeg	The image is in JPEG format, JFIF encoding.
	gif	The image is in GIF format.
Video	mpeg	MPEG format.
Audio	Basic	Single-channel 8-bit ISDN mu-law encoding at a sample rate of 8 kHz.
Application	PostScript	Adobe Postscript.
	octet-stream	General binary data consisting of 8-bit bytes.

For the text type of body, no special software is required to get the full meaning of the text, aside from support of the indicated character set. The primary subtype is plain text, which is simply a string of ASCII characters or ISO 8859 characters. The enriched subtype allows greater formatting flexibility. The multipart type indicates that the body contains multiple, independent parts. The Content-Type header field includes a parameter, called boundary, that defines the delimiter between body parts.

MIME Transfer Encodings

The other major component of the MIME specification, in addition to content type specification, is a definition of transfer encodings for message bodies. The objective is to provide reliable delivery across the largest range of environments.

The MIME standard defines two methods of encoding data. The Content-Transfer-Encoding field can actually take on six values. For SMTP transfer, it is safe to use the 7bit form. The 8bit and binary forms may be usable in other mai transport contexts. Another Content-Transfer-Encoding value is x-token, which indicates that some other encoding scheme is used, for which a name is to be supplied. The two actual encoding schemes defined are quoted-printable and base64.

MIME Transfer Encodings	
7bit	The data are all represented by short lines of ASCII characters.
8bit	The lines are short, but there may be non-ASCII characters (octets with the high-order bit set).
Binary	Not only may non-ASCII characters be present but the lines are not necessarily short enough for SMTP transport.
quoted-printable	Encodes the data in such a way that if the data being encoded are mostly ASCII text, the encoded form of the data remains largely recognizable by humans.
base64	Encodes data by mapping 6-bit blocks of input to 8-bit blocks of output, all of which are printable ASCII characters.
x-token	A named nonstandard encoding.

The quoted-printable transfer encoding is useful when the data consists largely of octets that correspond to printable ASCII characters. In essence, it represents nonsafe characters by the hexadecimal representation of their code and introduces reversible (soft) line breaks to limit message lines to 76 characters.

The base64 transfer encoding, also known as radix-64 encoding, is a common one for encoding arbitrary binary data in such a way as to be invulnerable to the processing by mail transport programs.

Canonical Form

An important concept in MIME and S/MIME is that of canonical form. Canonical form is a format, appropriate to the content type, that is standardized for use between systems. This is in contrast to native form, which is a format that may be peculiar to a particular system.

S/MIME Functionality

In terms of general functionality, S/MIME is very similar to PGP. Both offer the ability to sign and/or encrypt messages. In this subsection, we briefly summarize S/MIME capability. We then look in more detail at this capability by examining message formats and message preparation.

Functions

S/MIME provides the following functions:

- **Enveloped data:** This consists of encrypted content of any type and encrypted-content encryption keys for one or more recipients.
- **Signed data**: A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer. The content plus signature are then encoded using base64 encoding. A signed data message can only be viewed by a recipient with S/MIME capability.
- **Clear-signed data:** As with signed data, a digital signature of the content is formed. However, in this case, only the digital signature is encoded using base64. As a result, recipients without S/MIME capability can view the message content, although they cannot verify the signature.
- **Signed and enveloped data:** Signed-only and encrypted-only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted.

Cryptographic Algorithms

- hash functions: SHA-1 & MD5
- digital signatures: DSS & RSA
- session key encryption: ElGamal & RSA
- message encryption: Triple-DES, RC2/40 and others
- have a procedure to decide which algorithms to use.

S/MIME uses the following terminology, taken from RFC 2119 to specify the requirement level:

- Must: The definition is an absolute requirement of the specification. An implementation must include this feature or function to be in conformance with the specification.
- Should: There may exist valid reasons in particular circumstances to ignore this feature or function, but it is recommended that an implementation include the feature or function.

Cryptographic Algorithms Used in S/MIME	
Function	**Requirement**
Create a message digest to be used in forming a digital signature. Encrypt message digest to form digital signature.	MUST support SHA-1. Receiver SHOULD support MD5 for backward compatibility. Sending and receiving agents MUST support DSS. Sending agents SHOULD support RSA encryption. Receiving agents SHOULD support verification of RSA signatures with key sizes 512 bits to 1024 bits.
Encrypt session key for transmission with message.	Sending and receiving agents SHOULD support Diffie-Hellman. Sending and receiving agents MUST support RSA encryption with key sizes 512 bits to 1024 bits.
Encrypt message for transmission with one-time session key.	Sending and receiving agents MUST support encryption with triple DES Sending agents SHOULD support encryption with AES. Sending agents SHOULD support encryption with RC2/40.
Create a message authentication code	Receiving agents MUST support HMAC with SHA-1. Receiving agents SHOULD support HMAC with SHA-1.

S/MIME Messages

S/MIME makes use of a number of new MIME content types. All of the new application types use the designation PKCS. This refers to a set of public-key cryptography specifications issued by RSA Laboratories and made available for the S/MIME effort.

S/MIME Content Types			
Type	**Subtype**	**smime Parameter**	**Description**
Multipart	Signed		A clear-signed message in two parts: one is the message and the other is the signature.
Application	pkcs 7-mime	signedData	A signed S/MIME entity.
	pkcs 7-mime	envelopedData	An encrypted S/MIME entity.
	pkcs 7-mime	Degenerate signedData	An entity containing only public- key certificates.
	pkcs 7-mime	CompressedData	A compressed S/MIME entity
	pkcs 7-signature	signedData	The content type of the signature subpart of a multipart/signed message.

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (565-572)

Course Teacher

Verified by HOD

LECTURE HANDOUTS **L-53**

CSE **III/V**

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **IV - Authentication, Email & Web Security**

Date of Lecture:

Topic of Lecture: IP Security Overview

Introduction : (Maximum 5 sentences)

- The **IP security** (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the **IP** network that provide data authentication, integrity, and confidentiality.
- It also defines the encrypted, decrypted and authenticated packets

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ S/MIME
- ✓ TLC
- ✓ IP

Detailed content of the Lecture:

The **IP security (IPSec)** is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. **ses of IP Security –**

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

Protection Mechanisms

IPsec provides two mechanisms for protecting data:

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

Both mechanisms have their own Security Association Database (SADB).

Authentication Header

The authentication header provides data authentication, strong integrity, and replay protection to IP datagrams. AH protects the greater part of the IP datagram. AH cannot protect fields that change nondeterministically between sender and receiver. For example, the IP TTL field is not a predictable field and, consequently, not protected by AH. AH is inserted between the IP header and the transport header. The transport header can be TCP, UDP, ICMP, or another IP header when tunnels are being used.

Authentication Algorithms and the AH Module

IPsec implements AH as a module that is automatically pushed on top of IP. The /dev/ipsecah entry tunes AH with the ndd command. Future authentication algorithms can be loaded on top of AH. Current authentication algorithms include HMAC-MD5 and HMAC-SHA-1. Each authentication algorithm has its own key size and key format properties. See the authmd5h (7M) and authsha1(7M) man pages for details. For tuning IP configuration parameters,

Security Considerations for AH

Replay attacks threaten an AH when an AH does not enable replay protection. An AH does not protect against eavesdropping. Adversaries can still see data that is protected with AH.

Encapsulating Security Payload

The encapsulating security payload (ESP) header provides confidentiality over what the ESP encapsulates, as well as the services that AH provides. However, ESP only provides its protections over the part of the datagram that ESP encapsulates.

ESP's authentication services are optional. These services enable you to use ESP and AH together on the same datagram without redundancy. Because ESP uses encryption-enabling technology, ESP must conform to U.S. export control laws.

ESP encapsulates its data, so ESP only protects the data that follows its beginning in the datagram. In a TCP packet, ESP encapsulates only the TCP header and its data. If the packet is an IP-in-IP datagram, ESP protects the inner IP datagram.

Per-socket policy allows **self-encapsulation**, so ESP can encapsulate IP options when ESP needs to. Unlike the authentication header (AH), ESP allows multiple kinds of datagram protection. Using only a single form of datagram protection can make the datagram vulnerable. For example, if you use ESP to provide confidentiality only, the datagram is still vulnerable to replay attacks and cut-and-paste attacks. Similarly, if ESP protects only integrity, ESP could provide weaker protection than AH. The datagram would be vulnerable to eavesdropping.

Algorithms and the ESP Module

IPsec ESP implements ESP as a module that is automatically pushed on top of IP. The /dev/ipsecesp entry tunes ESP with the ndd command. ESP allows encryption algorithms to be pushed on top of ESP, in addition to the authentication algorithms that are used in AH. Encryption algorithms include Data Encryption Standard (DES), Triple-DES (3DES), Blowfish, and AES.

Security Considerations for ESP

An ESP without authentication is vulnerable to cut-and-paste cryptographic attacks and to replay attacks. When you use ESP without confidentiality, ESP is as vulnerable to eavesdropping as AH is.

Authentication and Encryption Algorithms

IPsec uses two types of algorithms, authentication and encryption. The authentication algorithms and the DES encryption algorithms are part of core Solaris installation. If you plan to use other algorithms that are supported for IPsec, you must install the Solaris Encryption Kit. The Solaris Encryption Kit is provided on a separate CD.

Authentication Algorithms

Authentication algorithms produce an integrity checksum value or **digest** that is based on the data and a key. The man pages for authentication algorithms describe the size of both the digest and key. The following table lists the authentication algorithms that are supported in the Solaris operating environment. The table also lists the format of the algorithms when the algorithms are used as security options to the IPsec utilities and their man page names.

Table 1–1 Supported Authentication Algorithms

Algorithm Name	Security Option Format	Man Page
HMAC-MD5	md5, hmac-md5	authmd5h(7M)
HMAC-SHA-1	sha, sha1, hmac-sha, hmac-sha1	authsha1(7M)

Encryption Algorithms

Encryption algorithms encrypt data with a key. The algorithms operate on data in units of a **block size**. The man pages for encryption algorithms describe the block size and the key size for each algorithm. By default, the DES–CBC and 3DES-CBC algorithms are installed.

The AES and Blowfish algorithms are available to IPsec when you install the Solaris Encryption Kit. The kit is available on a separate CD that is **not** part of the Solaris 9 installation box. The Solaris 9 Encryption Kit Installation Guide describes how to install the Solaris Encryption Kit.

The following table lists the encryption algorithms that are supported in the Solaris operating environment. The table lists the format of the algorithms when the algorithms are used as security options to the IPsec utilities. The table also lists their man page names, and lists the package that contains the algorithm.

Table 1–2 Supported Encryption Algorithms

Algorithm Name	Security Option Format	Man Page	Package
DES-CBC	des, des-cbc	encrdes(7M)	SUNWcsr, SUNWcarx.u
3DES–CBC or Triple-DES	3des, 3des-cbc	encr3des(7M)	SUNWcsr, SUNWcarx.u
Blowfish	blowfish, blowfish-cbc	encrbfsh(7M)	SUNWcryr, SUNWcryrx
AES-CBC	aes, aes-cbc	encraes(7M)	SUNWcryr, SUNWcryrx

Protection Policy and Enforcement Mechanisms

IPsec separates its protection policy from its enforcement mechanisms. You can enforce IPsec policies in the following places:

- On a system-wide level
- On a per-socket level

You use the ipsecconf command to configure the system-wide policy. See the ipsecconf(1M) man page.

IPsec applies the system-wide policy to incoming datagrams and outgoing datagrams. You can apply some additional rules to outgoing datagrams, because of the additional data that is known by the system. Inbound datagrams can be either accepted or dropped.

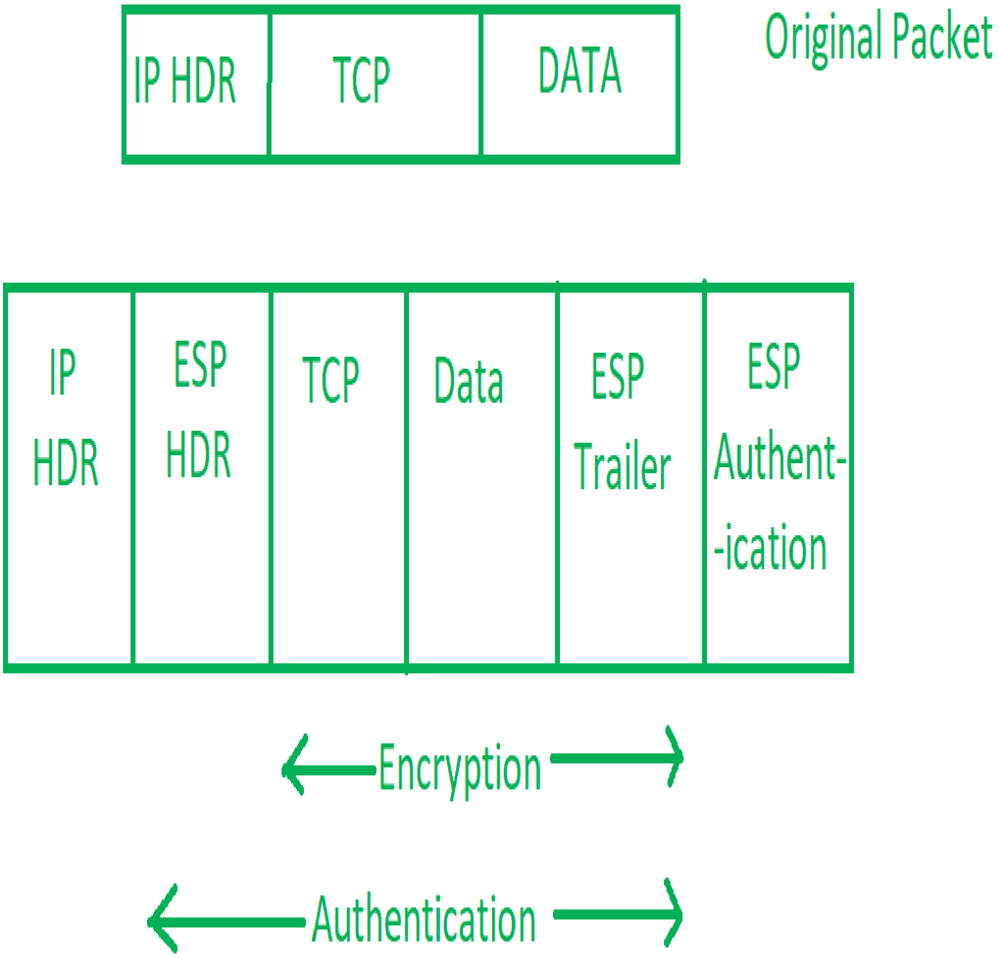
The decision to drop or accept an inbound datagram is based on several criteria, which sometimes overlap or conflict. Conflicts are resolved by determining which rule is parsed first. Except when a policy entry states that traffic should bypass all other policy, the traffic is automatically accepted. Outbound datagrams are either sent with protection or without protection. If protection is applied, the algorithms are either specific or non-specific.

Internet Key Exchange (IKE) –

It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and

Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.

Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produces a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets which are not authorized are discarded and not given to receiver.



Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (604-633)

Course Teacher

Verified by HOD

LECTURE HANDOUTS

L-54

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **IV - Authentication, Email & Web Security**

Date of Lecture:

Topic of Lecture: IP Security Services

Introduction : **(Maximum 5 sentences)**

- IPSec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ S/MIME
- ✓ TLC
- ✓ IP

Detailed content of the Lecture:

Two protocols are used to provide security: an authentication protocol designated by the header of the protocol, Authentication Header (AH); and a combined encryption/authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP).

The services are

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets (a form of partial sequence integrity)
- Confidentiality (encryption)
- Limited traffic flow confidentiality

Table 1.1 shows which services are provided by the AH and ESP protocols. For ESP, there are two cases: with and without the authentication option. Both AH and ESP are vehicles for access control, based on the distribution of cryptographic keys and security protocols. Table 1.1. IPSec Services A key concept that appears in both the authentication and confidentiality mechanisms for IP is the security association (SA). An association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it.

A security association is uniquely identified by three parameters:

Security Parameters Index (SPI): A bit string assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.

IP Destination Address: Currently, only unicast addresses are allowed; this is the address of the destination endpoint of the SA, which may be an end user system or a network system such as a firewall or router.

Security Protocol Identifier:

This indicates whether the association is an AH or ESP security association. Hence, in any IP packet, the security association is uniquely identified by the Destination Address in the IPv4 or IPv6 header and the SPI in the enclosed extension header (AH or ESP).

SA Parameters: In each IPSec implementation, there is a nominal Security Association Database that defines the parameters associated with each SA.

A security association is normally defined by the following parameters:

- **Sequence Number Counter:** A 32-bit value used to generate the Sequence Number field in AH or ESP headers.
- **Sequence Counter Overflow:** A flag indicating whether overflow of the Sequence Number Counter should generate an auditable event and prevent further transmission of packets on this SA (required for all implementations).
- **Anti-Replay Window:** Used to determine whether an inbound AH or ESP packet is a replay. • AH Information: Authentication algorithm, keys, key lifetimes, and related parameters being used with AH (required for AH implementations).
- **ESP Information:** Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP (required for ESP implementations).
- **Lifetime of This Security Association**: A time interval or byte count after which an SA must be replaced with a new SA (and new SPI) or terminated, plus an indication of which of these actions should occur (required for all implementations).
- **IPSec Protocol Mode:** Tunnel, transport, or wildcard (required for all implementations).
- **Path MTU:** Any observed path maximum transmission unit (maximum size of a packet that can be transmitted without fragmentation) and aging variables (required for all implementations). The key management mechanism that is used to distribute keys is coupled to the authentication and privacy mechanisms only by way of the Security Parameters Index. Hence, authentication and privacy have been specified independent of any specific key management mechanism.

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (604-633)

Course Teacher

Verified by HOD

LECTURE HANDOUTS

L-55

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **IV - Authentication, Email & Web Security**

Date of Lecture:

Topic of Lecture: IP Security Protocols

Introduction : (Maximum 5 sentences)

- IPSec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services

Prerequisite knowledge for Complete understanding and learning of Topic:

✓ S/MIME
✓ TLC
✓ IP

Detailed content of the Lecture:

IP Security (IPSec) provides a stable, long lasting base for providing network layer security.
IPSec supports all of the cryptographic algorithms in use today, and can also accommodate newer, more powerful algorithms as they become available.

IPSec protocols address these major security issues:

Data origin authentication
Verifies that each datagram was originated by the claimed sender.

Data integrity
Verifies that the contents of a datagram were not changed in transit, either deliberately or due to random errors.

Data confidentiality
Conceals the content of a message, typically by using encryption.

Replay protection
Ensures that an attacker cannot intercept a datagram and play it back at some later time.

Automated management of cryptographic keys and security associations
Ensures that your VPN policy can be used throughout the extended network with little or no manual configuration.

VPN uses two IPSec protocols to protect data as it flows through the VPN: Authentication Header (AH) and Encapsulating Security Payload (ESP).

The other part of IPSec enablement is the Internet Key Exchange (IKE) protocol, or key management. While IPSec encrypts your data, IKE supports automated negotiation of security associations (SAs), and automated generation and refreshing of cryptographic keys.

The principal IPSec protocols are listed below:

Authentication Header

The Authentication Header (AH) protocol provides data origin authentication, data integrity, and replay protection. However, AH does not provide data confidentiality, which means that all of your data is sent in the clear.

Encapsulating Security Payload

The Encapsulating Security Payload (ESP) protocol provides data confidentiality, and also optionally provides data origin authentication, data integrity checking, and replay protection.

AH and ESP combined

VPN allows you to combine AH and ESP for host-to-host connections in transport mode.

Enhanced Cryptographic Algorithms

Cryptographic algorithms supported in the VPN selection for Key Exchange Policy and Data policy security association attributes.

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (604-633)

Course Teacher

Verified by HOD

LECTURE HANDOUTS

L-56

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **IV - Authentication, Email & Web Security**

Date of Lecture:

Topic of Lecture: Web Security :SSL

Introduction : (Maximum 5 sentences)

- **Web security** is also known as "**Cybersecurity**".
- It basically means protecting a website or **web** application by detecting, preventing and responding to **cyber** threats.
- Anything that is applied over the **Internet** should have some form of **web security** to protect it.

Prerequisite knowledge for Complete understanding and learning of Topic:

- S/MIME
- IP Security
- Web Security:SSL

Detailed content of the Lecture:

WEB SECURITY CONSIDERATIONS

The World Wide Web is fundamentally a client/server application running over the Internet and TCP/IP intranets. As such, the security tools and approaches discussed so far in this book are relevant to the issue of Web security. But, as pointed out in [GARF02], the Web presents new challenges not generally appreciated in the context of computer and network security.

The Internet is two-way. Unlike traditional publishing environments—even electronic publishing systems involving teletext, voice response, or fax-back— the Web is vulnerable to attacks on the Web servers over the Internet.

The Web is increasingly serving as a highly visible outlet for corporate and product information and as the platform for business transactions. Reputations can be damaged and money can be lost if the Web servers are subverted.

Web Security Threats

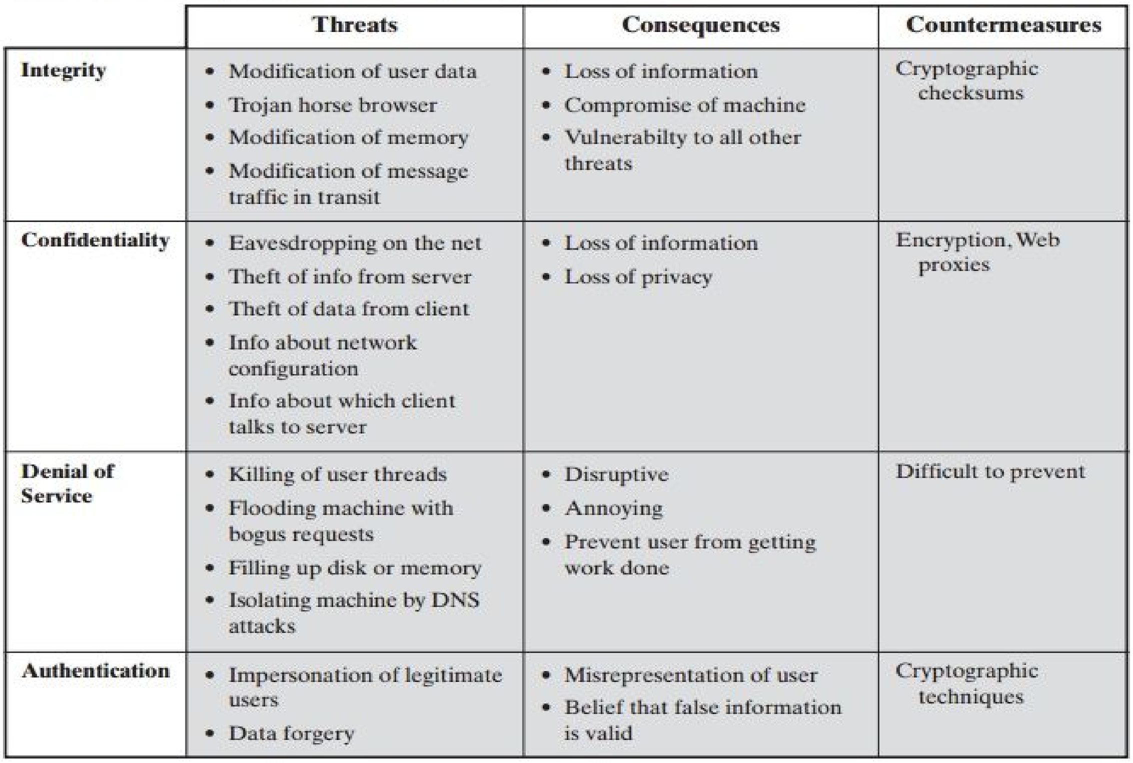
- The types of security threats faced when using the Web.
- One way to group these threats is in terms of passive and active attacks. Passive attacks include eavesdropping on network traffic between browser and server and gaining access to information on a Web site that is supposed to be restricted.
- Active attacks include impersonating another user, altering messages in transit between client and server, and altering information on a Web site.
- Another way to classify Web security threats is in terms of the location of the threat: Web server, Web browser, and network traffic between browser and server.

- Issues of server and browser security fall into the category of computer system secu- rity;
- Part Four of this book addresses the issue of system security in general but is also applicable to Web system security. Issues of traffic security fall into the category of network security and are addressed in this chapter.

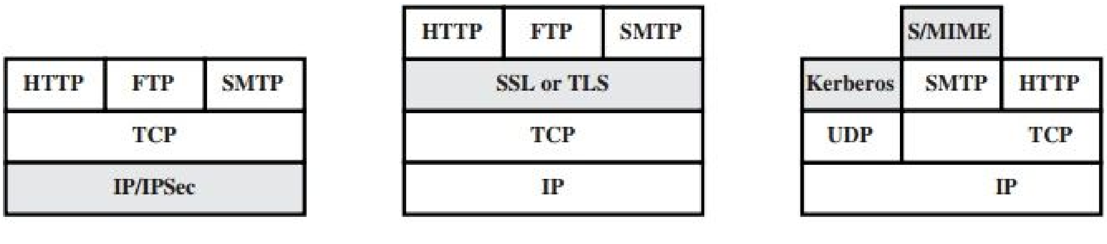
Web Traffic Security Approaches

- A number of approaches to providing Web security are possible. The various approaches that have been considered are similar in the services

Table 16.1 A Comparison of Threats on the Web



	Threats	Consequences	Countermeasures
Integrity	• Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerabilty to all other threats	Cryptographic checksums
Confidentiality	• Eavesdropping on the net • Theft of info from server • Theft of data from client • Info about network configuration • Info about which client talks to server	• Loss of information • Loss of privacy	Encryption, Web proxies
Denial of Service	• Killing of user threads • Flooding machine with bogus requests • Filling up disk or memory • Isolating machine by DNS attacks	• Disruptive • Annoying • Prevent user from getting work done	Difficult to prevent
Authentication	• Impersonation of legitimate users • Data forgery	• Misrepresentation of user • Belief that false information is valid	Cryptographic techniques



(a) Network level (b) Transport level (c) Application level

Figure 16.1 Relative Location of Security Facilities in the TCP/IP Protocol Stack

Video Content / Details of website for further learning (if any):
http://www.brainkart.com/article/Web-Security-Considerations_8479/

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014Page No: (513-525)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L-57

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **IV - Authentication, Email & Web Security**

Date of Lecture:

Topic of Lecture: SSL Protocol

Introduction : (Maximum 5 sentences)

Secure Socket Layer (SSL) provide security to the data that is transferred between web browser and server. SSL encrypt the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

Prerequisite knowledge for Complete understanding and learning of Topic:

- S/MIME
- IP Security
- Web Security:SSL

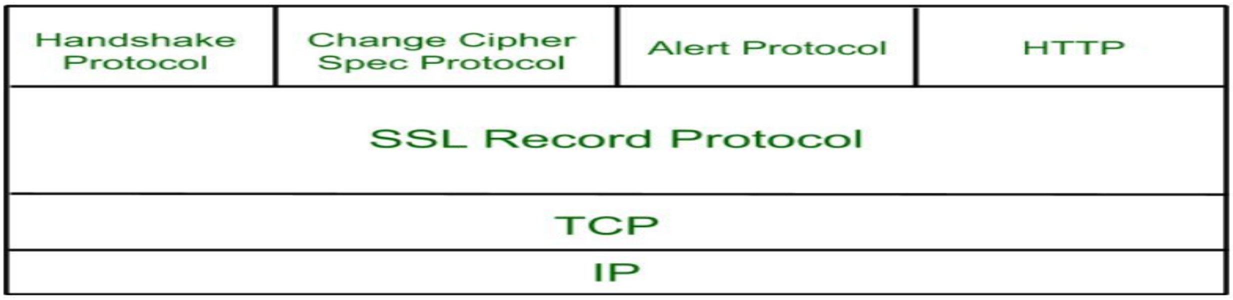
Detailed content of the Lecture:

Secure Socket Layer (SSL) provide security to the data that is transferred between web browser and server. SSL encrypt the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

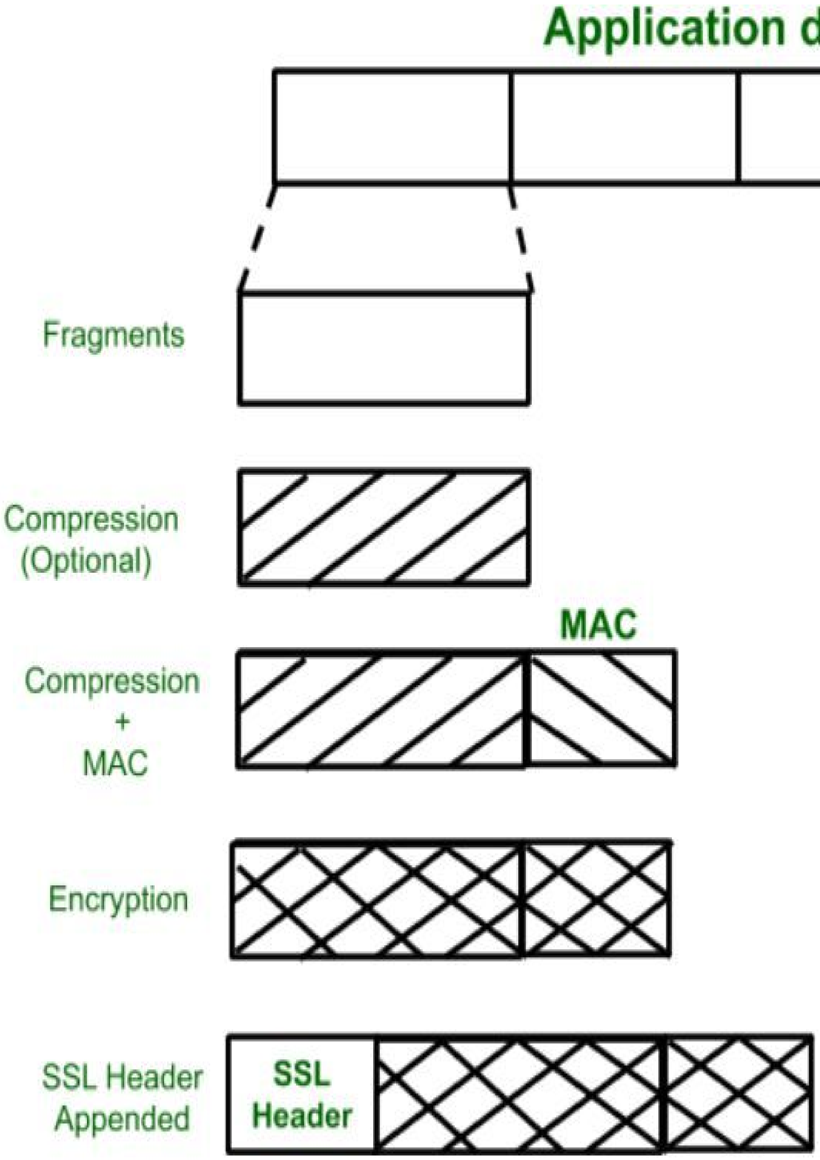
SSL Protocol Stack:



- **SSL Record Protocol:**

  SSL Record provide two services to SSL connection. Confidentiality
- Message Integerity

In SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.



Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: William Stallings, Cryptography and Network Security, Prentice Hall, 2014

Page No: (513-525)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L-58

LECTURE HANDOUTS

CSE

III/V

Course Name with Code : **Cr** **/16CSD09**

Course Teacher :

U : **IV - Authentication, Email & Web Security**

Date of Lecture:

Topic of Lecture: TLS

Introduction : (Maximum 5 sentences)
The SSL protocol was originally developed at Netscape to enable ecommerce transaction security on the Web, which required encryption to protect customers' personal data, as well as authentication and integrity guarantees to ensure a safe transaction. To achieve this, the SSL protocol was implemented at the application layer, directly on top of TCP (Figure 4-1), enabling protocols above it (HTTP, email, instant messaging, and many others) to operate unchanged while providing communication security when communicating across the network.

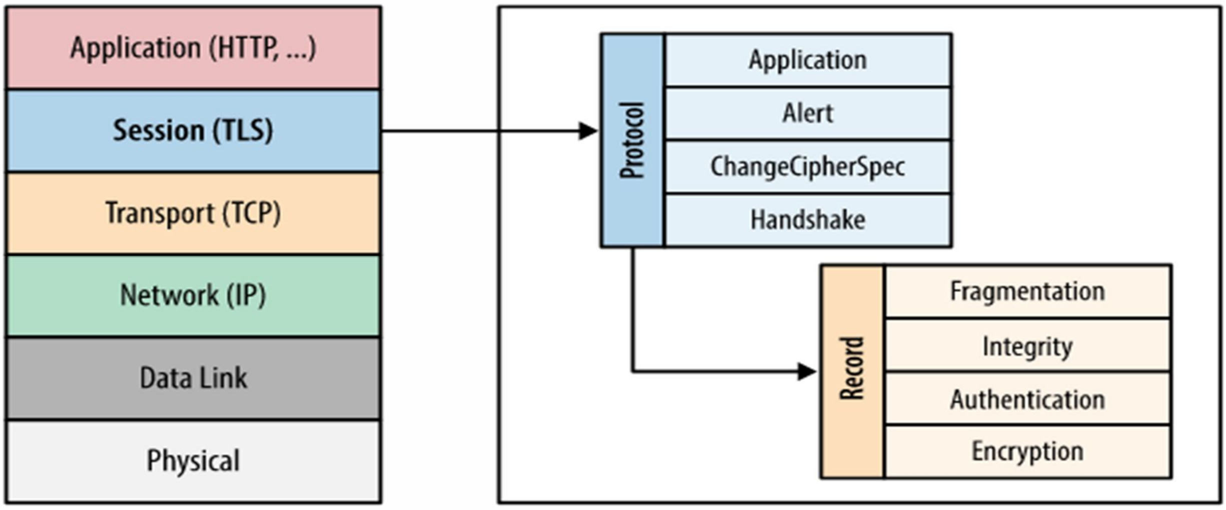
Prerequisite knowledge for Complete understanding and learning of Topic:

- S/MIME
- IP Security
- Web Security:SSL

Detailed content of the Lecture:

- The SSL protocol was originally developed at Netscape to enable ecommerce transaction security on the Web, which required encryption to protect customers' personal data, as well as authentication and integrity guarantees to ensure a safe transaction.
- To achieve this, the SSL protocol was implemented at the application layer, directly on top of TCP (Figure 4-1), enabling protocols above it (HTTP, email, instant messaging, and many others) to operate unchanged while providing communication security when communicating across the network.

When SSL is used correcy, a third-party observer can only infer the connection endpoints, type of encryption, as well as the frequency and an approximate amount of data sent, but cannot read or modify any of the actual data.



TLS 1.3

- Fortunately, help is on the way. Version 1.3 of the TLS protocol, currently in draft form but soon to be finalized, plugs a lot of these holes by jettisoning support for legacy encryption systems.
- There is backwards compatibility in the sense that connections will fall back to TLS 1.2 if one end isn't capable of using the newer encryptions systems on the 1.3 approved list.
- However, if, for instance, a man-in-the-middle attack tries to force a fallback to 1.2 in order to snoop on packets, that will be detected and the connection dropped.

There are still servers out there that are using versions of TLS even older than 1.2 — some are still using the original SSL protocol. If your sever is one of those, you should upgrade now, and just leap ahead and upgrade to the draft 1.3 spec.

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:

Book: William Stallings," Cryptography and Network Security ", Pearson Education, 2013
Page No: (526-530)

Course Teacher

Verified by HOD

LECTURE HANDOUTS

L-59

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **IV - Authentication, Email & Web Security**

Date of Lecture:

Topic of Lecture: SET:SET for E-Commerce Transactions

Introduction : (Maximum 5 sentences)

- Secure electronic **transaction** (**SET**) was an early communications protocol used by **e-commerce** websites to secure electronic debit and credit card payments.
- Secure electronic **transaction** was used to facilitate the secure transmission of consumer card information via electronic portals on the Internet.

Prerequisite knowledge for Complete understanding and learning of Topic:

- S/MIME
- IP Security
- Web Security:SSL

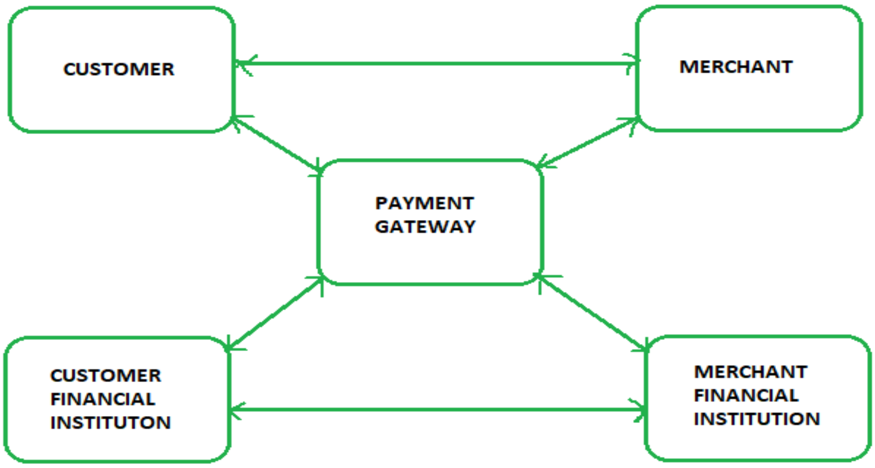
Detailed content of the Lecture:

Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied on those payments.

It uses different encryption and hashing techniques to secure payments over internet done through credit cards. SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which provided its Secure Transaction Technology (STT) and NetScape which provided technology of Secure Socket Layer (SSL).

SET protocol restricts revealing of credit card details to merchants thus keeping hackers and thieves at bay. SET protocol includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.

Before discussing SET further, let’s see a general scenario of electronic transaction, which includes client, payment gateway, client financial institution, merchant and merchant financial institution.



Requirements in SET :

SET protocol has some requirements to meet, some of the important requirements are :

- It has to provide mutual authentication i.e., customer (or cardholder) authentication by confirming if the customer is intended user or not and merchant authentication.
- It has to keep the PI (Payment Information) and OI (Order Information) confidential by appropriate encryptions.
- It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.
- SET also needs to provide interoperability and make use of best security mechanisms.

SET functionalities

- ○ **Provide Authentication**
  - **Merchant Authentication** – To prevent theft, SET allows customers to check previous relationships between merchant and financial institution. Standard X.509V3 certificates are used for this verification.
  - **Customer / Cardholder Authentication** – SET checks if use of credit card is done by an authorized user or not using X.509V3 certificates.
  -
- ○ **Provide Message Confidentiality** : Confidentiality refers to preventing unintended people from reading the message being transferred. SET implements confidentiality by using encryption techniques. Traditionally DES is used for encryption purpose.

- ○ **Provide Message Integrity** : SET doesn't allow message modification with the help of signatures. Messages are protected against unauthorized modification using RSA digital signatures with SHA-1 and some using HMAC with SHA-1.

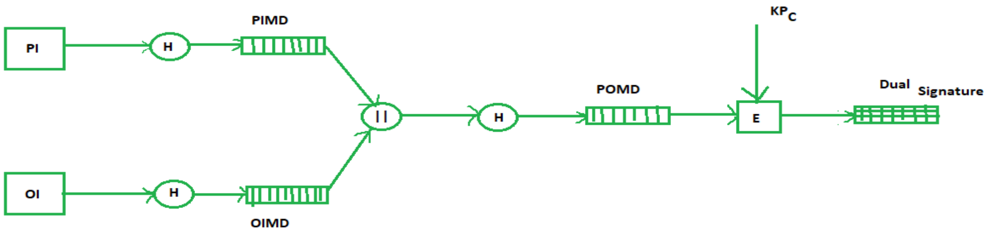
Dual Signature :

The dual signature is a concept introduced with SET, which aims at connecting two information pieces meant for two different receivers :

Order Information (OI) for merchant

Payment Information (PI) for bank

You might think sending them separately is an easy and more secure way, but sending them in a connected form resolves any future dispute possible. Here is the generation of dual signature:



Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:

Book: William Stallings," Cryptography and Network Security Principles and Practices", Pearson Education, 2010
Page No: (549-560)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L-60

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **IV - Authentication, Email & Web Security**

Date of Lecture:

Topic of Lecture: SET Participants

Introduction : (Maximum 5 sentences)

- Cardholder – customer.
- Issuer – customer financial institution.
- Merchant.
- Acquirer – Merchant financial.
- Certificate authority – Authority which follows certain standards and issues certificates(like X. 509V3) to all other **participants**.

Prerequisite knowledge for Complete understanding and learning of Topic:

- S/MIME
- IP Security
- Web Security:SSL

Detailed content of the Lecture:

Participants in SET :

In the general scenario of online transaction, SET includes similar participants:

1. **Cardholder** – customer
2. **Issuer** – customer financial institution
3. **Merchant**
4. **Acquirer** – Merchant financial
5. **Certificate authority** – Authority which follows certain standards and issues certificates(like X.509V3) to all other participants.

SET functionalities:

- **Provide Authentication**
  - **Merchant Authentication** – To prevent theft, SET allows customers to check previous relationships between merchant and financial institution. Standard X.509V3 certificates are used for this verification.
  - **Customer / Cardholder Authentication** – SET checks if use of credit card is done by an authorized user or not using X.509V3 certificates.
- **Provide Message Confidentiality** : Confidentiality refers to preventing unintended people from reading the message being transferred. SET implements confidentiality by using encryption techniques. Traditionally DES is used for encryption purpose.
- **Provide Message Integrity** : SET doesn't allow message modification with the help of signatures. Messages are protected against unauthorized modification using RSA digital signatures with SHA-1 and some using HMAC with SHA-1,

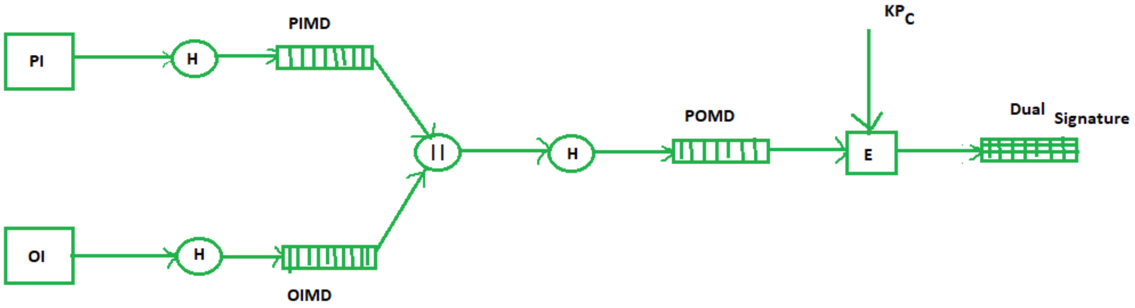
Dual Signature :

The dual signature is a concept introduced with SET, which aims at connecting two information pieces meant for two different receivers :

Order Information (OI) for merchant

Payment Information (PI) for bank

You might think sending them separately is an easy and more secure way, but sending them in a connected form resolves any future dispute possible. Here is the generation of dual signature:



Purchase Request Generation :

The process of purchase request generation requires three inputs:

- Payment Information (PI)

- Dual Signature
- Order Information Message Digest (OIMD)

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:

Book: William Stallings,” Cryptography and Network Security Principles and Practices”, Pearson Education, 2010
Page No: (549-560)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L-61

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **V - System Level Security, Malicious Software**

Date of Lecture:

Topic of Lecture: System Security Intruder

Introduction : (Maximum 5 sentences)

- Intruder attacks range from the benign to the serious. At the benign end of the scale, there are many people who simply wish to explore internets and see what is out there.
- At the serious end are individuals who are attempting to read privileged data, perform unauthorized modifications to data, or disrupt the system.
- Benign intruders might be tolerable, although they do consume resources and may slow performance for legitimate users

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- Masquerader
- Misfeasor
- Clandestine user

Detailed content of the Lecture:

System Security:

Security of a computer system is a crucial task. It is a process of ensuring confidentiality and integrity of the OS.
A system is said to be secure if its resources are used and accessed as intended under all the circumstances, but no system can guarantee absolute security from several of the various malicious threats and unauthorized access.

Security of a system can be threatened via two violations:

- **Threat:** A program which has the potential to cause serious damage to the system.
- **Attack:** An attempt to break security and make unauthorized use of an asset.

Security violations affecting the system can be categorized as malicious and accidental. **Malicious threats**, as the name suggests are a kind of harmful computer code or web script designed to create system vulnerabilities leading to back doors and security breaches. **Accidental Threats**, on the other hand, are comparatively easier to be protected against.
Example: Denial of Service DDoS attack.
Security can be compromised via any of the breaches mentioned:

- **Breach of confidentiality:** This type of violation involves the unauthorized reading of data.
- **Breach of integrity:** This violation involves unauthorized modification of data.
- **Breach of availability:** It involves an unauthorized destruction of data.
- **Theft of service:** It involves an unauthorized use of resources.

- **Denial of service:** It involves preventing legitimate use of the system. As mentioned before, such attacks can be accidental in nature.

Security System Goals –
Henceforth, based on the above breaches, the following security goals are aimed:

One of the most publicized attacks to security is the intruder, generally referred to as hacker or cracker. Three classes of intruders are as follows:

- **Masquerader** – an individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.

  Misfeasor – a legitimate user who accesses data, programs, or resources for which suchaccess is not authorized, or who is authorized for such access but misuse his or her privileges.

  Clandestine user – an individual who seizes supervisory control of the system and usesthis control to evade auditing and access controls or to suppress audit collection.

The masquerader is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user can be either an outsider or an insider.

- Intruder attacks range from the benign to the serious. At the benign end of the scale, there are many people who simply wish to explore internets and see what is out there.

- At the serious end are individuals who are attempting to read privileged data, perform unauthorized modifications to data, or disrupt the system. Benign intruders might be tolerable, although they do consume resources and may slow performance for legitimate users. However there is no way in advance to know whether an intruder will be benign or malign.

An analysis of previous attack revealed that there were two levels of hackers:

- The high levels were sophisticated users with a thorough knowledge of the technology.
- The low levels were the „foot soldiers" who merely use the supplied cracking programs with little understanding of how they work.

One of the results of the growing awareness of the intruder problem has been the establishment of a number of Computer Emergency Response Teams (CERT)

Video Content / Details of website for further learning (if any):

WilliamStallings.com/Crypto/Crypto4e.html.

Important Books/Journals for further learning including the page nos.:
Book:
Cryptography and network security principles and practice ,William Stalling,5th edition
Page No: R2(567-570)

Course Teacher

Verified by HOD

Estd. 2000

LECTURE HANDOUTS

L-62

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **V - System Level Security, Malicious Software**

Date of Lecture:

Topic of Lecture: Intrusion Detection

Introduction : (Maximum 5 sentences)

- Intruder attacks range from the benign to the serious. At the benign end of the scale, there are many people who simply wish to explore internets and see what is out there.
- At the serious end are individuals who are attempting to read privileged data, perform unauthorized modifications to data, or disrupt the system.
- Benign intruders might be tolerable, although they do consume resources and may slow performance for legitimate users

**Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)**

- Masquerader
- Misfeasor
- Clandestine user

Detailed content of the Lecture:

INTRUSIONDETECTION

- If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised.
- An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions.
- Intrusion detection enables the collection of information about intrusion techniques that can be

The approaches to intrusion detection

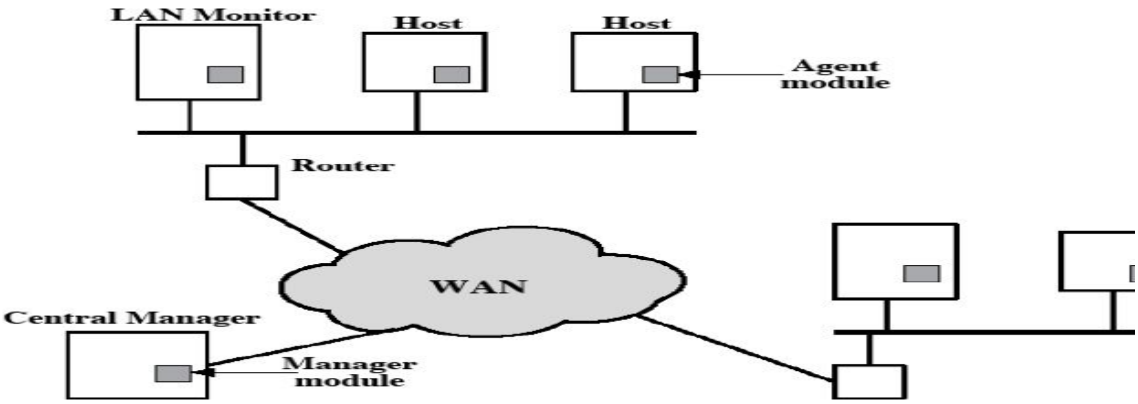
- ✓ Statistical anomaly detection
- ✓ Rule-based detection

Audit Records

- ✓ Native audit records
- ✓ Detection-specific audit records

Distributed Intrusion Detection

- ✓ Host agent module
- ✓ LAN monitor agent module
- ✓ **Central manager module**

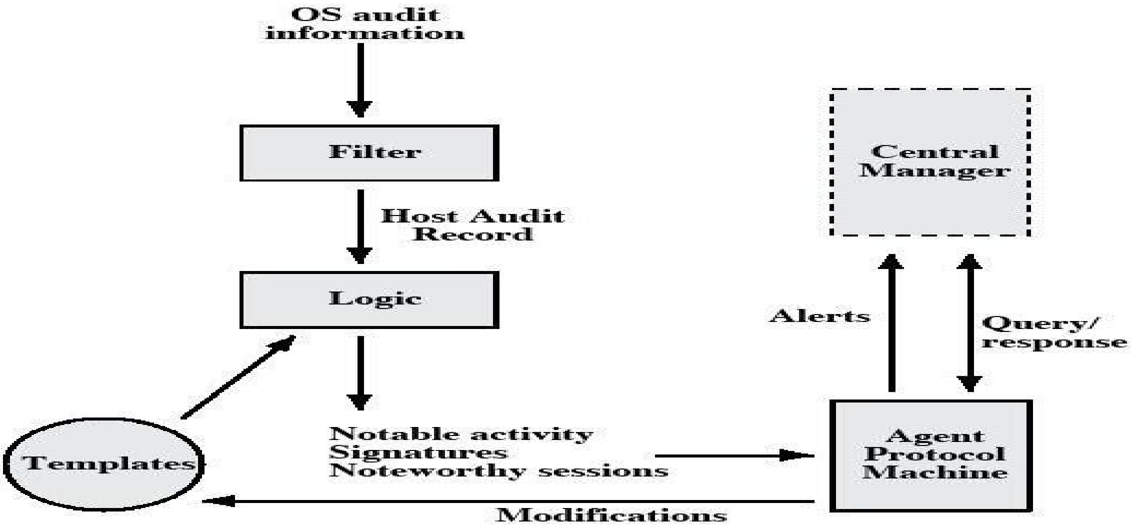


Honey pots

A relatively recent innovation in intrusion detection technology is the honey pot. Honey pots are decoy systems that are designed to lure a potential attacker away from critical systems

Honey pots are designed to

- divert an attacker from accessing critical systems
- collect information about the attacker's activity
- encourage the attacker to stay on the system long enough for administrators to respond



Video Content / Details of website for further learning (if any):

WilliamStallings.com/Crypto/Crypto4e.html.

Important Books/Journals for further learning including the page nos.:
Book:
Cryptography and network security principles and practice ,William Stalling,5th edition
Page No: R2(567-570)

Course Teacher

Verified by HOD

LECTURE HANDOUTS

L-63

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **V - System Level Security, Malicious Software**

Date of Lecture:

Topic of Lecture: Intrusion Prevention System

Introduction : (Maximum 5 sentences)

- Intrusion Prevention System is also known as Intrusion Detection and Prevention System.
- It is a network security application that monitors network or system activities for malicious activity.

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- Masquerader
- Misfeasor
- Clandestine user

Detailed content of the Lecture:
Intrusion Prevention System

- Major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it.
- Intrusion prevention systems are contemplated as augmentation of Intrusion Detection Systems (IDS) because both IPS and IDS operate network traffic and system activities for malicious activity.
- IPS typically record information related to observed events, notify security administrators of important observed events and produce reports.

They use various response techniques, which involve the IPS stopping the attack itself, changing the security environment or changing the attack's content.

Classification of Intrusion Prevention System (IPS):

Intrusion Prevention System (IPS) is classified into 4 types:

1. **Network-based intrusion prevention system (NIPS):**
   It monitors the entire network for suspicious traffic by analyzing protocol activity.
2. **Wireless intrusion prevention system (WIPS):**
   It monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.
3. **Network behavior analysis (NBA):**
   It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy violations.
4. **Host-based intrusion prevention system (HIPS):**

It is an inbuilt software package which operates a single host for doubtful activity by scanning events that occur within that host.

Detection Method of Intrusion Prevention System (IPS):

1. **Signature-based detection:**
   Signature-based IDS operates packets in the network and compares with pre-built and preordained attack patterns known as signatures.
2. **Statistical anomaly-based detection:**
   Anomaly based IDS monitors network traffic and compares it against an established baseline. The baseline will identify what is normal for that network and what protocols are used. However, It may raise a false alarm if the baselines are not intelligently configured.
3. **Stateful protocol analysis detection:**
   This IDS method recognizes divergence of protocols stated by comparing observed events with pre-built profiles of generally accepted definitions of not harmful activity.

Comparison of IPS with IDS:

The main difference between Intrusion Prevention System (IPS) with Intrusion Detection Systems (IDS) are:

1. Intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected.
2. IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.
3. IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues and clean up unwanted transport and network layer options.

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html.

Important Books/Journals for further learning including the page nos.:
Book: Cryptography and network security principles and practice ,William Stalling,5th edition
Page No: R2(567-570)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

DESIGNING YOUR FUTURE
Estd. 2000

IQAC

LECTURE HANDOUTS

L-64

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **V - System Level Security, Malicious Software**

Date of Lecture:

Topic of Lecture: FIREWALLS

Introduction : (Maximum 5 sentences)

- ✓ Internet connectivity is no longer an option for most organizations. However, while internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets.
- ✓ This creates the threat to the organization. While it is possible to equip each workstation and server on the premises network with strong security features, such as intrusion protection, this is not a practical approach. The alternative, increasingly accepted, is the firewall.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- ✓ Service control
- ✓ Direction control
- ✓ User control
- ✓ Behavior control

Detailed content of the Lecture:

Firewall design principles

- Internet connectivity is no longer an option for most organizations. However, while internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets.
- This creates the threat to the organization. While it is possible to equip each workstation and server on the premises network with strong security features, such as intrusion protection, this is not a practical approach. The alternative, increasingly accepted, is the firewall.
- The firewall is inserted between the premise network and internet to establish a controlled link and to erect an outer security wall or perimeter.
- The aim of this perimeter is to protect the premises network from internet based attacks and to provide a single choke point where security and audit can be imposed. The firewall can be a single computer system or a set of two or more systems that cooperate to perform the firewall function.

Firewall characteristics:

- ✓ All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible.

- ✓ Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies.
- ✓ The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system. This implies that use of a trusted system with a secure operating system.

Four techniques that firewall use to control access and enforce the site's security policy is as follows:

- Service control – determines the type of internet services that can be accessed, inbound or outbound. The firewall may filter traffic on this basis of IP address and TCP port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as web or mail service.
- Direction control – determines the direction in which particular service request may be initiated and allowed to flow through the firewall.
- User control – controls access to a service according to which user is attempting to access it.
- Behavior control – controls how particular services are used.

Capabilities of firewall

- ✓ A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.
- ✓ A firewall provides a location for monitoring security related events. Audits and alarms can be implemented on the firewall system.
- ✓ A firewall is a convenient platform for several internet functions that are not security related.
- ✓ A firewall can serve as the platform for IPSec.

Limitations of firewall

- ✓ The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters.
- ✓ The firewall does not protect against internal threats. The firewall does not protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
- ✓ The firewall cannot protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: Cryptography and network security principles and practice ,William Stalling,5th edition
Page No:(622-624)

Course Teacher

Verified by HOD

DESIGNING YOUR FUTURE
Estd. 2000

IQAC

LECTURE HANDOUTS

L-65

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **V - System Level Security, Malicious Software**

Date of Lecture:

Topic of Lecture: Firewalls Types

Introduction : (Maximum 5 sentences)

- ✓ Internet connectivity is no longer an option for most organizations. However, while internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets.
- ✓ This creates the threat to the organization. While it is possible to equip each workstation and server on the premises network with strong security features, such as intrusion protection, this is not a practical approach. The alternative, increasingly accepted, is the firewall.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- ✓ Service control
- ✓ Direction control
- ✓ User control
- ✓ Behavior control

Detailed content of the Lecture:

Types of firewall

There are 3 common types of firewalls.

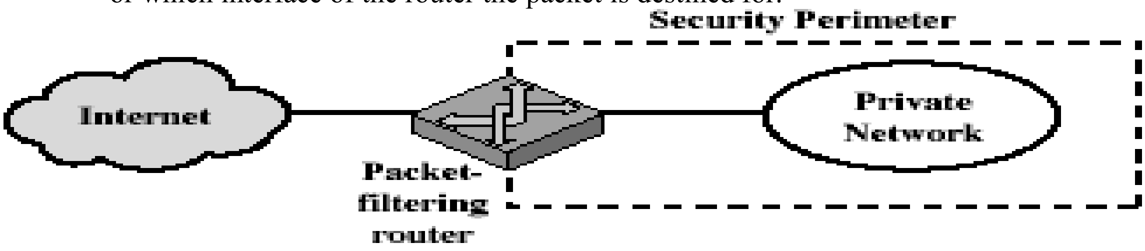
- ✓ Packet filters
- ✓ Application-level gateways
- ✓ Circuit-level gateways

Packet filtering router

A packet filtering router applies a set of rules to each incoming IP packet and then forwards or discards the packet. The router is typically configured to filter packets going in both directions. Filtering rules are based on the information contained in a network packet:

- ✓ Source IP address – IP address of the system that originated the IP packet.
- ✓ Destination IP address – IP address of the system, the IP is trying to reach.
- ✓ Source and destination transport level address – transport level port number.
- ✓ IP protocol field – defines the transport protocol.
- Interface – for a router with three or more ports, which interface of the router the packet come from

or which interface of the router the packet is destined for.



(a) Packet-filtering router

Two default policies are possible:

- Default = discard: That which is not expressly permitted is prohibited.
- Default = forward: That which is not expressly prohibited is permitted.

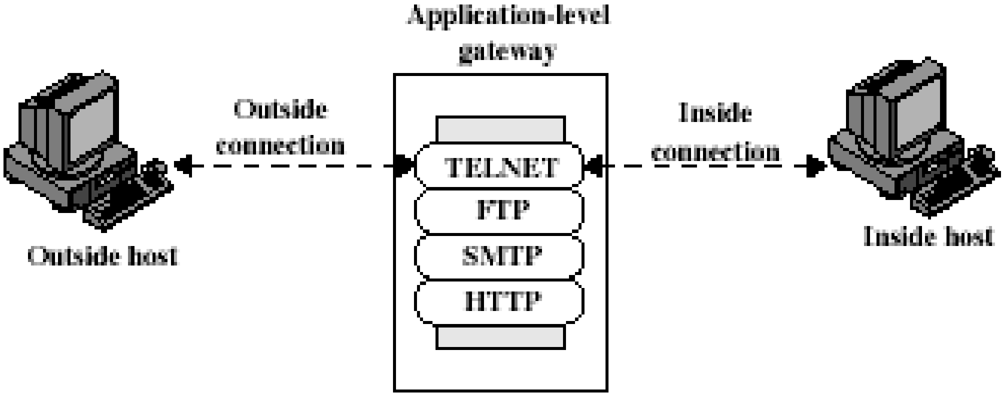
The default discard policy is the more conservative. Initially everything is blocked, and services must be added on a case-by-case basis. This policy is more visible to users, who are most likely to see the firewall as a hindrance. The default forward policy increases ease of use for end users but provides reduced security.

Advantages of packet filter router

- Simple
- Transparent to users
- Very fast

Application level gateway

An Application level gateway, also called a proxy server, acts as a relay of application level traffic. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.



(b) Application-level gateway

circuit-level gateways

As another simplistic firewall type that is meant to quickly and easily approve or deny traffic without consuming significant computing resources, circuit-level gateways work by verifying the transmission control protocol (TCP) handshake. This TCP handshake check is designed to make sure that the session the packet is from is legitimate.

While extremely resource-efficient, these firewalls do not check the packet itself. So, if a packet held malware, but had the right TCP handshake, it would pass right through. This is why circuit-level gateways are not enough to protect your business by themselves.

Basiton host

It is a system identified by the firewall administrator as a critical strong point in the networks security. The Bastion host serves as a platform for an application level and circuit level gateway.

Firewall configurations

1. Screened host firewall, single-homed bastion configuration
2. Screened host firewall, dual homed bastion configuration
3. Screened subnet firewall configuration

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: Cryptography and network security principles and practice ,William Stalling,5th edition
Page No:(622-624)

Course Teacher

Verified by HOD

LECTURE HANDOUTS

L-66

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **V - System Level Security, Malicious Software**

Date of Lecture:

Topic of Lecture: Firewall Configuration

Introduction : (Maximum 5 sentences)

- ✓ Just as a firewall in building attempts to prevent a fire from spreading, a computer firewall attempts to prevent computer viruses from spreading to your computer and to prevent unauthorized users from accessing your computer.
- ✓ A firewall exists between your computer and the network.

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- ✓ Service control
- ✓ Direction control
- ✓ User control
- ✓ Behavior control

Detailed content of the Lecture:

It determines which services on your computer remote users on the network can access. A properly configured firewall can greatly increase the security of your system. It is recommended that you configure a firewall for any Red Hat Enterprise Linux system with an Internet connection.

Security Level Configuration Tool

During the **Firewall Configuration** screen of the Red Hat Enterprise Linux installation, you were given the option to enable a basic firewall as well as to allow specific devices, incoming services, and ports.

- After installation, you can change this preference by using the **Security Level Configuration Tool**.
- To start the application, select **Main Menu Button** (on the Panel) => **System Settings** => **Security Level** or type the command system-config-securitylevel from a shell prompt (for example, in an **XTerm** or a **GNOME** terminal).

Enabling and Disabling the Firewall

Disable firewall — Disabling the firewall provides complete access to your system and does no security checking. Security checking is the disabling of access to certain services. This should only be selected if you are running on a trusted network (not the Internet) or plan to do more firewall configuration later.

Enable firewall — This option configures the system to reject incoming connections that are not in response to outbound requests, such as DNS replies or DHCP requests. If access to services running on this machine is needed, you can choose to allow specific services through the firewall.

Trusted Services

Enabling options in the **Trusted services** list allows the specified service to pass through the firewall.

WWW (HTTP)

The HTTP protocol is used by Apache (and by other Web servers) to serve web pages. If you plan on making your Web server publicly available, enable this option. This option is not required for viewing pages locally or for developing web pages.

FTP

The FTP protocol is used to transfer files between machines on a network. If you plan on making your FTP server publicly available, enable this option. The vsft pd package must be installed for this option to be useful.

SSH

Secure Shell (SSH) is a suite of tools for logging into and executing commands on a remote machine. To allow remote access to the machine via ssh, enable this option. The open ssh-server package must be installed to access your machine remotely using SSH tools.

Telnet

Telnet is a protocol for logging into remote machines. Telnet communications are unencrypted and provide no security from network snooping. Allowing incoming Telnet access is not recommended. To allow inbound Telnet access, you must have the telnet-server package installed.

Mail (SMTP)

To allow incoming mail delivery through your firewall so that remote hosts can connect directly to your machine to deliver mail, enable this option. You do not need to enable this if you collect your mail from your ISP's server using POP3 or IMAP, or if you use a tool such as fetch mail.

Trusted Devices

Selecting any of the **Trusted devices** allows access to your system for all traffic from that device; it becomes excluded from the firewall rules. For example, if you are running a local network, but are connected to the Internet via a PPP dialup, you can check **eth0** and any traffic coming from your local network is allowed. Selecting **eth0** as trusted means all traffic over the Ethernet is allowed, but the **ppp0** interface is still firewalled. To restrict traffic on an interface, leave it unchecked.

Video Content / Details of website for further learning (if any):
http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sag-en-4/ch-basic-firewall.html

Important Books/Journals for further learning including the page nos.:
Book: Cryptography and network security principles and practice ,William Stalling,5th edition
Page No:(622-624)

Course Teacher

Verified by HOD

LECTURE HANDOUTS

L-67

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **V - System Level Security, Malicious Software**

Date of Lecture:

Topic of Lecture: Viruses

Introduction : (Maximum 5 sentences)

- ✓ Perhaps the most sophisticated types of threats to computer systems are presented by programs that exploit vulnerabilities in computing systems

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Dormant phase
- ✓ Propagation phase
- ✓ Triggering phase
- ✓ Execution phase

Detailed content of the Lecture:

Perhaps the most sophisticated types of threats to computer systems are presented by programs that exploit vulnerabilities in computing systems

The Nature of Viruses

A virus is a piece of software that can "infect" other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs.

A virus can do anything that other programs do. The only difference is that it attaches itself to another program and executes secretly when the host program is run. Once a virus is executing, it can perform any function, such as erasing files and programs.

During its lifetime, a typical virus goes through the following four phases:

- **Dormant phase**: The virus is idle. The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have this stage.
- **Propagation phase:** The virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.
- **Triggering phase:** The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.
- **Execution phase:** The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

Virus Structure

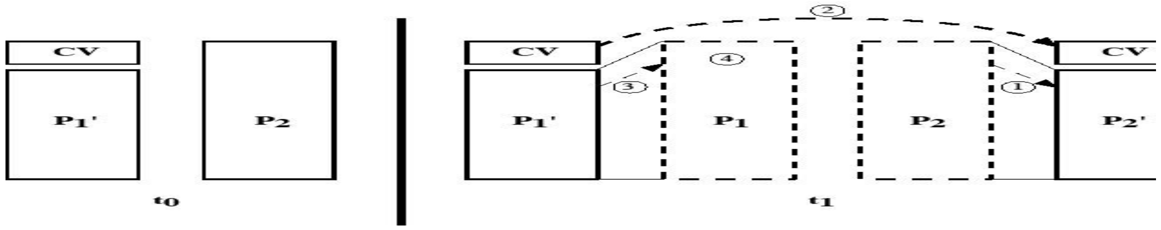
A virus can be prepended or post pended to an executable program, or it can be embedded in some other fashion. The key to its operation is that the infected program, when invoked, will first execute the virus code and then execute the original code of the program.

An infected program begins with the virus code and works as follows.

- The first line of code is a jump to the main virus program. The second line is a special marker that is used by the virus to determine whether or not a potential victim program has already been infected with this virus.
- When the program is invoked, control is immediately transferred to the main virus program. The virus program first seeks out uninfected executable files and infects them. Next, the virus may perform some action, usually detrimental to the system.
- This action could be performed every time the program is invoked, or it could be a logic bomb that triggers only under certain conditions.
- Finally, the virus transfers control to the original program. If the infection phase of the program is reasonably rapid, a user is unlikely to notice any difference between the execution of an infected and un infected program.

Program P_1 is infected with the virus CV. When this program is invoked, control passes to its virus, which performs the following steps:

1. For each uninfected file P_2 that is found, the virus first compresses that file to produce P'_2, which is shorter than the original program by the size of thevirus.
2. A copy of the virus is prepended to the compressedprogram.
3. The compressed version of the original infected program, P'_1, isuncompressed.
4. The uncompressed original program isexecuted.



Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: Cryptography and network security principles and practice ,William Stalling,5th edition ,Pg. No: R2(599-605)

Course Teacher

Verified by HOD

Estd. 2000

LECTURE HANDOUTS

L-68

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **V - System Level Security, Malicious Software**

Date of Lecture:

Topic of Lecture: Types of Viruses

Introduction : (Maximum 5 sentences)

- ✓ Perhaps the most sophisticated types of threats to computer systems are presented by programs that exploit vulnerabilities in computing systems

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Dormant phase
- ✓ Propagation phase
- ✓ Triggering phase
- ✓ Execution phase

Detailed content of the Lecture:

Types of Viruses

following categories as being among the most significant types of viruses:

- ➢ **Parasitic virus**: The traditional and still most common form of virus. A parasitic virus attaches itself to executable files and replicates, when the infected program is executed, by finding other executable files to infect.
- ➢ **Memory-resident virus**: Lodges in main memory as part of a resident system program. From that point on, the virus infects every program that executes.
- ➢ **Boot sector virus**: Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.
- ➢ **Stealth virus**: A form of virus explicitly designed to hide itself from detection by antivirus software.
- ➢ **Polymorphic virus**: A virus that mutates with every infection, making detection by the "signature" of the virus impossible.
- ➢ **Metamorphic virus**: As with a polymorphic virus, a metamorphic virus mutates with every infection. The difference is that a metamorphic virus rewrites itself completely at each iteration, increasing the difficulty of detection. Metamorphic viruses my change their behavior as well as their appearance

E-mail Viruses

A more recent development in malicious software is the e-mail virus.

- The first rapidly spreading e-mail viruses, such as Melissa, made use of a Microsoft Word macro embedded in an attachment. If the recipient opens the e-mail attachment, the Word macro is activated.
- Then, the e-mail virus sends itself to everyone on the mailing list in the user's e-mail package.

The virus does local damage

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: Cryptography and network security principles and practice ,William Stalling,5th edition
Page No: R2(599-605)

Course Teacher

Verified by HOD

Estd. 2000

LECTURE HANDOUTS

L-69

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **V - System Level Security, Malicious Software**

Date of Lecture:

Topic of Lecture: Virus Counter Measures

Introduction : (Maximum 5 sentences)

- ✓ The ideal solution to the threat of viruses is prevention: Do not allow a virus to get into the system in the first place, or block the ability of a virus to modify any files containing executable code or macros.

Prerequisite knowledge for Complete understanding and learning of Topic:

- ✓ Dormant phase
- ✓ Propagation phase
- ✓ Triggering phase
- ✓ Execution phase

Detailed content of the Lecture:

This goal is, in general, impossible to achieve,although prevention can reduce the number of successful viral attacks.

The next best approach is to be able to do the following:

• **Detection:** Once the infection has occurred, determine that it has occurred and locate the virus.

• **Identification:** Once detection has been achieved, identify the specific virus that has infected a program.

• **Removal:** Once the specific virus has been identified, remove all traces of theVirus from the infected program and

Restore it to its original state. Remove thevirus from all infected system so that the virus cannot spread further.

If detection succeeds but either identification or removal is not possible, then the alternative is to discard the infected file and reload a clean backup version.

Advances in virus and antivirus technology go hand in hand. Early viruses were relatively simple code fragments and could be identified and purged with relatively simple antivirus software packages.

As the virus arms race has evolved, both viruses and, necessarily, antivirus software have grown more complex and sophisticated.

identifies four generations of antivirus software:

• First generation: simple scanners

• Second generation: heuristic scanners

• Third generation: activity traps

• Fourth generation: full-featured protection

Advanced Antivirus Techniques

More sophisticated antivirus approaches and products continue to appear. In this subsection, we highlight some of the most important.

Video Content / Details of website for further learning (if any):
http://www.brainkart.com/article/Computer-Virus-Countermeasures_8508/

Important Books/Journals for further learning including the page nos.:
Book: Cryptography and network security principles and practice ,William Stalling,5th edition
Page No: R2(599-605)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L-70

LECTURE HANDOUTS

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **V - System Level Security, Malicious Software**

Date of Lecture:

Topic of Lecture: Security Standards

Introduction : (Maximum 5 sentences)

- All Firewall implementations should adopt the principal of "least privilege" and deny all inbound traffic by default.
- The Rule set should be opened incrementally to only allow permissible traffic. This is done by the ISO for all ITS managed firewall infrastructure.

Prerequisite knowledge for Complete understanding and learning of Topic:

✓ Security standards ISO

Detailed content of the Lecture:

All Firewall implementations should adopt the principal of "least privilege" and deny all inbound traffic by default.

The Ruleset should be opened incrementally to only allow permissible traffic. This is done by the ISO for ITS entire managed firewall infrastructure.

Standard number/name	Description/Benefits	Published by
BS ISO/IEC 27033-1 Network security. Overview and concepts	Provides a comprehensive overview of network security issues and technologies for planning purposes	BSI
BS ISO/IEC 27033-2 Guidelines for the design and implementation of network security	Can help define network security requirements	BSI
BS ISO/IEC 27033-3 Network security. Reference networking scenarios. Threats, design techniques and control issues	Identifies threats, design techniques and control issues associated with various types of network.	BSI
BS ISO/IEC 27033-4, Securing communications between networks using security gateways	Gives detailed technical guidance for securing communications between networks using security gateways. Describes different types of firewalls and other gateway security devices such as routers and Intrusion Protection Systems.	BSI

BS ISO/IEC 27033-5, Securing communications across networks using Virtual Private Networks (VPNs)	Provides detailed technical guidance for securing network interconnections and connecting remote users to networks by use of Virtual Private Networks.	BSI
NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*	Provides practical guidance on developing firewall policies and selecting, configuring, testing, deploying and managing firewalls. This is a free special publication from the US National Institute of Standards and Technology	US National Institute of Standards and Technology
NIST SP 800-46, *Guide to Enterprise Telework and Remote Access Security*	Provides recommendations for securing remote access to both clients and servers. This is a free special publication from the US National Institute of Standards and Technology	US National Institute of Standards and Technology
NIST Special guides	There are a number of further specialist guides available from NIST.	US National Institute of Standards and Technology
PCI-DDS supplement	The PCI Security Standards Council has a useful supplement its PCI-DSS standard that deals with using firewalls to protect web applications.	PCI Security Standards Council

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book: Cryptography and network security principles and practice ,William Stalling,5th edition
Page No:(544-558)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

L-71

CSE

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **V - System Level Security, Malicious Software**

Date of Lecture:

Topic of Lecture: Malicious software : Types of Malicious software

Introduction : (Maximum 5 sentences)

- **Malicious software**, commonly known as **malware**, is any **software** that brings harm to a computer system.
- **Malware** can be in the form of worms, viruses, trojans, spyware, adware and root kits, etc., which steal protected data, delete documents or add **software** not approved by a user

Prerequisite knowledge for Complete understanding and learning of Topic:

- Viruses
- Firewalls

Detailed content of the Lecture:

- **Malicious software**, commonly known as **malware**, is any **software** that brings harm to a computer system.
- **Malware** can be in the form of worms, viruses, trojans, spyware, adware and root kits, etc., which steal protected data, delete documents or add **software** not approved by a user
- Malware is software designed to cause harm to a computer and user. Some forms of malware “spy” on user Internet traffic. Examples include spyware and adware.
- Spyware monitors a user’s location and if enabled, it can capture sensitive information, e.g., credit card numbers, promoting identity theft.
- Adware also acquires user information, which is shared with advertisers and then integrated with unwanted, triggered pop-up ads.
- Worms and viruses behave differently, as they can quickly proliferate and undermine an entire computer system.
- They also may perform unsavory activities from a user’s computer without the user’s knowledge. In the wake of a virus or worm, a computer system can experience significant damage.
- Anti-malware should determine if there are threats by scanning a computer and removing them, if found. Prevention is better than corrective action after infection.
- Although anti-virus programs should be continually enabled and updated, certain types of threats, like spyware, often make their way into a computer system.
- At all times, a firewall should be in place for additional security. Multiple, compatible protective sources are encouraged as additional insurance against malware.

Malicious software can be divided into two categories:

Those that need a host program, and those that are independent.

- The former are essentially fragments of programs that cannot exist independently of some actual application program, utility, or system program.

- Viruses, logic bombs, and backdoors are examples. The latter are self-contained programs that can be scheduled and run by the operating system.

  Worms and zombie programs are examples

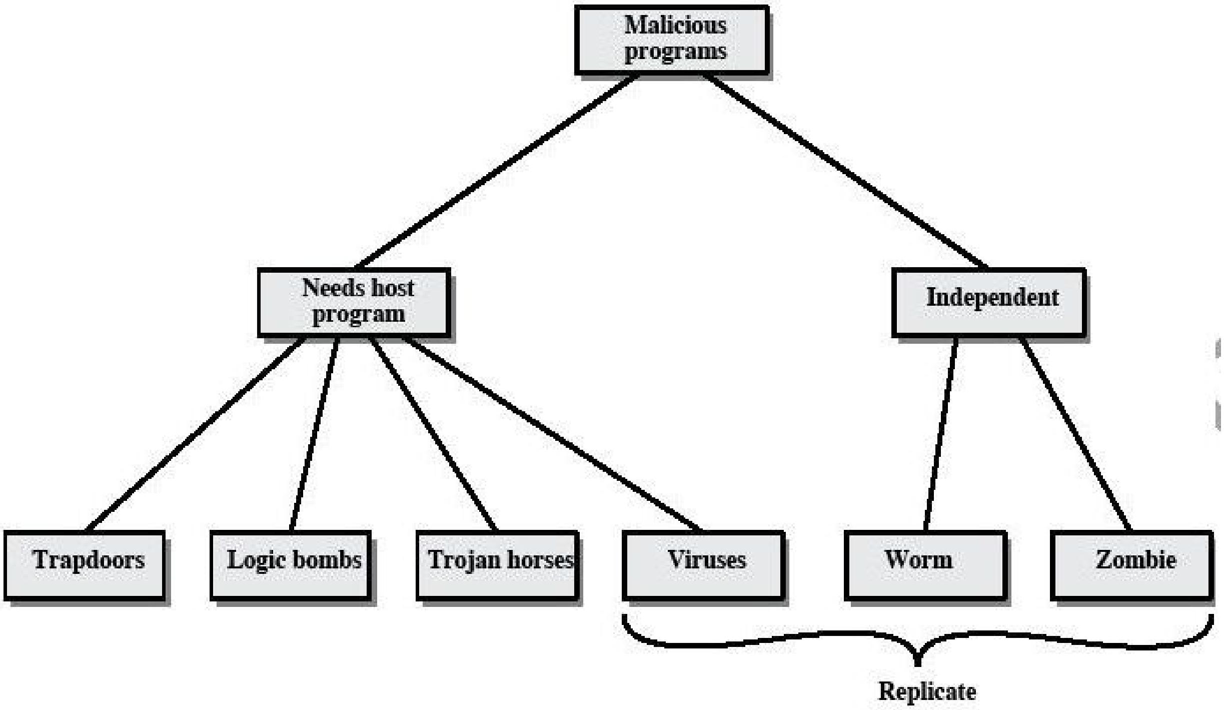


Figure 19.1 Taxonomy of Malicious Programs

Name	**Description**
Virus	Attaches itself to a program and propagates copies of itself to other Programs
Worm	Program that propagates copies of itself to other computers
Logic bomb	Triggers action when condition occurs
Trojan horse	Program that contains unexpected additional functionality
Backdoor (trapdoor)	Program modification that allows unauthorized access to functionality
Exploits	Code specific to a single vulnerability or set of vulnerabilities
Downloaders	Program that installs other items on a machine that is under attack. Usually, a downloader is sent in an e-mail.
Auto-rooter	Malicious hacker tools used to break into new machines remotely
Kit (virus generator)	Set of tools for generating new viruses automatically
Spammer programs	Used to send large volumes of unwanted e-mail

Flooders	Used to attack networked computer systems with a large volume of traffic to carry out a denial of service (DoS) attack
Keyloggers	Captures keystrokes on a compromised system
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access
Zombie	Program activated on an infected machine that is activated to launch attacks on other machines

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/malwares-malicious-software/

Important Books/Journals for further learning including the page nos.:
Book:
Cryptography and network security principles and practice ,William Stalling,5th edition
Page No:(605-607)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

L-72

CSE

III/V

Course Name with Code : Cryptography and Network Security/16CSD09

Course Teacher :

Unit : V - System Level Security, Malicious Software

Date of Lecture:

Topic of Lecture: Worms

Introduction : (Maximum 5 sentences)

- ✓ A worm is a program that can replicate itself and send copies from computer to computer across network connections.
- ✓ Upon arrival, the worm may be activated to replicate and propagate again.
- ✓ Network worm programs use network connections to spread from system to system.
- ✓ Once active within a system, a network worm can behave as a computer virus or bacteria, or it could implant Trojan horse programs or perform any number of disruptive or destructive actions

Prerequisite knowledge for Complete understanding and learning of Topic:

- Electronic mail facility
- Remote execution capability
- Remote login capability

Detailed content of the Lecture:

- A worm is a program that can replicate itself and send copies from computer to computer across network connections.
- Upon arrival, the worm may be activated to replicate and propagate again. Network worm programs use network connections to spread from system to system.
- Once active within a system, a network worm can behave as a computer virus or bacteria, or it could implant Trojan horse programs or perform any number of disruptive or destructive actions
  - Electronic mail facility: A worm mails a copy of itself to other systems.
  - Remote execution capability: A worm executes a copy of itself on another system.
  - Remote login capability: A worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other.

The new copy of the worm program is then run on the remote system where, in addition to any functions that it performs at that system, it continues to spread in the same fashion.

A network worm exhibits the same characteristics as a computer virus: a dormant phase, a propagation phase, a triggering phase, and an execution phase. The propagation phase generally performs the following functions:

1. Search for other systems to infect by examining host tables or similar repositories of remote system addresses.
2. Establish a connection with a remote system.
3. Copy itself to the remote system and cause the copy to berun.

As with viruses, network worms are difficult to counter

The Morris Worm

The Morris worm was designed to spread on UNIX systems and used a number of different techniques for propagation.

4. It attempted to log on to a remote host as a legitimate user. In this method, the worm first

attempted to crack the local password file, and then used the discovered passwords and corresponding user IDs. The assumption was that many users would use the same password on different systems. To obtain the passwords, the worm ran a password- cracking program that tried

Each user's account name and simple permutations of it

A list of 432 built-in passwords that Morris thought to be likely candidates All

the words in the local system directory

5. It exploited a bug in the finger protocol, which reports the whereabouts of a remote user.

6. It exploited a trapdoor in the debug option of the remote process that receives and sends mail.
If any of these attacks succeeded, the worm achieved communication with the operating system command interpreter.

Recent Worm Attacks

In late 2001, a more versatile worm appeared, known as Nimda. Nimda spreads by multiple mechanisms:

- from client to client via e-mail
- from client to client via open network shares
- from Web server to client via browsing of compromised Websites
- from client to Web server via active scanning for and exploitation of various Microsoft IIS 4.0 / 5.0 directory traversal vulnerabilities
- from client to Web server via scanning for the back doors left behind by the "Code Red II"worms

The worm modifies Web documents (e.g., .htm, .html, and .asp files) and certain executable files found on the systems it infects and creates numerous copies of itself under various filenames.

In early 2003, the SQL Slammer worm appeared. This worm exploited a buffer overflow vulnerability in Microsoft SQL server.

Video Content / Details of website for further learning (if any):
WilliamStallings.com/Crypto/Crypto4e.html

Important Books/Journals for further learning including the page nos.:
Book:
Cryptography and network security principles and practice ,William Stalling,5th edition Page No: R2(607-609)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

DESIGNING YOUR FUTURE
Estd. 2000

IQAC

LECTURE HANDOUTS

L-73

CSE

III/V

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **V - System Level Security, Malicious Software**

Date of Lecture:

Topic of Lecture: Virus &Worms	
Introduction : (Maximum 5 sentences) ✓ A worm is a program that can replicate itself and send copies from computer to computer across network connections. ✓ Upon arrival, the worm may be activated to replicate and propagate again.	
Prerequisite knowledge for Complete understanding and learning of Topic: • Electronic mail facility • Remote execution capability • Remote login capability	

Detailed content of the Lecture:

Virus: Small pieces of software that attach themselves to real programs.

- The term "virus" is also commonly but erroneously used to refer to other types of malware, adware, and spyware programs that do not have the reproductive ability.
- A true virus can spread from one computer to another (in some form of executable code).
- Viruses can increase their chances of spreading on to other computers by infecting files on a network file system or a file system that is accessed by another computer.
- Viruses always mostly corrupt or modify system files on the targeted computer.

Worm: A self-replicating program

- The major difference between a virus and a worm is that worm does not attach itself to other existing program as viruses do .
- Worms spread across networks due to poor security of the infected computers.
- As this type of infection runs by itself it can have devastating impacts.
- **Worm Viruses Include:** lov gate .F, so big.D ,trile. C

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/worms-viruses-and-beyond/?ref=lbp

Important Books/Journals for further learning including the page nos.:
Book:
Cryptography and network security principles and practice ,William Stalling,5th edition Page No: R2(607-609)

Course Teacher

Verified by HOD

Course Name with Code : **Cryptography and Network Security/16CSD09**

Course Teacher :

Unit : **V - System Level Security, Malicious Software**

Date of Lecture:

Topic of Lecture: Advantage of Anti-Virus

Introduction : (Maximum 5 sentences)

- A virus is a piece of software that can "infect" other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs.
- A virus can do anything that other programs do.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Electronic mail facility
- Remote execution capability
- Remote login capability

Detailed content of the Lecture:

Advanced Antivirus Techniques

More sophisticated antivirus approaches and products continue to appear. In this subsection, we highlight some of the most important.

GENERIC DECRYPTION

Generic decryption (GD) technology enables the antivirus program to easily detect even the most complex polymorphic viruses while maintaining fast scanning speeds.

Recall that when a file containing a polymorphic virus is executed, the virus must decrypt itself to activate.

CPU Emulator:

A software-based virtual computer. Instructions in an exe- cutable file are interpreted by the emulator rather than executed on the underlying processor.

Virus signature scanner:

A module that scans the target code looking for known virus signatures.

Emulation control module:

Controls the execution of the target code.

DIGITAL IMMUNE SYSTEM

The digital immune system is a comprehensive approach to virus protection developed by IBM [KEPH97a, KEPH97b, WHIT99] and subsequently refined by Symantec [SYMA01].

The motivation for this development has been the rising threat of Internet-based virus propagation. We first say a few words about this threat and then summarize IBM's approach.

Integrated mail systems:

Systems such as Lotus Notes and Microsoft Outlook make it very simple to send anything to anyone and to work with objects that are received.

Mobile-program systems:

Capabilities such as Java and ActiveX allow programs to move on their own from one system to another.

Video Content / Details of website for further learning (if any):
http://www.brainkart.com/article/Computer-Virus-Countermeasures_8508/

Important Books/Journals for further learning including the page nos.:
Book:
Cryptography and network security principles and practice ,William Stalling,5th edition Page No: R2(607-609)

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L-75

Course Name with Code **: Cryptography and Network Security/16CSD09**

Course Teacher **:**

Unit **: V - System Level Security, Malicious Software**

Date of Lecture:

Topic of Lecture: Behavior Blocking Software

Introduction : (Maximum 5 sentences)

- **Behavior-blocking software** integrates with the operating system of a host computer and monitors program **behavior** in real-time for malicious actions.
- The **behavior blocking software** then blocks potentially malicious actions before they have a chance to affect the system.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Worms
- Virus

Detailed content of the Lecture:

Behavior-blocking software integrates with the operating system of a host computer and monitors program **behavior** in real-time for malicious actions. The **behavior blocking software** then blocks potentially malicious actions before they have a chance to affect the system.

- Behavior Monitoring may Include
- Attempt to open ,view or delete / modify system files
- Attempt to format disk drives
- Modifying logic of executables files
- Scripting of e-mail and instant messaging clients to send executable content.
- Initiating network communications.
- If the behavior blocker,detects program initiation is malicious, it can block the behaviors and terminate the response

Video Content / Details of website for further learning (if any):
http://www.faadooengineers.com/online-study/post/cse/cryptography/4/behavior-blocking-software

Important Books/Journals for further learning including the page nos.:
Book: Cryptography and network security principles and practice ,William Stalling,5th edition Page No: R2(607-609)

Course Teacher

Verified by HOD