--- (Cryptography & System Security) ---

#	Chapters	Page No.	Weightage (Avg. Marks)
1.	Introduction	01	9
2.	Basics of Cryptography	11	8
3.	Secret Key Cryptography	21	17
4.	Public Key Cryptography	39	17
5.	Cryptographic Hash Functions	54	13
6.	Authentication Applications	65	14
7.	Security & Firewalls	79	21
8.	IP Security	96	30
9.	Miscellaneous	124	5

--- Marks Distribution ---

#	DEC-15	MAY-16	DEC-16	MAY-17	DEC-17	MAY-18
1.	10	05	-	-	-	10
2.	10	05	10	05	10	-
3.	15	15	20	15	20	15
4.	20	15	20	30	10	10
5.	05	10	15	15	10	25
6.	10	15	05	10	20	25
7.	15	20	35	10	30	15
8.	40	40	20	35	25	20
9.	-	-	-	05	-	-
-	-	25	60	40	50	50

Cryptography & System Security Semester - 7 Topper's Solutions

--- Analysis by Topper's Solutions Team ---

LAST MINUTE PREPARATION:

Engineering is a notoriously demanding field of study. Being successful in engineering exams requires a **systematic and focused approach**. In order to do well, you will need to learn how to prepare for semester exam in engineering. Have you have already given up thinking, **"What the hell I can do at this moment? Tomorrow is exam!"** Think again! You are engineering student & last night studies are every engineering student's epitome.

"We engineers are known for our creativity"

Don't Worry entire **Topper's Solutions Team** is working out for betterment of students. Here are some techniques about **Cryptography & System Security (CSS)** Subject.

- **How to score first 50 marks:**

Study **any one** of the below set and make sure you can easily attempt any questions from below chapters included in particular set.

SET - 1

#	Chapter Name	Weightage (Marks)
8	IP Security	30
7	Security & Firewalls	21
3	Secret Key Cryptography	17
4	Public Key Cryptography	17

OR

SET - 2

#	Chapter Name	Weightage (Marks)
8	IP Security	30
7	Security & Firewalls	21
5	Cryptographic Hash Functions	13
6	Authentication Applications	14

➢ **How to score next 20 marks:**

Study the following 3 chapters.

#	Chapter Name	Weightage (Marks)
1	Introduction	9
2	Basics of Cryptography	8
3/5	Secret Key Cryptography/Cryptographic Hash Functions	17 / 13

Note: If you want to score good marks, study **ALL Chapters.**

Please Note: The Above Analysis is suggest by Topper's Solutions Team. Don't be completely dependent on it. It may change as per University of Mumbai Guidelines.

Contact No: 7507531198

Email ID: Support@ToppersSolutions.com

Website: www.ToppersSolutions.com

CHAPTER - 1: INTRODUCTION

Qt] Operating System Security.

Ans: **[5M – Dec15]**

SECURITY:

1. Security refers to providing a **protection system** to computer system resources.
2. Resources can be a CPU, memory, disk, software programs and most importantly data/information stored in the computer system.

OS SECURITY:

1. Operating System Security (OS security) is the process of ensuring **OS integrity, confidentiality and availability.**
2. If a computer program is run by an unauthorized user, then he/she may cause severe damage to computer or data stored in it.
3. So a computer system must be protected against unauthorized access, threats, viruses, worms and malwares.

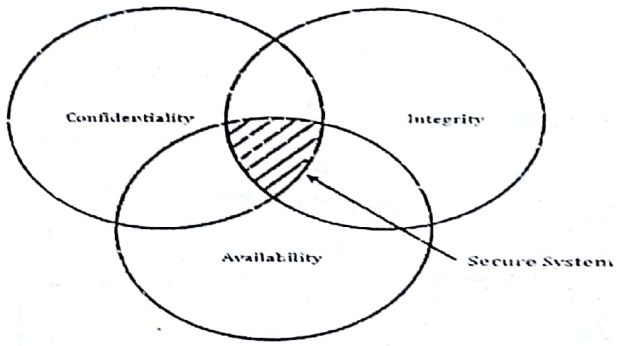


Figure 1.1: OS Security.

GOALS OF OS SECURITY:

I) Confidentiality:

- It is the best security policy.
- It assures that data is accessed by authorized user only.

II) Integrity:

- It ensures that the data received by the receiver is exactly same as the data send by sender.
- The data should not be modified by any unauthorized entity.

III) Availability:

- It ensures that the data is always accessible/ available to authorized persons.
- Whenever an authorized system entity demands for system resource, it must be accessible and usable at all times by him/her.

Q2] Define the goals of security and specify mechanisms to archive each goal.

Q3] List with example the different mechanisms to achieve security.

Ans: **[Q2 | 5M – Dec15] & [Q3 | 5M – May16]**

Note: For Q3) Refer only Security Mechanism Part.

SECURITY GOALS:

I) **Confidentiality:**

- It is the best security policy.
- Confidentiality assures that **data is accessed by authorized user only.**
- No unauthorized party can have access to the data.
- Accessing data means to read, to print or just to know the existence of data.
- It is also called as secrecy or privacy.
- Confidentially can be achieved by means of encryption, so that even third party gets access to the message, they cannot reveal the exact meaning of that message.
- **Example:** Figure 1.2 shows the example of Confidentiality. Consider that A & B wants to communicate with each other. When A sends a message "m" to B, only B should receive it. Only then confidentially is maintained.

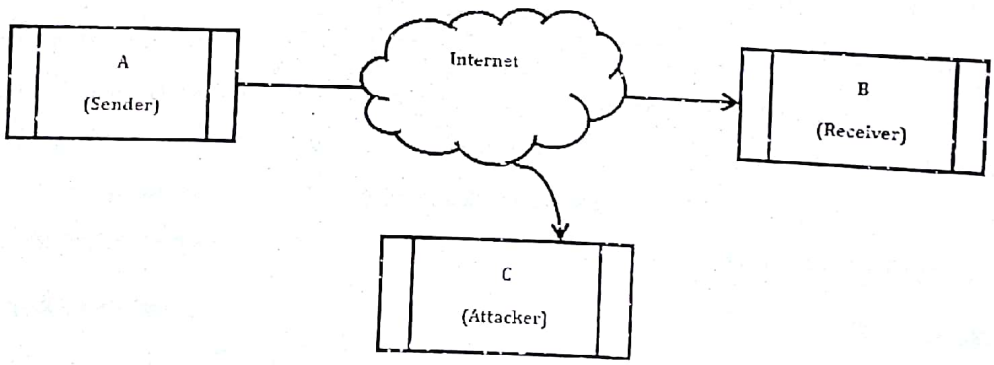


Figure 1.2: Example of Confidentiality.

II) Integrity:

- Integrity ensures that the data received by the receiver is exactly same as the data send by sender.
- The data should not be modified by any unauthorized entity.
- Only authorized entity or person should be able to modify or update the data.
- Modification means modification of data through insertion, deletion or replay of data.
- Integrity can be achieved by using checksum or hashing methods such as MD5, SHA-1 & Tiger Hash.

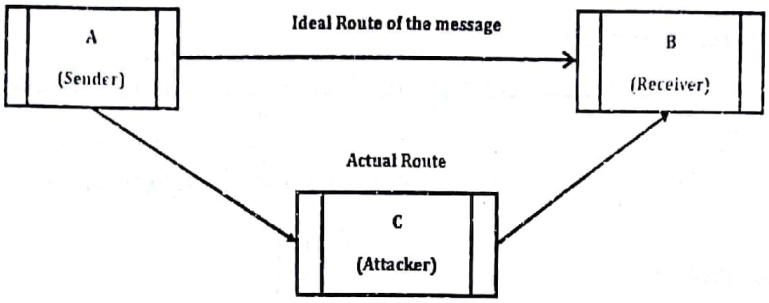


Figure 1.3: Example of Integrity.

III) Availability:

- It ensures that the data is always accessible/ available to authorized persons.
- Whenever an authorized system entity demands for system resource, it must be accessible and usable at all times by him/her.
- The information created and stored by an organization needs to be available to authorized entities. Information is useless if it is not available.
- **Example:** The situation can be difficult for a bank if the customer could not access their accounts for transactions. Interruption puts the availability of resources in danger.

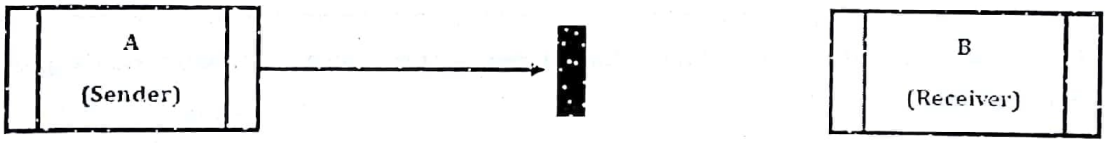


Figure 1.4: Example of Availability.

SECURITY MECHANISMS:

I) Encipherment:

- This is hiding or covering of data which provides confidentiality.
- It is also used to complement other mechanisms to provide other services.
- Cryptography and Steganography are used for enciphering.

II) Digital Integrity:

- The data integrity mechanism appends a short check value to the data that has been created by a specific process from the data itself.
- Data integrity is preserved by comparing check value received to the check value generated.

III) Digital Signature:

- A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.
- Public and private keys can be used.

IV) **Authentication Exchange:**

- In this two entities exchange some messages to prove their identity to each other.

V) **Traffic Padding:**

- Traffic padding means inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis.

VI) **Routing Control:**

- Routing control means selecting and continuously changing different available routes between sender and receiver to prevent the opponent from eavesdropping on a particular route.

VII) **Notarization:**

- Notarization means selecting a third trusted party to control the communication between two entities.
- The receiver can involve a trusted third party to store the sender request in order to prevent the sender from later denying that she has made a request.

VIII) **Access Control:**

- Access control used methods to prove that a user has access right to the data or resources owned by a system.
- Examples of proofs are passwords and PINs.

Q4] Give examples of replay attacks. List three general approaches for dealing with replay attacks

Ans:

[5M – May18]

REPLAY ATTACKS:

1. Replay attack is also knows as **playback attack.**
2. It is type of **active security attack.**
3. Replay attacks are the network attacks in which an attacker spies the conversation between the sender and receiver and takes the authenticated information e.g. sharing key and then contact to the receiver with that key.
4. In replay attack, the attacker gives the proof of his **identity and authenticity.**
5. Replay attack is one of the lower tier versions of a **"Man in the middle attack"**
6. in Replay Attack, an attacker captures the data and retransmits it after some delay as shown in Figure 1.5.

EXAMPLE:

- A sends Rs. 1, 00,000 to B Through an online transmission.
- An Attacker captures this data and sends it again after some time to produce unauthorized effects.

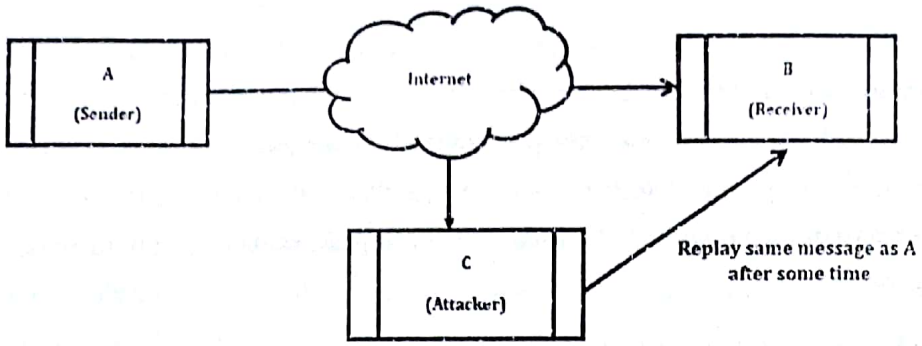


Figure 1.5: Example of Replay Attack.

GENERAL APPROACHES FOR DEALING WITH REPLAY ATTACKS:

I) **Attach a sequence number to each message used in an authentication exchange:**

- A new message is accepted only if its sequence number is in the proper order.
- Difficulty with this approach is that it requires each party to keep track of the last sequence number for each claimant it has dealt with.
- Generally not used for authentication and key exchange because of overhead.

II) **Timestamps:**

- Requires that clocks among the various participants be synchronized.
- Party A accepts a message as fresh only if the message contains a timestamp that, in A's judgment, is close enough to A's knowledge of current time.

III) **Challenge/response:**

- Party A, expecting a fresh message from B, first sends B a nonce (challenge) and requires that the subsequent message (response) received from B contain the correct nonce value.

Q5] List and explain various types of attacks on encrypted message

Ans: [5M -- May18]

CRYPTOGRAPHIC ATTACKS:

1. Attack is the action which **exploits the vulnerability of system.**
2. In cryptographic attacks the basic intention of an attacker is to break a cryptosystem and to find the plaintext from the ciphertext.
3. To obtain the plaintext, the attacker only needs to find out the secret decryption key, as the algorithm is already in public domain.
4. Hence, attacker applies maximum effort towards finding out the secret key used in the cryptosystem.
5. Once the attacker is able to determine the key, the attacked system is considered as broken or compromised.

TYPES:

I) **Ciphertext Only Attack (COA):**

- In this method, the attacker has access to a set of ciphertext(s).
- Attacker does not have access to corresponding plaintext.
- COA is said to be successful when the corresponding plaintext can be determined from a given set of ciphertext.

II) **Known Plaintext Attack (KPA):**

- In this method, the attacker knows the plaintext for some parts of the ciphertext.
- The task is to decrypt the rest of the ciphertext using this information.
- This may be done by determining the key or via some other method.
- The best example of this attack is **linear cryptanalysis against block ciphers.**

III) **Chosen Plaintext Attack (CPA):**

- In this method, the attacker has the text of his choice encrypted.
- So attacker has the ciphertext-plaintext pair of his choice.
- This simplifies his task of determining the encryption key.
- An example of this attack is differential cryptanalysis applied against block ciphers as well as hash functions.

IV) **Dictionary Attack:**

- This attack has many variants, all of which involve compiling a 'dictionary'.
- In simplest method of this attack, attacker builds a dictionary of cipher texts and corresponding plaintexts that he has learnt over a period of time.
- In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext.

V) **Brute Force Attack (BFA):**

- In this method, the attacker tries to determine the key by attempting all possible keys.
- If the key is 8 bits long, then the number of possible keys is 28 = 256.
- The attacker knows the ciphertext and the algorithm, now he attempts all the 256 keys one by one for decryption.
- The time to complete the attack would be very high if the key is long.

VI) **Birthday Attack:**

- A birthday attack is a class of brute force attack used against hashing functions.
- It is based on the "**birthday paradox**"
- This states that in a group of 23 people, there is at least a 50% probability that at least two people will share the same birthday.
- In a group of 60 people, the probability is over 99%.

VII) **Man in Middle Attack (MIM):**

- The targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place.
- Host A wants to communicate to host B, hence requests public key of B.
- An attacker intercepts this request and sends his public key instead.
- Thus, whatever host A sends to host B, the attacker is able to read.
- In order to maintain communication, the attacker re-encrypts the data after reading with his public key and sends to B.
- The attacker sends his public key as A's public key so that B takes it as if it is taking it from A.

VIII) **Side Channel Attack (SCA):**

- Side channel attack is used to exploit the weakness in physical implementation of the cryptosystem.
- Side channel attacks are a type of attacks based on implementation details such as **timing, power, and radiation emissions.**
- By carefully measuring the amount of time required to perform private key operations, attackers may be able to find fixed Diffie-Hellman exponents, factor RSA keys, and break other cryptosystems.

IX) **Timing Attacks:**

- Timing attack exploit the fact that different computations take different times to compute on processor.
- By measuring such timings, it is be possible to know about a particular computation the processor is carrying out.
- For example, if the encryption takes a longer time, it indicates that the secret key is long.

X) **Power Analysis Attacks:**

- These attacks are similar to timing attacks except that the amount of power consumption is used to obtain information about the nature of the underlying computations.

XI) **Fault analysis Attacks:**

- In these attacks, errors are induced in the cryptosystem and the attacker studies the resulting output for useful information.

--- EXTRA QUESTIONS ---

Q1] **Security Attacks.**

Ans:

SECURITY ATTACKS:

1. Attack is the action which **exploits the vulnerability of system.**
2. Security **Attack** is a method or technique that violates security policy of a system or organization.
3. While transferring an information, attack may occur.
4. This attack may be either active or passive.

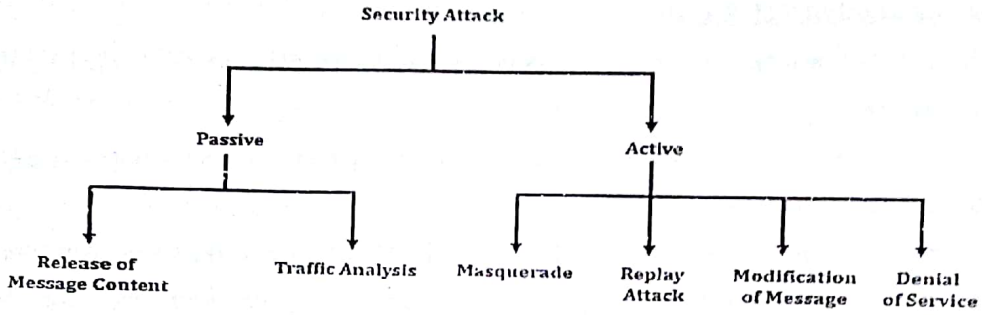


Figure 1.6: Types of Attacks.

PASSIVE ATTACK:

1. In Passive Attack, an attacker just obtains an information being transmitted.
2. It does not alter the message.

I) **Release of Message Content:**

- This Attack discloses the message information.
- It may happen through various ways such as: Listening to telephone conversation, accessing e-mails or observing a transferred file which may contain sensitive information.

II) **Traffic Analysis:**

- In Traffic Analysis, an attacker observes the network traffic and tries to analyze the nature of communication.
- Encryption technique is used to prevent Traffic Analysis.

ACTIVE ATTACK:

Active Attack is an Attack that modifies the original Message.

i) **Masquerade:**

- This attack occurs when unauthorized entity pretends to be an authorized entity.
- That is an attacker takes an identity of someone and acts on behalf of them without their knowledge.

- **Phishing** is one of the variation of masquerade.

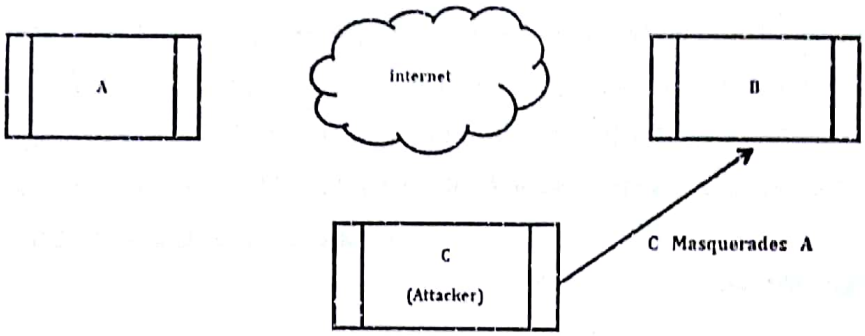


Figure 1.7: Example of Masquerade.

II) Replay Attack:

- In Replay Attack, an attacker captures the data and retransmits it after some delay as shown in Figure 1.8.
- **Example:** A sends Rs. 1, 00,000 to B Through an online transmission.
- An Attacker captures this data and sends it again after some time to produce unauthorized effects.

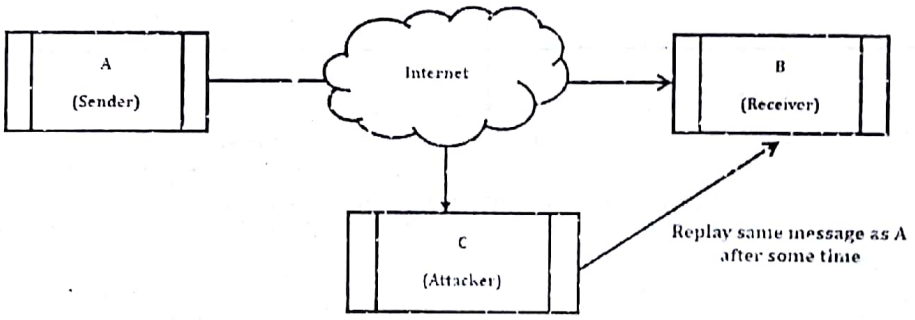


Figure 1.8: Example of Replay Attack.

III) Modification of Messages:

- In this technique, an attacker tries to modify the message.
- This modification may be in terms of message alteration, delay or reordering.
- **Example:** If the original message is Transfer Rs. 1, 00,000 from A to B, it may be modified to Transfer Rs. 1, 00,000 from A to C.

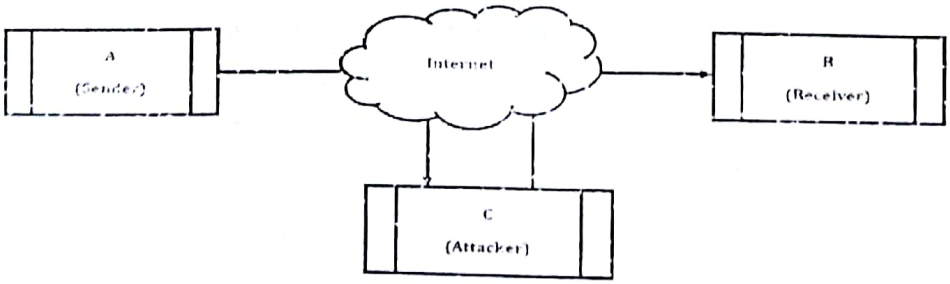


Figure 1.9: Modification of Message.

IV) **Denial of Service (DoS):**

- Denial of Service (DoS) is also known as **Availability Attack.**
- It prevents authorized users from getting access to system communication facilities or resources.
- It may disrupt the network either by disabling the network or by overloading it with message.
- Active Attacks are easy to detect but difficult to prevent.

Q2] **Security Services**

Ans:

SECURITY SERVICES:

1. Security service is a service that enhances the security of the system or data transfer.
2. They are intended to counter Security Attacks.
3. Security Services make use of one or more security mechanisms to provide the service.
4. Figure 1.10 shows the Categories of Security Services.

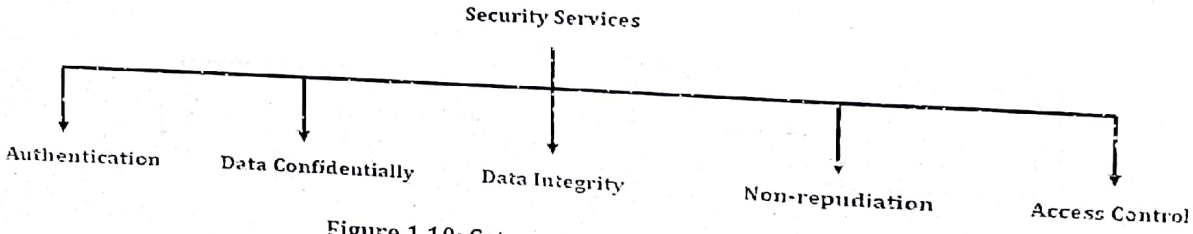


Figure 1.10: Categories of Security Services.

I) **Authentication:**

- It ensures that the communicating entity is the one claimed.

II) **Data Confidentially:**

- It protects the data from unauthorized disclosure.

III) **Data Integrity:**

- It assures that data received is as sent by an authorized entity.

IV) **Non-Repudiation:**

- It protects against Denial by one of the parties in a communication.

V) **Access Control:**

- It prevents from authorized use of a resources

CHAPTER - 2: BASIC OF CRYPTOGRAPHY

Q1] Define the following examples:

(i) Substitution cipher.

(ii) Poly-alphabetic cipher.

Q2] With the help of suitable examples compare and contrast monoalphabetic ciphers and polyalphabetic ciphers?

Ans: **[Q1 | 5M – Dec15] & [Q2 | 5M – Dec17]**

SUBSTITUTION CIPHER:

1. Substitution cipher is a method of **encoding** by which units of plaintext are replaced with cipher text, according to a fixed system.
2. The "units" may be single letters, pairs of letters, and triplets of letters or mixtures of the above.
3. The receiver deciphers the text by performing the **inverse substitution.**
4. In short, in Substitution, one symbol/letter is replaced by another.
5. Substitution Cipher can be divided as:

I) Monoalphabetic Cipher:

- A character in plain text is always changed to the same character in the cipher text regardless of its position.
- Example of this is the **Ceaser Cipher** which involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

Plain Text	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
Cipher Text	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

Plain Text: ViVA Institute of Technology

Cipher Text: YLYD LQVWLWXWH RI WHFKQRORJB

II) Polyalphabetic Cipher:

- In a polyalphabetic cipher, multiple cipher alphabets are used.
- A polyalphabetic cipher uses a number of substitutions at different times in the message.
- In polyalphabetic cipher, relationship between characters in plain text to a character in cipher text is one-to-many.
- **Example:** Consider the previous example of Monoalphabetic Cipher, where 'A' is replaced by 'D' at 4 different places.

➢ If we use polyalphabetic cipher, 'A' will be replaced by 4 different letters.

Key	Topper	19	14	15	15	4	17
Plain Text	Sagar	18	0	6	0	17	-
Cipher Text	LOVPV	37	14	21	15	21	-

COMPARISON:

Table 2.1: Comparison between Monoalphabetic & Polyalphabetic Cipher

Monoalphabetic Cipher	Polyalphabetic Cipher
In monoalphabetic cipher single cipher alphabet is used per message.	In polyalphabetic cipher there are multiple cipher text letters for each plaintext letter.
The relationship between a character in the plaintext and the character in the cipher text is one to one.	The relationship between a character in the plaintext and the character in the cipher text is one to many.
Monoalphabetic cipher is easy to break.	Polyalphabetic cipher is difficult to break as compared to monoalphabetic cipher.
A stream cipher is a monoalphabetic cipher if the value of 'ki' does not depend on the position of the plaintext character in the plaintext stream.	A stream cipher is a monoalphabetic cipher if the value of 'ki' does depend on the position of the plaintext character in the plaintext stream.
Monoalphabetic cipher includes additive, multiplication, affine and monoalphabetic substitution cipher.	Polyalphabetic cipher includes autokey, playfair, vigenere, hill and one time pad cipher.
Example: Refer example given above.	**Example:** Refer example given above.

Q3] Explain with example, keyed and keyless transposition ciphers.

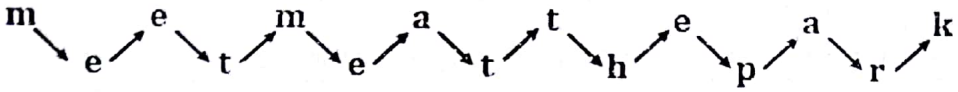
Ans:

TRANSPOSITION CIPHER: **[5M – May16]**

1. Transposition cipher is a method of encryption by which the positions held by units of plain text are shifted according to a regular system, so that the cipher text constitutes a permutation of the plaintext.
2. That is, the order of the units is changed.
3. Transposition cipher does not substitute one symbol for another instead it changes the location of the symbols.
4. Transposition Cipher can be divided as keyless and keyed transposition cipher.

I) **Keyless Transposition Cipher:**

- It is **Simplest Transposition Cipher**.
- In first method the text is written into a table column by column and then row by row.
- For example, to send the message "Meet me at the park" to Bob, Alice writes



The cipher text is created reading the pattern row by row.

Cipher text is "MEMATEAKETETHPR".

- In the second method the text is written into the table row by row and then transmitted column by column.
- For example, Alice and Bob can agree on the number of columns and use the second method.
- Alice writes the same plain text, row by row, in a table of four columns.

m	e	e	t
m	e	a	t
t	h	e	p
a	r	k	

The cipher text is created reading the pattern Column by Column.

Cipher text is "MMTAEEHREAEKTTP".

II) **Keyed Transposition Cipher:**

- In Keyed Transposition Cipher, plain text is divided into groups of predetermined size called blocks.
- Then it use a key to permute the characters in each block separately.
- **Example:** Alice needs to send the message "Enemy attacks tonight" to Bob.
- Let the block size be 5.

e	n	E	m	Y		a	T	t	a	c		k	s	t	o	n		i	g	h	t	z

- The key used for encryption and decryption is a permutation key, which shows how the characters are permuted.

Key:

Encryption ↓	3	1	4	5	2	Decryption ↑
	1	2	3	4	5	

Consider the Figure 2.1 which shows the example of keyed transposition cipher.

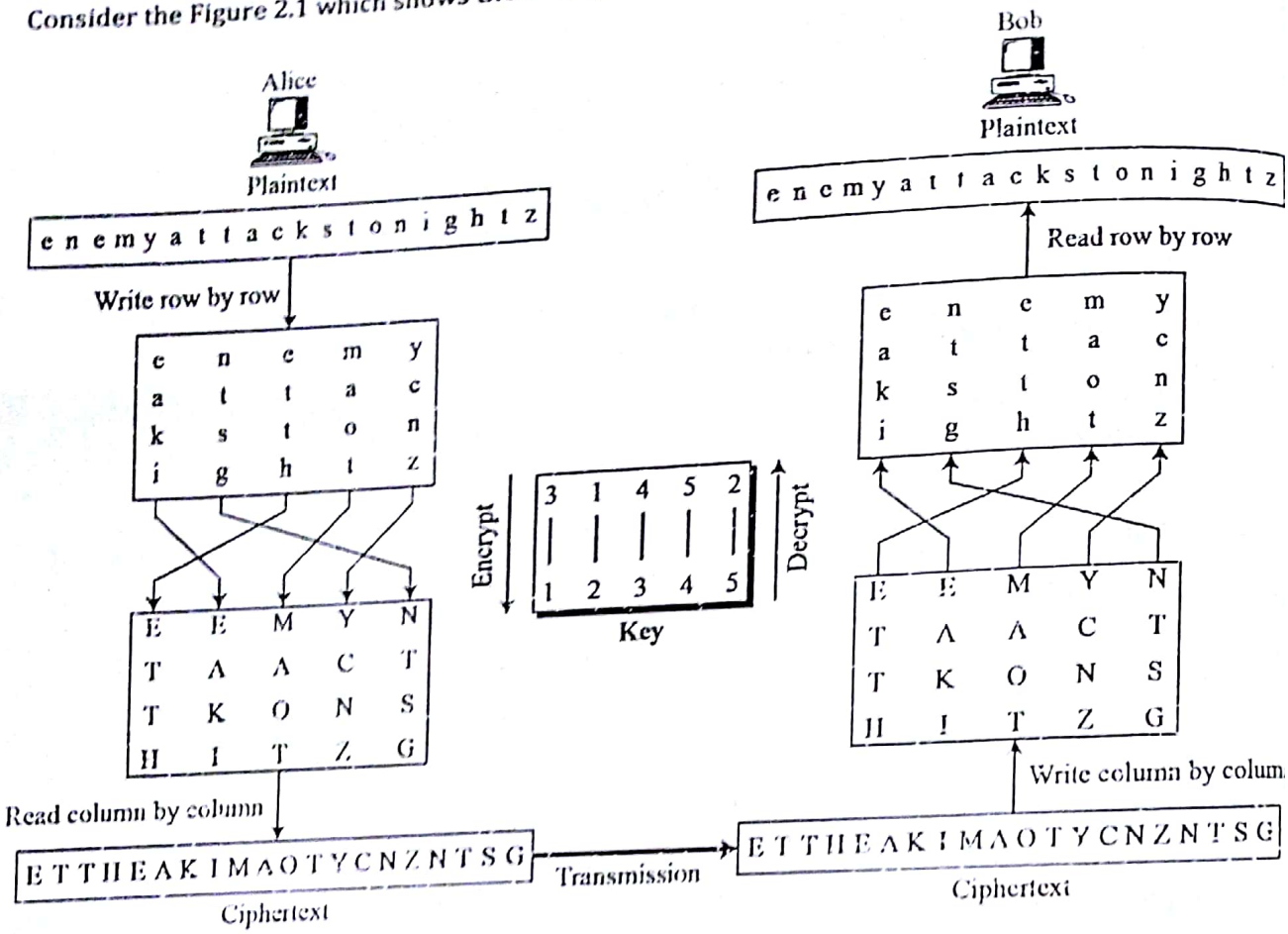


Figure 2.1: Example of Keyed Transposition Cipher

Q4] Encrypt "The key is hidden under the door" using play fair cipher with keyword "domestic"

[5M – Dec15]

Ans:

PLAY FAIR CIPHER:

1. Play Fair Cipher is one of the **Multi-letter Cipher.**
2. Play Fair Cipher uses a **5 x 5 Matrix** of alphabets containing a keyword or phrase.
3. This cipher encrypts pair of letters instead of single letter.
4. It is difficult to break because frequency analysis does not work in Play Fair Cipher.

EXAMPLE:

Plain Text: The key is hidden under the door.

Key: Domestic

Steps:

1. Pair the plain text alphabets in two.

Th ek ey is hi dd en un de rt he do or

2. If any character in the plain text is 'J' then replace it with 'I',

Th ek ey is hi dd en un de rt he do or

3. Double letter or consecutively repeated same letters are separated by x or z.

Th ek ey is hi dxd en un de rt he dox or

4. If an odd character is left out pair it with x or z.

Th ek ey is hi dx de nu nd er th ed ox or

5. Prepare a table same as Monoalphabetic table but this table will be 5 x 5 table because 'I' & 'J' will be merge together. (Using Key i.e. Domestic)

d	o	M	e	s
t	i/j	C	a	b
f	g	H	k	l
n	p	Q	r	u
v	w	X	y	z

6. Replace the pair of characters with the intersection, if the intersection is not found follow the rule.

Rules:

- If both letters are in the same column, take the letter below each one (going back to the top if at the bottom)
- If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right)
- If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

Th ek ey is hi dx de nu nd er th ed ox or

After Applying Rules: cf ar ae bo gc mv os pn vt ay cf so mw ep

Therefore, Cipher Text is: **cf ar ae bo gc mv os pn vt ay cf so mw ep**

Q5] Encrypt the string "This is an easy task" using a playfair cipher with key "monarchy" [5M – Dec16]

Ans:

PLAY FAIR CIPHER:

1. Play Fair Cipher is one of the **Multi-letter Cipher.**
2. Play Fair Cipher uses a **5 x 5 Matrix** of alphabets containing a keyword or phrase.
3. This cipher encrypts pair of letters instead of single letter.
4. It is difficult to break because frequency analysis does not work in Play Fair Cipher.

EXAMPLE:

Plain Text: This is an easy task.

Key: Monarchy

Steps:

1. Pair the plain text alphabets in two.

Th is is an ea sy ta sk

2. If any character in the plain text is 'J' then replace it with 'I'. (in our case character 'J' is not present)

Th is is an ea sy ta sk

3. Double letter or consecutively repeated same letters are separated by x or z. (in our case there is no consecutively repeated same letters)

Th is is an ea sy ta sk

4. If an odd character is left out pair it with x or z. (in our case there is no odd character)

Th is is an ea sy ta sk

5. Prepare a table same as Monoalphabetic table but this table will be 5 x 5 table because 'I' & 'J' will be merge together. (Using Key i.e. Monarchy)

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

Rules:

- If both letters are in the same column, take the letter below each one (going back to the top if at the bottom)
- If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right)
- If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

Th is is an ea sy ta sk

th → Rule 3 → pd
is → Rule 2 → sx
is → Rule 2 → sx
an → Rule 1 → ra
ea → Rule 3 → im
sy → Rule 3 → qb
ta → Rule 3 → sr
sk → Rule 3 → ti

After Applying Rules: **pd sx sx ra im qb sr ti**

Therefore, Cipher Text is: **pd sx sx ra im qb sr ti**

Q6] Use the Play fair cipher with the keyword: "MEDICINE" to encipher the message "The greatest wealth is health".

Ans: **[5M – May17]**

PLAY FAIR CIPHER:

1. Play Fair Cipher is one of the Multi-letter Cipher.
2. Play Fair Cipher uses a 5 x 5 Matrix of alphabets containing a keyword or phrase.
3. This cipher encrypts pair of letters instead of single letter.
4. It is difficult to break because frequency analysis does not work in Play Fair Cipher.

EXAMPLE:

Plain Text: The greatest wealth is health.

Key: MEDICINE

Steps:

1. Pair the plain text alphabets in two.

Th eg re at es tw ea lt hi sh ea lt h

2. If any character in the plain text is 'J' then replace it with 'I'. (in our case character 'J' is not present)

Th eg re at es tw ea lt hi sh ea lt h

3. Double letter or consecutively repeated same letters are separated by x or z. (in our case there is no consecutively repeated same letters)

Th eg re at es tw ea lt hi sh ea lt h

4. If an odd character is left out pair it with x or z. (we pair it with 'x')

Th eg re at es tw ea lt hi sh ea lt hx

5. Prepare a table same as Monoalphabetic table but this table will be 5 x 5 table because 'I' & 'J' will be merge together. (Using Key i.e. Medicine)

M	E	D	I/J	C
N	a	b	f	g
h	k	l	o	p
q	r	s	t	u
v	w	x	y	z

Rules:

- If both letters are in the same column, take the letter below each one (going back to the top if at the bottom)
- If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right)
- If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

Th eg re at es tw ea lt hi sh ea lt hx

th → Rule 3 → qo
eg → Rule 3 → ca
re → Rule 1 → wa
at → Rule 3 → fr
es → Rule 3 → dr
tw → Rule 3 → ry

ea → Rule 3 → ak

lt → Rule 3 → os

hi → Rule 3 → om

sh → Rule 3 → ql

ea → Rule 3 → ak

lt → Rule 3 → os

hx → Rule 3 → lv

After Applying Rules: **qo caw a fr dr ry ak os om ql ak os lv**

Therefore, Cipher Text is: **qo caw a fr dr ry ak os om ql ak os lv**

Q7] Compare and contrast: Block and stream ciphers. **[5M – Dec16]**

Ans:

Table 2.2: Comparison between Block & Stream Cipher.

Stream Cipher	Block Cipher
Stream Cipher operates on smaller units of plain text.	Block Cipher operates on larger block of data.
Faster than Block Cipher.	Slower than Stream Cipher.
Stream Cipher has Low Diffusion.	Block Cipher has High Diffusion.
Requires less code.	Requires more code.
It does not provide integrity protection or authentication.	It provide integrity protection or authentication.
Stream Cipher is more suitable for hardware implementation.	Block Cipher is more suitable for software implementation.
Key is used only once.	Reuse of key is possible.
Example: One Time Pad	Example: DES
Application: SSL	Application: Database, File Encryption.

Q8] Block & Stream Cipher.

Ans: [5M – Dec17]

BLOCK CIPHER:

1. Block Cipher is a symmetric key cipher which operates on a fixed length group of bits, called **block.**
2. It encrypts entire block of message one at a time.
3. In this the plain text are combined with a pseudorandom cipher bit stream by an XOR operation.
4. Cipher text is generated by encrypting the plain text bits one at a time.
5. **Example:** RSA, Diffie Hellman, DES and AES.

STREAM CIPHER:

1. Stream Cipher is also called as **state cipher.**
2. It is a symmetric key cipher, which operates on bits/ bytes.
3. In this the plain text are combined with a pseudorandom cipher bit stream by an XOR operation.
4. Cipher text is generated by encrypting the plain text bits one at a time.
5. **Example:** A5/1, RC 4.

COMPARISON:

Refer Q7.

CHAPTER - 3: SECRET KEY CRYPTOGRAPHY

Q1] IDEA.

Q2] Key generation in IDEA.

[Q1 | 5M – May16] & [Q2 | 5M – Dec15]

Ans:

IDEA:

1. IDEA stands for **International Data Encryption Algorithm.**
2. It is **Block Cipher Algorithm.**
3. IDEA is the replacement of DES (Data Encryption Standard).
4. IDEA operates on 64-bit blocks using a 128 bit key.
5. IDEA derives much of its security by interleaving operations from different groups like modular addition and multiplication, and bitwise exclusive OR (XOR).

KEY GENERATION:

- The 128 bit key is divided into 8 sub parts that is 16 bits each.
- Then the 128 bit key is cyclically shifted to the left by 25 position, so by doing this we will have one new 128 bit key.
- Now similarly as above it is divided into 8 sub blocks and will be used in next round.
- The same process is performed 9 times and 56 keys are generated from which the first 52 keys will be used.
- So likewise from K1 to K52 keys are generated as shown in figure 3.1.

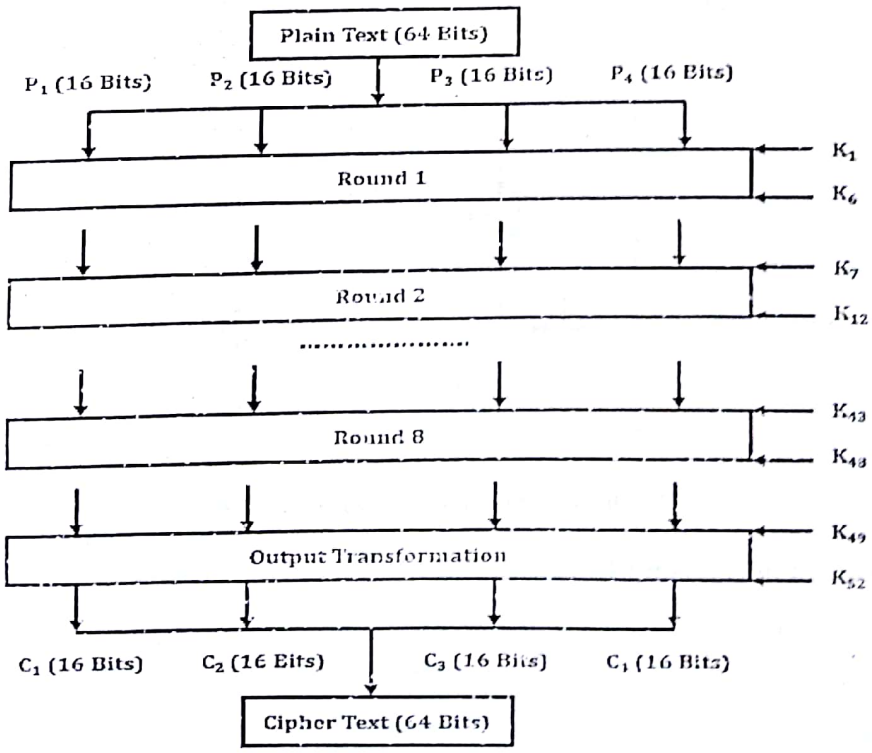


Figure 3.1: IDEA Key Generation.

Sequence of operation in one round:

1. Multiply P_1 and K_1.
2. Add P_2 and second K_2.
3. Add P_3 and third K_3.
4. Multiply P_4 and K_4.
5. Step 1 ⊕ step 3.
6. Step 2 ⊕ step 4.
7. Multiply step 5 with K_5.
8. Add result of step 6 and step 7.
9. Multiply result of step 8 with K_6.
10. Add result of step 7 and step 9.
11. XOR result of steps 1 and step 9.
12. XOR result of steps 3 and step 9.
13. XOR result of steps 2 and step 10.
14. XOR result of steps 4 and step 10.

Same operations are performed in 8 rounds.

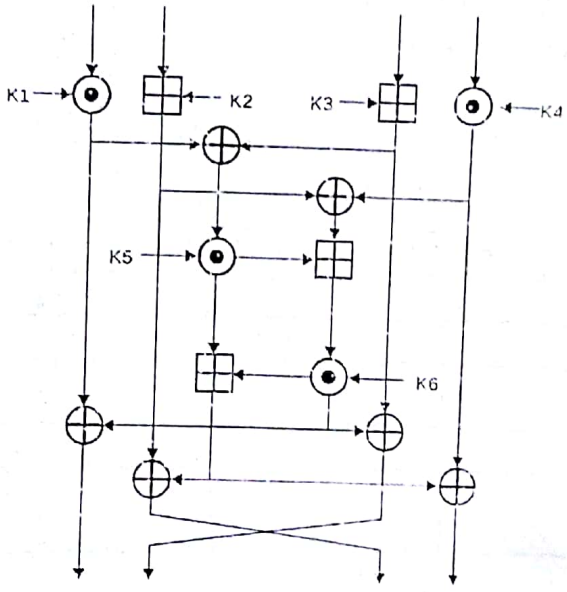


Figure 3.2: Encryption round of IDEA.

Sequence of operation in last round:

1. Multiply P_1 with K_{49}.
2. Add P_2 and K_{50}.
3. Add P_3 and K_{51}.
4. Multiply P_4 and K_{52}.

Q3] Blowfish

Ans: **[5M – May17]**

BLOWFISH:

1. Blowfish is an **encryption algorithm.**
2. It can be used as a **replacement for the DES or IDEA algorithms.**
3. It is a **symmetric block cipher.**
4. It was designed in 1993 by **Bruce Schneier** as an alternative to existing encryption algorithms.
5. It uses a variable-length key, from 32 bits to 448 bits.
6. It useful for **both domestic and exportable use.**
7. This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually.
8. Blowfish can be found in software categories ranging from e-commerce platforms for securing payments to password management tools, where it used to protect passwords.

STRUCTURE OF BLOWFISH ALGORITHM:

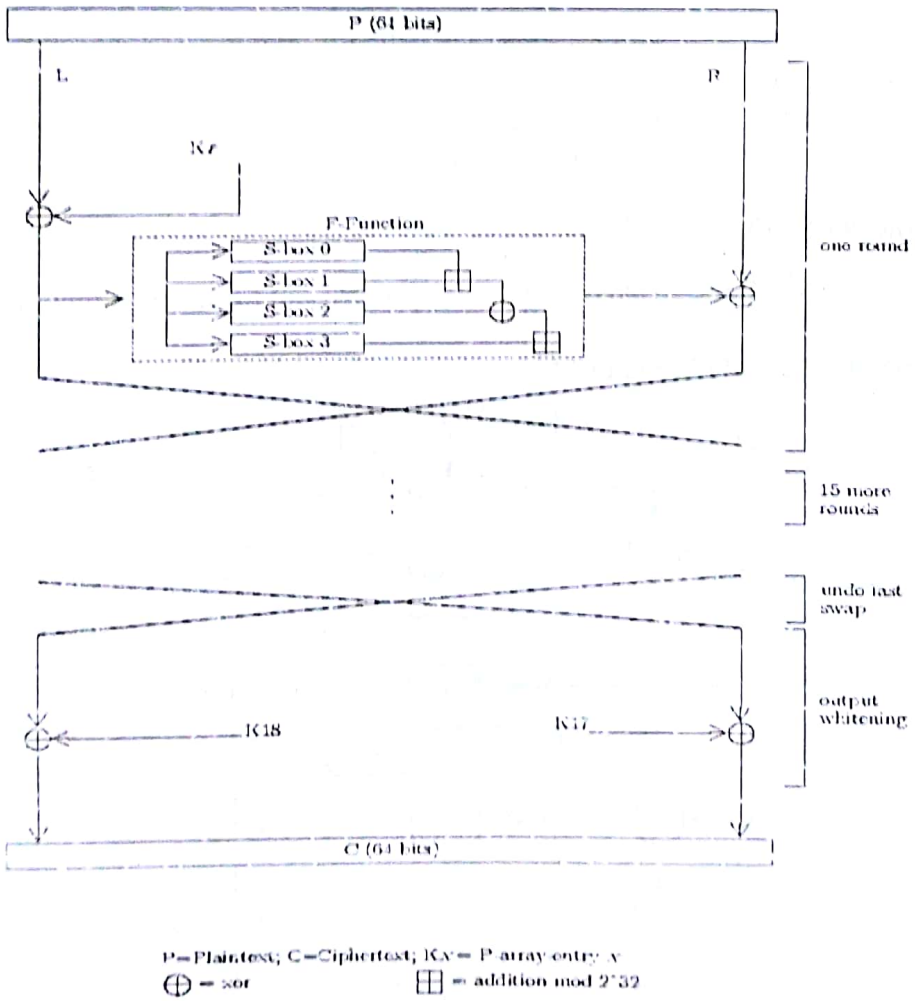


Figure 3.3: The Feistel structure of Blowfish.

- Blowfish has a 64-bit block size.
- It has a key length of anywhere from 32 bits to 448 bits.
- It is a 16-round Fiestel cipher.
- It uses large key-dependent S-boxes.
- It is similar in structure to CAST-128, which uses fixed S-boxes.
- Each line represents 32 bits.
- The algorithm keeps **two sub key arrays**: the 18-entry P-array and four 256-entry S-boxes.
- The S-boxes accept 8-bit input and produce 32-bit output.
- One entry of the P-array is used every round, and after the final round, each half of the data block is XORed with one of the two remaining unused P-entries.
- Since Blowfish is a Fiestel network, it can be inverted simply by XORing K17 and K18 to the ciphertext block, then using the P-entries in reverse order.
- Figure 3.3 shows the action of Blowfish.

Q4] Key generation in IDEA and Blowfish

Ans: **[5M – Dec17]**

KEY GENERATION IN IDEA:

Refer Q2.

KEY GENERATION IN BLOWFISH:

Blowfish algorithm is divided into two parts: Round Structure and Key Expansion Function.

I) Round Structure / Data Encryption:

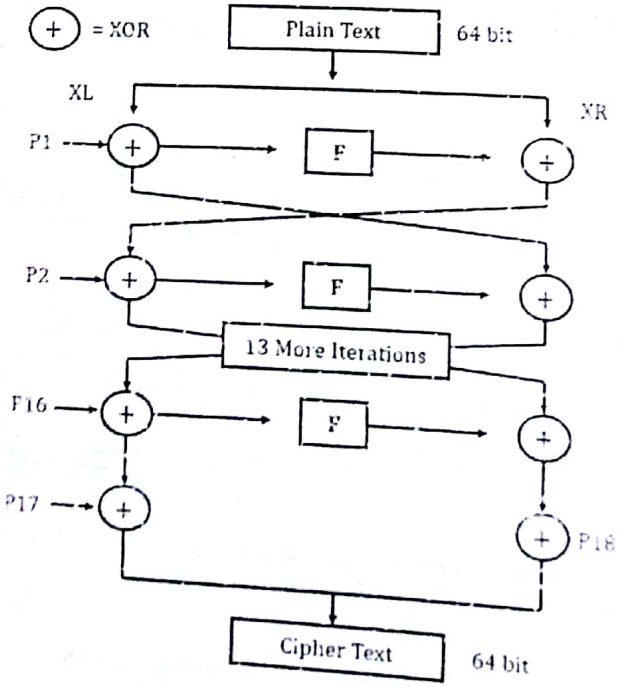


Figure 3.4: Data Encryption.

- Data Encryption has a function to iterate 16 times of network.
- Each round consists of key-dependent permutation and a key and data-dependent substitution.
- All operations are XORs and additions on 32-bit words.
- The only additional operations are four indexed array data lookup tables for each round.

Algorithm:

Divide x into two 32-bit halves: xL, xR

For i = 1 to 16:

xL = XL XOR Pi

xR = F(XL) XOR xR

Swap XL and xR

Swap XL and xR (Undo the last swap.)

xR = xR XOR P17

xL = xL XOR P18

Recombine xL and xR

II) **Key Expansion:**

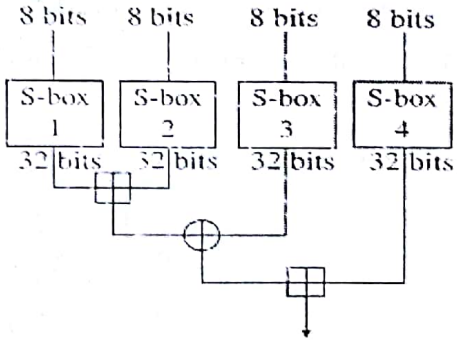


Figure 3.5: Key Expansion.

- Key Expansion is used to convert a key of at most 448 bits into several subkey arrays totaling 4168 bytes.
- These keys are generated earlier to any data encryption or decryption.
- The P-Array consists of 18 sub keys of 32 bit. i.e. P_1 - P_{18}
- Four 32-bit S-Boxes consists of 256 entries each i.e. $S1_0 - S1_{255}$, $S2_0 - S2_{255}$, $S3_0 - S3_{255}$ & $S4_0 - S4_{255}$

Sub Key Calculation:

1. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.
2. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14).

3. Encrypt the all-zero string with the Blowfish algorithm, using the subkeys described in steps (1) and (2).
4. Replace P1 and P2 with the output of step (3).
5. Encrypt the output of step (3) using the Blowfish algorithm with the modified subkeys.
6. Replace P3 and P4 with the output of step (5).
7. Continue the process, replacing all entries of the P array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm.
8. In total, 521 iterations are required to generate all required subkeys.

Q5] Explain working of DES.

Q6] Explain working of DES detailing the Fiestel structure.

Q7] Explain DES, detailing the Fiestel structure and S-block design.

Ans: [Q5 | 10M – May16], [Q6 | 10M – Dec15] & [Q7 | 10M – May17]

DES:

1. DES stands for **Data Encryption Standard.**
2. It is also known as Data Encryption Algorithm or DEA – 1.
3. It is a **symmetric-key block cipher** published by the National Institute of Standards and Technology (NIST).
4. DES is an implementation of a **Feistel Cipher.**
5. It uses 16 round Feistel structure.
6. DES is nothing but an algorithm developed by IBM based on "Lucifer".
7. The successor of DES are Triple DES, G – DES, DES – X.
8. DES algorithm is a powerful combination of two basic encryption techniques.
   a. Confusion.
   b Diffusion.

WORKING:

Figure 3.6 shows working of DES.

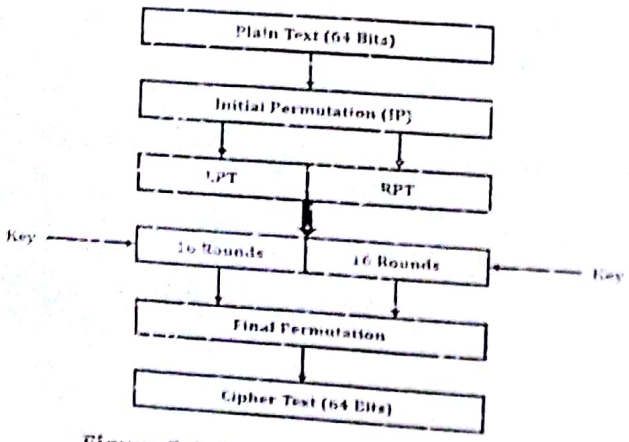


Figure 3.6: Working of DES.

STEPS:

I) **Initial Permutation:**

- Initial Permutation means rearranging the bits of the plain text.
- Initial Permutation is performed over plain text.
- For **Example:** P = 1010101010 → 1111100000
- It produces two halves of the permuted blocks i.e. Left Plain Text (LPT) & Right Plain Text (RPT)

II) **Detail of one round in DES:**

- Each Round in DES performs following Steps as shown in Figure 3.7

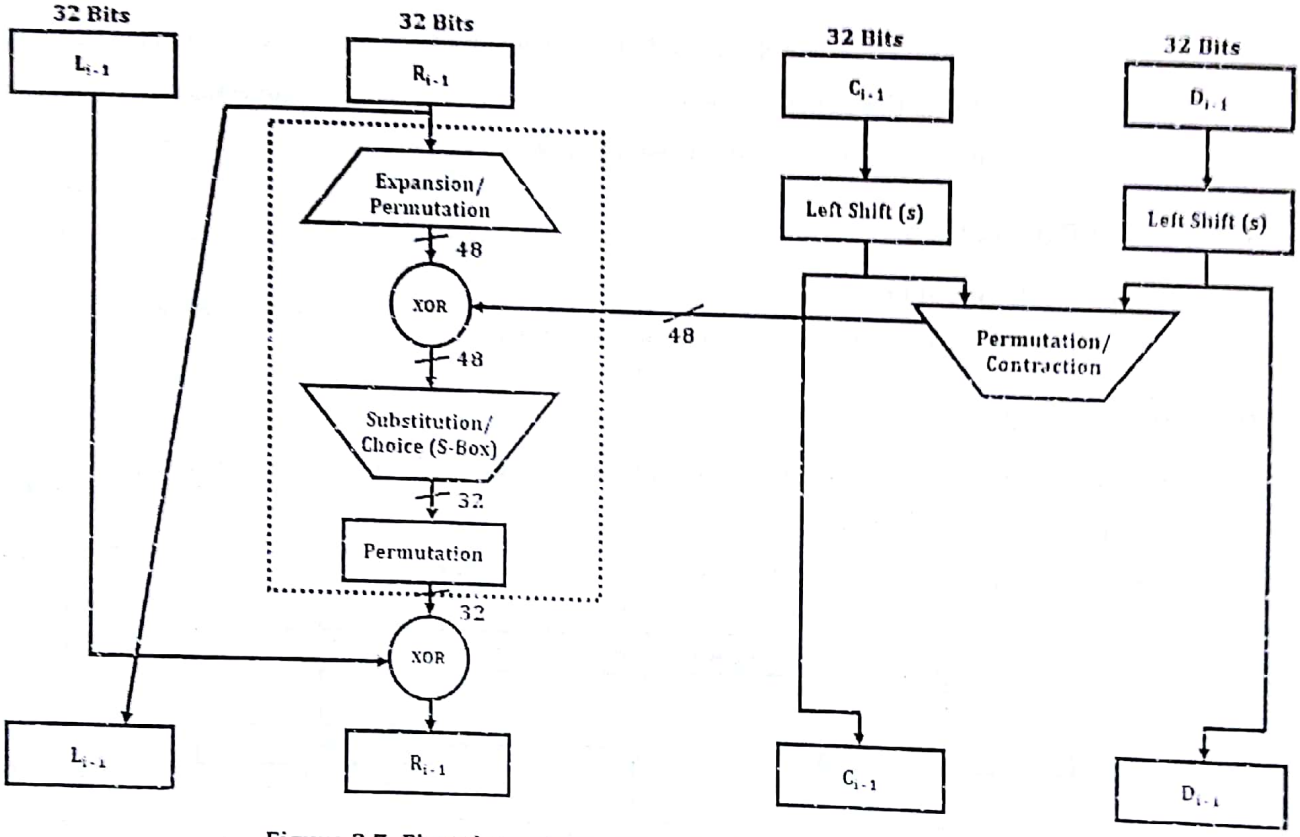


Figure 3.7: Fiestel structure of Detail of one round in DES.

III) **Key Discarding Process:**

- 56 Bit Key is used during encryption process.
- In Key Discarding Process, 56 bit key is transformed into 48 bit key by discarding every 8th bit of initial key.

IV) **Expansion Permutation:**

- In Expansion Permutation, the right half is expanded from 32 bits to 48 bits.
- Expansion permutation permutes order of the bit and repeats certain bits, so that both the inputs of first XOR operation are comparable.

V) **S-BOX Substitution:**

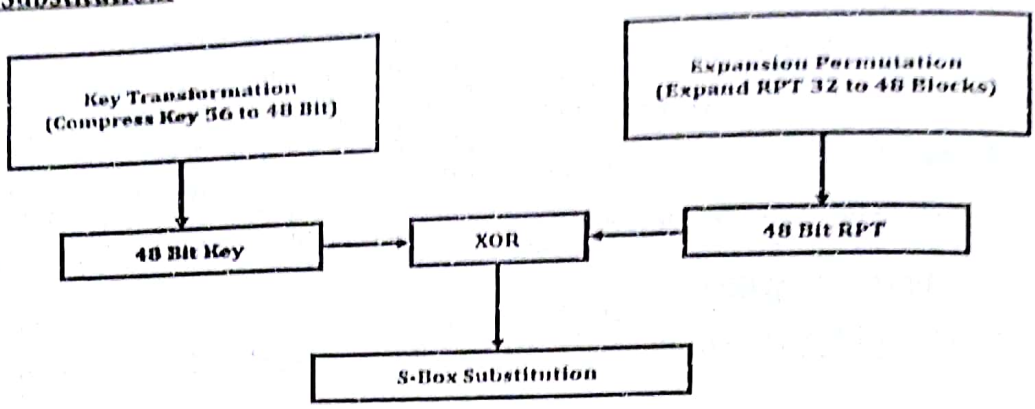


Figure 3.8: S-Box Substitution.

- S-Box Substitution is the process which accepts 48 bit key and expanded right plain text of 48 bit which get XOR and produces 32 bit output as shown in figure 3.8

VI) **P-BOX Permutation:**

- It is similar to Initial Permutation.
- In this step, the 32 bit output from eight boxes is permuted.

VII) **XOR & SWAP:**

- In this Step, the output of XOR operation becomes new right plain text and old right plain text becomes new left plain text.
- The complete process is called as XOR and swapping operations.

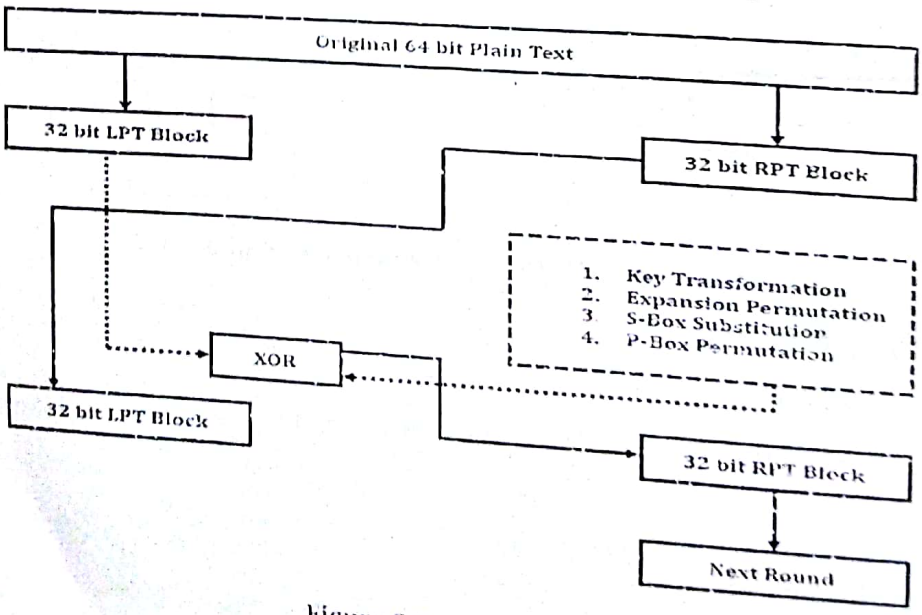


Figure 3.9: XOR & Swap.

VIII) **Final Permutation:**

- Final Permutation is performed after successful completion of 16 rounds.
- It produces 64-bit encrypted block.

Q8] With reference to DES comment on the following:
(i) Block size and key size.
(ii) Need for expansion permutation.
(iii) Avalanche and completeness effects.
(iv) Weak keys and semi-weak keys.
(v) Role of S-box

Q9] What is the purpose of S-boxes in DES? Explain the avalanche effect?

Ans: **[Q8 | 10M – Dec17] & [Q9 | 5M – May18]**

DES:

1. DES stands for **Data Encryption Standard.**
2. It is also known as Data Encryption Algorithm or DEA – 1.
3. It is a **symmetric-key block cipher** published by the National Institute of Standards and Technology (NIST).
4. DES is an implementation of a **Feistel Cipher.**

BLOCK SIZE AND KEY SIZE:

- Key sizes: 56 bits (+8 parity bits)
- Block sizes: 64 bits

NEED FOR EXPANSION PERMUTATION:

- The heart of DES Cipher is the DES function.
- The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.
- Since right input is 32-bit and round key is a 48-bit, Expansion Permutation is used to expand right input to 48 bits.

AVALANCHE AND COMPLETENESS EFFECTS:

- The DES satisfies both the desired properties of block cipher.
- These avalanche and completeness property make cipher very strong
  - **Avalanche Effect:** A small change in plaintext results in the very great change in the cipher text.
  - **Completeness:** Each bit of cipher text depends on many bits of plain text.

WEAK KEY IN DES:

- Four out of 256 possible keys in DES are called **Weak Keys.**
- A weak key is the one that, after parity drop operation, consists either of all 0s, all 1s, or half 0s and half 1s.
- These keys are shown in Table 3.1.

Table 3.1: Weak keys.

Keys before parities drop (64 bits)	Actual key (56 bits)
0101 0101 0101 0101	000000 000000
1F1F 1F1F 0E0E 0E0E	000000 FFFFFF
E0E0 E0E0 F1F1 F1F1	FFFFFFF 0000000
FEFE FEFE FEFE FEFE	FFFFFFF FFFFFFF

- The round keys created from any of these weak keys are the same and have the same pattern as the cipher key.
- Weak key is the inverse of itself.

SEMI-WEAK KEY IN DES:

- There are six key pairs that are called semi-weak keys.
- These six pairs are shown in Table 3.2 (64-bit format before dropping the parity bits)

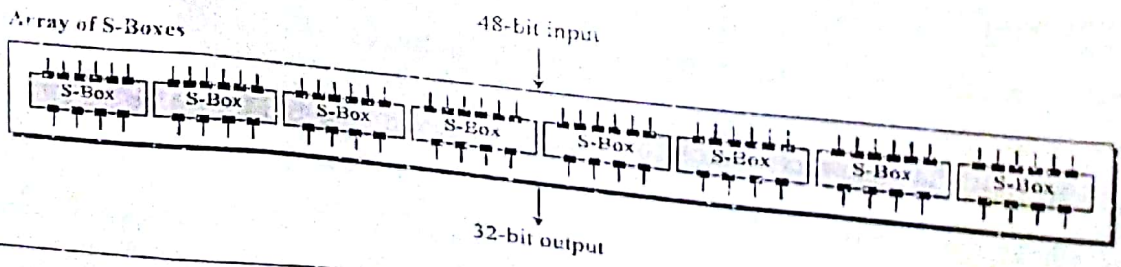
Table 3.2: Semi-weak keys.

First key in the pair	Second key in the pair
01FE 01FE 01FE 01FE	FE01 FE01 FE01 FE01
1FE0 1FE0 0EF1 0EF1	E01F E01F F10E F10E
01E0 01E1 01F1 01F1	E001 E001 F101 F101
1FFE 1FFE 0EFE 0EFE	FE1F FE1F FE0E FE0E
011F 011F 010E 010E	1F01 1F01 0E01 0E01
E0FE E0FE F1FE F1FE	FEE0 FEE0 FEF1 FEF1

- A semi-weak key creates only two different round keys and each of them is repeated eight times.
- In addition, the round keys created from each pair are the same with different orders

ROLE OF S-BOX:

- The S-boxes do the real mixing (confusion).
- DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output.



- The 48-bit data from the second operation is divided into eight 6-bit chunks, and each chunk is fed into a box.
- The result of each box is a 4-bit chunk.
- When these are combined the result is a 32-bit text.
- For example, in S1, for input 011001, the row is 01 and the column is 1100.
- The value in row 1, column 12 is 9, so the output is 1001.

Q10] Describe triple DES with two DES keys. Is man in the middle attack possible on triple DES?

Ans: **[5M – Dec16]**

TRIPLE DES:

1. The DES algorithm uses a key length of **56 bits**, with which becomes very easy for an attacker to break the encryption.
2. To improve the security of DES at higher level Triple DES was proposed.
3. This uses three stages on DES for encryption and Decryption.
4. It has two versions: **Triple DES with Two Keys and Triple DES with Three Keys.**

Triple DES with Two Keys:

- In this two keys are used.
- In first and third stage Key K1 is used while in second stage Key K2 is used.
- First the plain text is encrypted with key K1 then the output of stage 1 is decrypted with key K2 and final output second step is encrypted again with key K1.
- Figure 3.8 shows the encryption & decryption using triple DES with 2 keys.

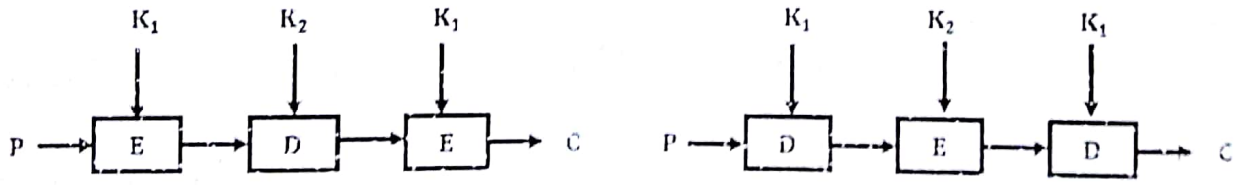


Figure 3.10: Triple DES with 2 Keys.

Man in the Middle Attack:

- **No Man-in-the-middle attack or Meet-in-the-middle attack is not possible in Triple DES.**
- For the given known pair of plain text-cipher text (P, C), the attacker will Encrypt P with all 2^{56} possible keys for K1 (size of key is 56 bits in DES) and Decrypt C with all 2^{56} possible keys for K2.
- If E (K1, P) = D (K2, C) then K1, K2 are most likely the correct pair of keys.
- The attacker confirms this key pair by checking it with another pair of P, C.

- In order to counter Man-in-the-middle attack or Meet-in-the-middle attack, three stages of encryption-decryption with two different keys is used.
- This raises the cost of the Man-in-the-middle attack or Meet-in-the-middle attack to 2^{168} which is not practical for now.
- However, it has the drawback of requiring a key length of 56 x 3 = 168 bits, which may be somewhat unwieldy.
- For this reason Triple DES with 2 keys is used.
- Using Triple DES with 2 keys we get the same cost of attacking for less number of keys.
- One half has (K1, K2) and the other K1.
- Attacking the first half costs 2^{112} operations, attacking the second half costs 2^{56} operations.

Q11] Compare DES and IDEA. Explain the round key generation scheme in both these algorithms.

[10M – Dec16]

Ans:

COMPARISON BETWEEN DES & IDEA:

Table 3.3: Comparison between DES & IDEA.

DES	IDEA
DES Stands for Data Encryption Standard Algorithm.	IDEA stands for International Data Encryption Algorithm.
It uses 56-bit key.	It uses 128-bit key.
DES is now considered insecure (mainly due to a small key size of 56-bits).	Considered to be a good and secure algorithm.
DES divides plain text/cipher text into 64 bits per block.	IDEA divides plain text/cipher text into 64 bits per block.
It has 16 rounds of encryption/decryption process.	It has 8 rounds of encryption/decryption process followed by a final round of output transformation.
Each round uses different 48-bit sub key generated from the 56-bit key.	Each of the 8 rounds uses different 6 sub key and last round uses 4 sub keys.
16 different sub keys are used in DES.	52 different sub keys are used in IDEA.
DES is weaker than IDEA.	IDEA is stronger than DES.

Round key generation scheme in DES:

Refer Q5.

Round key generation scheme in IDEA:

Refer Q2.

Q12] What are block ciphers? Explain with examples the CBC and ECB modes of block ciphers

Ans: **[5M – Dec16]**

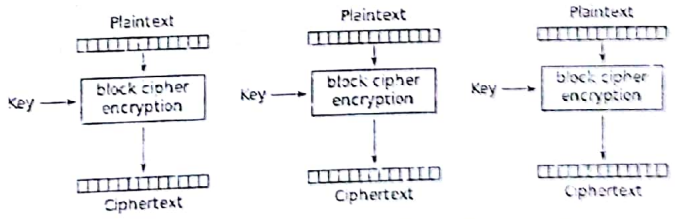
BLOCK CIPHER:

1. Block Cipher is a symmetric key cipher which operates on a fixed length group of bits, called **block.**
2. It encrypts entire block of message one at a time.
3. In this the plain text are combined with a pseudorandom cipher bit stream by an XOR operation.
4. Cipher text is generated by encrypting the plain text bits one at a time.
5. **Example:** RSA, Diffie Hellman, DES and AES.

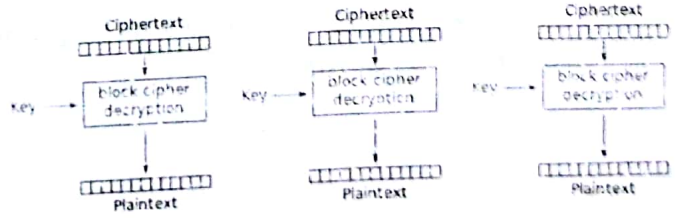
MODES OF OPERATION:

I) **ECB Mode:**

- ECB Mode stands for **Electronic Code Book Mode.**
- It is simplest **encryption mode.**
- The message is divided into blocks, and each block is encrypted separately.
- If the size of plaintext is not a multiple of block size, padding is used to maintain uniform size of block.
- Since it is symmetric, it uses same key for encryption and decryption of each block.
- The encryption and decryption can be done as follows as shown in figure 3.11.



Electronic Codebook (ECB) mode encryption

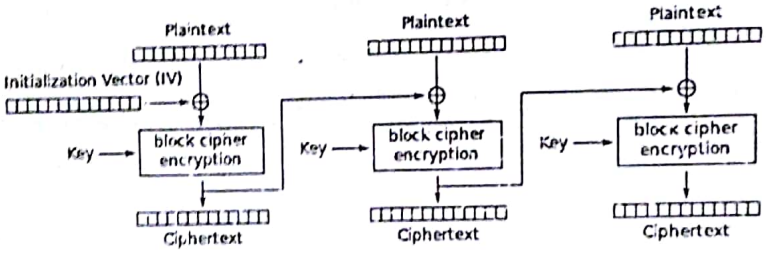


Electronic Codebook (ECB) mode decryption

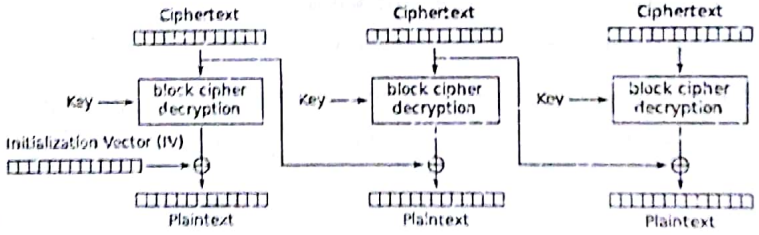
Figure 3.11: ECB Mode.

II) **CBC Mode:**

- CBC Mode Stands for **Cipher Block Chaining Mode.**
- It was invented by IBM.
- It is used to overcome the security deficiencies of ECB Mode.
- In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted.
- This way, each ciphertext block depends on all plaintext blocks processed up to that point.
- To make each message unique, an **initialization vector** (IV) must be used in the first block.
- The encryption and decryption can be done as follows as shown in figure 3.12.



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Figure 3.12: CBC Mode.

If the first block has index 1, the mathematical formula for CBC encryption is

$C_i = E_K (P_i \oplus C_{i-1})$ and $C_0 = IV$

While the mathematical formula for CBC decryption is

$P_i = D_K (C_i) \oplus C_{i-1}$ and $C_0 = IV$

Q13] Encrypt the message "Cryptography is fun" with a multiplicative cipher with key = 15. Decrypt to get back original plaintext

Ans:

[5M – Dec17]

MULTIPLICATIVE CIPHER:

1. Multiplicative cipher is a type of substitution cipher.
2. It is similar to caesar cipher.

3. The only difference is instead of addition, we use multiplication.
4. Multiplicative cipher can represented mathematically as:

   $C = (P \times K) \bmod 26$

   $P = (C \times K^{-1}) \bmod 26$
5. Multiplicative cipher has only 12 possible keys.

EXAMPLE:

Plain Text: Cryptography is fun

Key: 15

Encryption:

Plain Test	Number	C = (P x K) mod 26	Cipher Text
C	2	2 x 15 mod 26 = 4	E
R	17	17 x 15 mod 26 = 21	V
Y	24	24 x 15 mod 26 = 22	W
P	15	15 x 15 mod 26 = 17	R
T	19	19 x 15 mod 26 = 25	Z
O	14	14 x 15 mod 26 = 2	C
G	6	6 x 15 mod 26 = 12	M
R	17	17 x 15 mod 26 = 21	V
A	0	0 x 15 mod 26 = 0	A
P	15	15 x 15 mod 26 = 17	R
H	7	7 x 15 mod 26 = 1	B
Y	24	24 x 15 mod 26 = 22	W
I	8	8 x 15 mod 26 = 16	Q
S	18	18 x 15 mod 26 = 10	K
F	5	5 x 15 mod 26 = 23	X
U	20	20 x 15 mod 26 = 14	O
N	13	13 x 15 mod 26 = 13	N

Decryption:

Cipher Test	Number	P = (C x K^{-1}) mod 26	Plain Text
E	4	4 x 7 mod 26 = 2	C
V	21	21 x 7 mod 26 = 17	R
W	22	22 x 7 mod 26 = 24	Y
R	17	17 x 7 mod 26 = 15	P

Z	25	25 x 7 mod 26 = 19	T
C	2	2 x 7 mod 26 = 14	O
M	12	12 x 7 mod 26 = 6	G
V	21	21 x 7 mod 26 = 17	R
A	0	0 x 7 mod 26 = 0	A
R	17	17 x 7 mod 26 = 15	P
B	1	1 x 7 mod 26 = 7	H
W	22	22 x 7 mod 26 = 24	Y
Q	16	16 x 7 mod 26 = 8	I
K	10	10 x 7 mod 26 = 18	S
X	23	23 x 7 mod 26 = 5	F
O	14	14 x 7 mod 26 = 20	U
N	13	13 x 7 mod 26 = 13	N

Q14] Use Hill cipher to encrypt the text "short". The key to be used is "hill"

[10M – May18]

Ans:

HILL CIPHER:

1. Hill cipher is a **polygraphic substitution cipher.**
2. Invented by Lester S. Hill in 1929.
3. It is based on linear algebra.
4. The Hill cipher is an example of a **block cipher.**
5. In hill cipher, each letter is represented by a number modulo 26.
6. To encrypt a message, each block of n letters is multiplied by an invertible n × n matrix, against modulus 26.
7. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.
8. The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).

EXAMPLE:

Plaintext: short

Key: hill

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

We have to encrypt the message 'short' (n = 5). The key is 'hill' which can be written as the n x n matrix:

$$\text{Hill} = \begin{bmatrix} H & I \\ L & L \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$$

$$\text{Short} = \begin{bmatrix} S & O & T \\ H & R & - \end{bmatrix} = \begin{bmatrix} 18 & 14 & 19 \\ 7 & 17 & 0 \end{bmatrix}$$

The enciphered vector is given as:

$$\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}\begin{bmatrix} 18 & 14 & 19 \\ 7 & 17 & 0 \end{bmatrix} \bmod (26) = \begin{bmatrix} 182 & 234 & 133 \\ 275 & 341 & 209 \end{bmatrix} \bmod (26)$$

$$= \begin{bmatrix} 0 & 0 & 3 \\ 15 & 3 & 1 \end{bmatrix}$$

Encrypted Text = apaddb

--- EXTRA QUESTION ---

Q1] Variant of DES

Ans:

DOUBLE DES:

1. The DES algorithm uses a key length of 56 bits, with which becomes very easy for an attacker to break the encryption.
2. Double DES is the encryption standard which provides greater security, since it uses key length of 80 bits.
3. In this two keys are used say K_1 and K_2.
4. It first performs DES on the original plain text using Key K_1 to get the encrypted text.
5. It performs DES again on the encrypted text but this time with the other key K_2.
6. The final output is the encryption of encrypted text with the original plain text encrypted twice with two different keys shown below in figure 3.13.

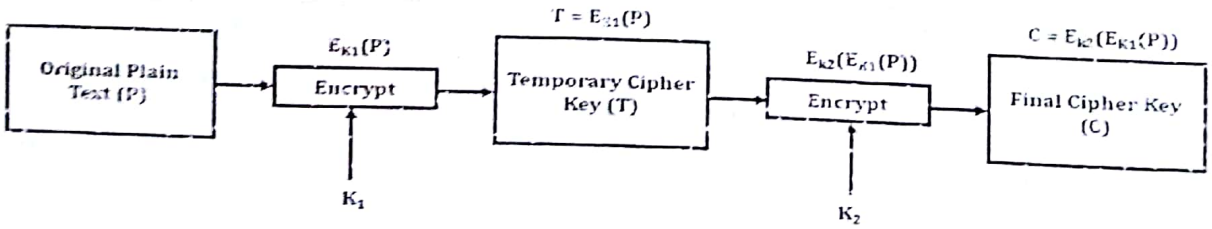


Figure 3.13: Double DES.

7. Man in the middle attack is the drawback of double DES.

TRIPLE DES:

1. To improve the security of DES at higher level Triple DES was proposed.
2. This uses three stages on DES for encryption and Decryption.
3. It has two versions:

I) **Triple DES with Two Keys:**

- In this two keys are used.
- In first and third stage Key K1 is used while in second stage Key K2 is used.
- First the plain text is encrypted with key K1 then the output of stage 1 is decrypted with key K2 and final output second step is encrypted again with key K1.
- Figure 3.12 shows the encryption & decryption using triple DES with 2 keys.

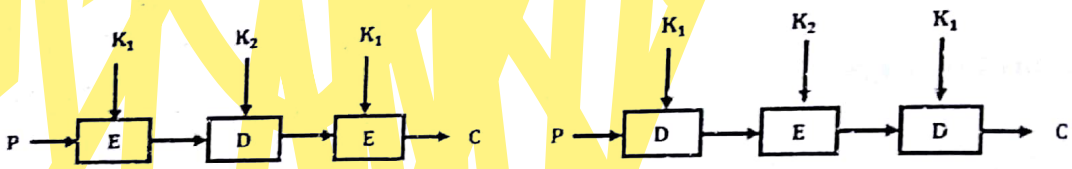


Figure 3.12: Triple DES with 2 Keys.

II) **Triple DES with Three Keys:**

- In this three keys are used
- In first stage Key K1 is used while in second stage Key K2 is used and in third stage key K3.
- First the plain text is encrypted with key K1 then the output of stage 1 is decrypted with key K2 and final output second step is encrypted again with key K3.
- Figure 3.13 shows the encryption & decryption using triple DES with 3 keys.

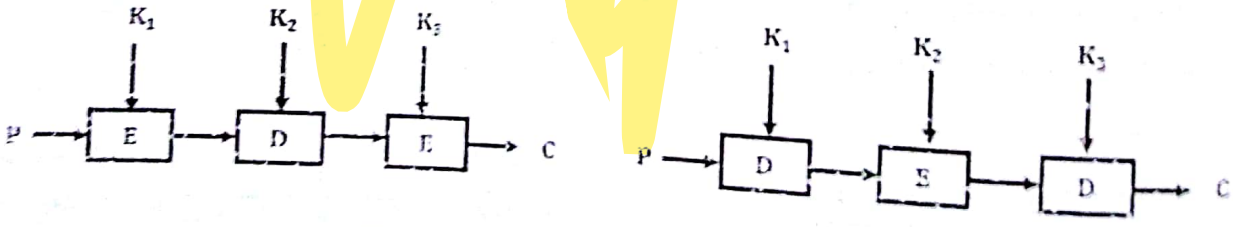


Figure 3.13: Triple DES with 3 Keys.

CHAPTER - 4: PUBLIC KEY CRYPTOGRAPHY

Q1] Elaborate the steps of key generation using RSA Algorithm.

Ans: **[5M – May16]**

RSA:

1. RSA is a **public key encryption algorithm.**
2. RSA is derived from its inventors Rivest, Shamir and Adleman in 1978.
3. RSA works on the principle that says it is too difficult to find the factors of large prime numbers.
4. It involves **multiplying two large prime numbers.**
5. It is used for both public key encryption and digital signature.
6. RSA uses modular exponentiation for encrypting and decrypting the message.

ALGORITHM:

1. Choose two different large random prime numbers say "p" and "q".
2. Calculate n = p x q. Since "n" is the modulus for the public key and the private keys
3. Calculate the totient: **Ø (n) = (p - 1)(q - 1)**
4. Choose an integer "e" such that **1 < e < Ø (n)** and "e" is co-prime to Ø (n) i.e. "e" and Ø (n) share no factors other than 1.
5. Find out decryption key "d" such that $e * d = 1 \bmod (p - 1)(q - 1)$.
6. Encrypt the message "m" using encryption key e, $c = m^e \bmod n$.
7. Decrypt the message "m" using decryption key d, $m = c^d \bmod n$.

In above algorithm, e and n are public whereas d is kept public.

Q2] Briefly define idea behind RSA and also explain
1) What is the one way function in this system?
2) What is the trap door in this?
3) Give Public key and Private Key.
4) Describe security in this system.

Ans: **[10M – May17]**

RSA:

Refer Q1.

What is the one way function in this system?

- A one-way function is a function that is "easy" to compute and "difficult" to reverse.

- There are two one-way functions involved in the security of RSA.
  - Encryption Function.
  - Multiplication of Two Primes.

What is the trap door in this?

- A trapdoor function is a function that is easy to perform one way, but has a secret that is required to perform the inverse calculation efficiently.
- Trapdoor in RSA is the **private key.**

Give Public key and Private Key

- Refer RSA Algorithm from Q1.

Describe security in this system.

- There are two one-way functions involved in the security of RSA.

1. **Encryption Function:**

- The encryption function is a trapdoor one-way function, whose trapdoor is the private key.
- The difficulty of reversing this function without the trapdoor knowledge is **believed** (but not known) to be as difficult as factoring.

2. **Multiplication of Two Primes:**

- The difficulty of determining an RSA private key from an RSA public key is **known** to be equivalent to factoring n.
- An attacker thus cannot use knowledge of an RSA public key to determine an RSA private key unless they can factor n.
- Because multiplication of two primes is believed to be a one-way function, determining an RSA private key from an RSA public key is believed to be very difficult.

Q3] In an RSA system the public key (e, n) of user A is defined as (7, 119). Calculate Φ_n and private key d. what is the cipher text when you encrypt message m=10, using the public key?

Ans:

RSA: [10M – Dec15]

Refer Q1.

EXAMPLE:

Given:

Public Key (e, n) = (7, 119)

To Calculate: Ø (n) and private key 'd'.

Solution:

n = p x q .....where p & q are two prime numbers

∴ p = 17 and q = 7

Now Ø (n) = (p - 1) x (q - 1)
= (17 - 1) x (7 - 1)
= 16 x 6
= 96

∴ Ø (n) = 96

Now Private Key 'd' $= \frac{1 + k\,Ø\,(n)}{e}$

$= \frac{1 + 4\,(96)}{7}$

= 385/7
= 55

∴ d = 55

Thus, private key is (d, n) = (55, 119)

Then As given m = 10
Using formula for encryption key e: $c = m^e \bmod n$
$= 10^7 \bmod 119$
= 73

∴ Cipher Text (c) = 73

Ø (n) = 96, d = 55 & Cipher Text (c) = 73

Q4] A and B wish to use RSA to communicate securely. A chooses public key (e, n) as (7, 247) and B chooses public key (e, n) as (5, 221). Calculate their private keys. What will be the cipher text sent by A to B if A wishes to send message m = 5 securely to B?

Ans: **[10M -- May16]**

RSA:

Refer Q1.

EXAMPLE:

Given:

A: Public Key (e, n) = (7, 247)

B: Public Key (e, n) = (5, 221)

To Calculate: Ø (n) and private key 'd'.

Solution:

FOR A:

e = 7

n = 247

Since n = p x q .....where p & q are two prime numbers

∴ p = 13 and q = 19

Now Ø (n) = (p - 1) x (q - 1)

= (13 - 1) x (19 - 1)

= 12 x 18

= 216

∴ **Ø (n) = 216**

Now Private Key d $= \frac{1 + k\,Ø\,(n)}{e}$

$= \frac{1 + k\,(216)}{7}$

When k = 1,

Private Key d $= \frac{1 + 1\,(216)}{7}$

= 217/7

= 31 ... (which is an integer)

∴ d = 31

Thus, private key of A is (d, n) = (31, 247)

FOR B:

e = 5

n = 221

Since n = p x q .....where p & q are two prime numbers

∴ p = 13 and q = 17

Now Ø (n) = (p - 1) x (q - 1)

= (13 - 1) x (17 - 1)

= 12 x 16

= 192

∴ **Ø (n) = 192**

Now Private Key d $= \frac{1 + k\,Ø\,(n)}{e}$

$$= \frac{1 + k\,(192)}{5}$$

When k = 1,

Private Key d $= \frac{1 + 1\,(192)}{5}$

$= 193/5$

= 38.6 ... (which is not an integer)

When k = 2,

Private Key d $= \frac{1 + 2\,(192)}{5}$

$= 385/5$

= 77 ... (which is an integer)

∴ d = 77

Thus, private key of A is (d, n) = (77, 221)

Now, A wishes to send message m = 5 to B.

A will encrypt the message using public key of B (e, n) = (5, 221)

P = Plaintext = 5

C = Ciphertext = ?

C $= P^e \bmod n$

$= (5)^5 \bmod 221$

$= 31$

Thus, cipher text = 31 for plain text = 5

Q5] A and B wish to use RSA to communicate securely. A chooses public key as (7, 119) and B chooses public key as (13, 221). Calculate their private keys. A wishes to send message m = 10 to B. What will be the cipher text? With what key will A encrypt the message "m" if A needs to authenticate itself to B

Ans: [10M – Dec17]

RSA:

Refer Q1.

EXAMPLE:

Given:

A: Public Key (e, n) = (7, 119)

B: Public Key (e, n) = (13, 221)

To Calculate: Ø (n) and private key 'd'.

Solution:

FOR A:

e = 7

n = 119

Since n = p x q .....where p & q are two prime numbers

∴ p = 7 and q = 17

Now Ø (n) = (p - 1) x (q - 1)

= (7 - 1) x (17 - 1)

= 6 x 16

= 96

∴ Ø (n) = 96

Now Private Key d $= \frac{1 + k\,Ø\,(n)}{e}$

$= \frac{1 + k\,(96)}{7}$

When k = 1,

Private Key d $= \frac{1 + 1\,(96)}{7}$

= 97/7

= 13.857 ... (which is not an integer)

Similarly, k = 2 & k = 3 does not result an integer.

When k = 4,

Private Key d $= \frac{1 + 4(96)}{7}$

= 385/7

= 55 ... (which is an integer)

∴ d = 55

Thus, private key of A is (d, n) = (55, 119)

FOR B:

e = 13

n = 221

Since n = p x q .....where p & q are two prime numbers

∴ p = 13 and q = 17

Now Ø (n) $= (p - 1) \times (q - 1)$

$= (13 - 1) \times (17 - 1)$

$= 12 \times 16$

$= 192$

∴ Ø (n) = 192

Now Private Key d $= \frac{1 + k\,Ø\,(n)}{e}$

$= \frac{1 + k\,(192)}{13}$

When k = 1,

Private Key d $= \frac{1 + 1\,(192)}{13}$

$= 193/13$

$= 14.84$ ... (which is not an integer)

When k = 9,

Private Key d $= \frac{1 + 9\,(192)}{13}$

$= 1729/13$

$= 133$ ... (which is an integer)

∴ d = 133

Thus, private key of A is (d, n) = (133, 221)

Now, A wishes to send message m = 10 to B.

A will encrypt the message using public key of B (e, n) = (13, 221)

P = Plaintext = 10

C = Ciphertext = ?

C $= P^e \bmod n$

$= (10)^{13} \bmod 221$

$= 62$

Thus, cipher text = 62 for plain text = 10

Q6] In RSA system the public key of a given user e = 7 & n= 187

1) What is the private key of this user?

2) If the intercepted CT=11 and sent to a user whose public key e=7 & n=187. What is the PT?

3) Elaborate various kinds of attacks on RSA algorithm?

Ans: [10M – May18]

RSA:

Refer Q1.

EXAMPLE:

(1) Private key of this user?

Public Key (e, n) = (7, 187)

Since n = p x q .....where p & q are two prime numbers

∴ p = 17 and q = 11

Now Ø (n) = (p - 1) x (q - 1)

= (17 - 1) x (11 - 1)

= 16 x 10

= 160

∴ Ø (n) = 160

Now Private Key $d = \frac{1 + k\,Ø(n)}{e}$

$= \frac{1 + k\,(160)}{7}$

When k = 1,

Private Key $d = \frac{1 + 1\,(160)}{7}$

= 161/7

= 23 ... (which is an integer)

∴ d = 23

Thus, private key is (d, n) = (23, 187)

(2) If the intercepted CT=11 and sent to a user whose public key e=7 & n=187. What is the PT?

Cipher Text = 11

Public Key (e, n) = (7, 187)

Private key (d, n) = (23, 187)

Now, Based on RSA decryption algorithm,

PT = $CT^d \bmod n$

= $11^{23} \bmod 187$

= $79720245 \bmod 187$

= 88

We also can verify the correctness by the RSA encryption algorithm as the following:

CT = $PT^e \bmod n$

= $88^7 \bmod 187$

= 11

Therefore, we conclude that the plaintext (PT) is 88.

(3) Elaborate various kinds of attacks on RSA algorithm?

Possible approaches to attacking the RSA algorithm are as follows:

I) **Brute Force Attack:**

- This attack involves trying all possible private keys.

II) **Mathematical Attacks:**

- This attack depend on factoring the product of two primes.

III) **Timing Attacks:**

- This attack depend on the running time of the decryption algorithm.

IV) **Chosen Cipher Text Attacks:**

- This type of attack exploits properties of the RSA algorithm.

Q7] Explain how a key is shared between two parties using Diffie-Hellman by exchange algorithm. What is the drawback of this algorithm?

[10M – Dec15]

Ans:

DIFFIE-HELLMAN ALGORITHM:

1. Diffie-Hellman algorithm was developed by Whitfield Diffie & Martin Hellman in 1976.
2. It is used to solve the **key distribution problem of symmetric key encryption.**
3. Diffie Hellman is a **public key cryptosystem.**
4. It does not encrypt the message.
5. It is a **special method of exchanging keys.**
6. This algorithm generates a secret key to be used for encrypting a message.
7. Once a key is decided, both the sender and receiver can encrypt and decrypt the message using same key.

ALGORITHM:

Consider A and B are two users.

- A and B will take two large prime numbers "n" & "g".
- A will choose any large random number say "x".
- A will then compute $\mathbf{m = g^x \bmod n}$.
- Similarly B will choose any independent large random number say "y".
- It the compute $\mathbf{s = g^y \bmod n}$.
- A will send "m" to B and B will send "s" to A.
- Key for A: $\mathbf{K_1 = s^x \bmod n}$
- Key for B: $\mathbf{K_2 = m^y \bmod n}$
- Both the key K_1 and K_2 are equal i.e. $K = K_1 = K_2$

EXAMPLE:

A	B
A choose x = 3	B choose y = 6
$M = g^x \bmod n.$	$S = g^y \bmod n.$
$= 7^3 \bmod n$	$= 7^6 \bmod n$
= 343 mod 11	= 117649 mod 11
M = 2	S = 4
A sends M = 2 to B	B send S = 4 to A
$K_1 = s^x \bmod n$	$K_2 = m^y \bmod n$
$= 4^3 \bmod 11$	$= 2^6 \bmod 11$
= 64 mod 11	= 64 mod 11
$K_1 = 9$	$K_2 = 9$

$\therefore K = K_1 = K_2 = 9$

DRAWBACKS:

- Diffie-Hellman key exchange is vulnerable to a man in the middle attack.
- Diffie-Hellman Algorithm cannot be used to encrypt messages, it can only be used to establishing a secret key.
- Expensive exponential operations are involved.
- This algorithm is also a **lack of authentication.**

Q8] Explain Diffie-Hellman Key exchange algorithm with suitable example. Also explain the problem of MIM attack in it

Ans:

[10M – May

DIFFIE-HELLMAN KEY EXCHANGE ALGORITHM:

Refer Q7.

PROBLEM OF MIM ATTACK IN DIFFIE-HELLMAN KEY EXCHANGE ALGORITHM:

- MIM stands for **Man in Middle Attack.**
- The Diffie-Hellman key exchange is vulnerable to a man-in-the-middle attack.
- In this attack, an opponent Carol intercepts Alice's public value and sends her own public value to Bob.
- When Bob transmits his public value, Carol substitutes it with her own and sends it to Alice.
- Carol and Alice thus agree on one shared key and Carol and Bob agree on another shared key.
- After this exchange, Carol simply decrypts any messages sent out by Alice or Bob, and then reads and possibly modifies them before re-encrypting with the appropriate key and transmitting them to the other party.
- This vulnerability is present because Diffie-Hellman key exchange does not authenticate the participants.
- Possible solutions include the use of digital signatures and other protocol variants.
- Figure 4.1 shows the MIM attack in Diffie Hellman Algorithm.

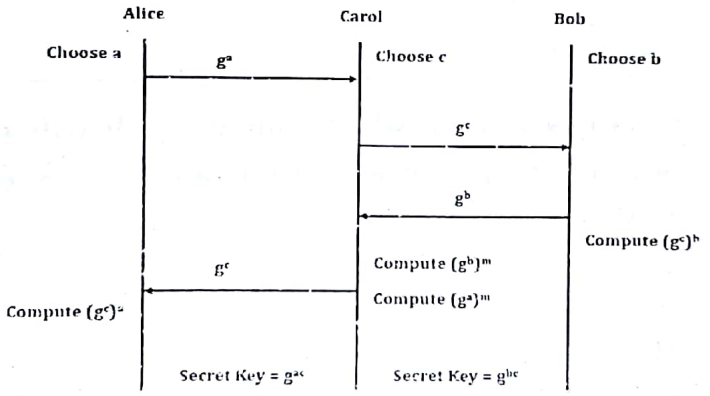


Figure 4.1: Man in Middle Attack in Diffie Hellman Algorithm.

Q9] A and B decide to use Diffie Hellman Algorithm to share a key. They choose P = 23 and G = 5 as the public parameters. Their secret keys are 6 and 15 respectively. Compute the secret key that they share.

[10M – May16 & Dec16]

Ans:

*** Note: Explain what Diffie Hellman Algorithm is before soiving any Diffie Hellman Example. For Diffie Hellman Algorithm Theory refer Q7 ***

Given:

Public parameter (P = 23 & G = 5)

Secret Keys 6 & 15 i.e. x = 6 & y = 15

To Calculate: Secret Key shared between A & B i.e. K

Solution:

A	B
A choose x = 6	B choose y = 15
M = g^x mod p.	S = g^y mod p.
= 5^6 mod 23	= 5^{15} mod 23
= 15625 mod 23	= 30517578125 mod 23
M = 8	S = 19
A sends M = 8 to B	B send S = 19 to A
$K_1 = s^x$ mod p	$K_2 = m^y$ mod p
= 19^6 mod 23	= 8^{15} mod 23
= 47045881 mod 23	= 35184372088832 mod 23
K_1 = 2	K_2 = 2

$\therefore K = K_1 = K_2 = 2$

Therefore, A & B Share Secret Key as 2

Q10] What are the various ways in which public key distribution is implemente Explain the working of public key certificates clearly detailing the role certificate authority.

Ans: **[10M – Mayı**

PUBLIC KEY DISTRIBUTION:

- In public key cryptography, only public key needs to be distributed, whereas private key is kep secret.
- Following are the ways in which public keys can be distributed:

I) Public Announcement:

- One of the simplest approach to distribute public keys is to **announce it publicly.**
- One can display his/her public key on his/her website or advertise it in local or nationa newspaper.
- For Example: When Rutuja wants to send a confidential message to Tanvi, she can obtain Tanvi's public key either from her website or from newspaper and then encrypt the message using it.
- Figure 4.2 describes the situation.

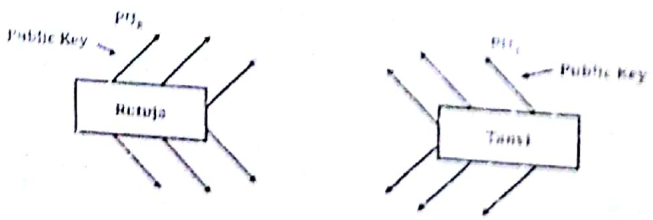


Figure 4.2: Announcement of public key.

Drawbacks:

The announced public key can be forged i.e. man in the middle attack is possible.

II) Publicly Available Directory:

- A better security approach is to maintain a publicly available directory of public keys, which is updated dynamically.
- It is the responsibility of some trusted center or organization to maintain and distribute the directory.
- The concept of directory is as follows:
  - The directory contains (name, public key) pair for each user.
  - Each user registers a public key with directory authority.
  - A user can also modify the public key as and when needed.
  - The directory can also be accessed electronically by the users.
- Figure 4.3 shows maintenance of public key directory.

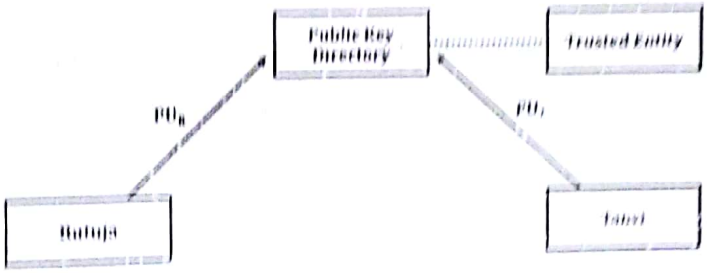


Figure 4.3: Maintenance of public key directory.

Drawback:

An adversary/intruder may obtain the private key of directory authority and impersonate any user. Thus, the messages are disclosed to intruder.

III) Public Key Authority:

- A higher level of security for public key distribution can be achieved if tighter control on distribution of public keys is provided.
- To prevent interception and modification of the response, public key announcements include a timestamp T which is signed by an authority.
- **For Example:** If Rutuja wants to know the public key of Tanvi, she sends a time stamped message to the public key authority containing (name, timestamp)
- The authority then responds with a message which is encrypted by using its private key.
- The encrypted message contains following:
  - Tanvi's public key.
  - Original request made by Rutuja.
  - The timestamp.
- Now, to verify the timestamp, Rutuja decrypts the message using authority's public key.

- After decryption, Rutuja gets Tanvi's public key.
- The procedure is described in figure 4.4.

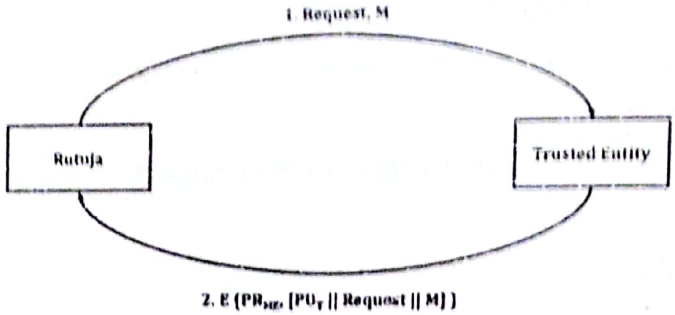


Figure 4.4: Distribution of public key through authority.

Drawback:

- Public keys maintained by authority are vulnerable to modification.
- Public key authority gets overloaded if the number of requests is large.

IV) Public Key Certificates:

- The alternative to previous approach is to create public key certificates.
- Using the public key certificates, users can exchange the keys without contacting a public ke authority.
- The certificates consists of:
  - A public key.
  - An identification of key owner.
- This certificate is signed by a certificate authority such as a government agency, a financia institution or a state organization.
- Consider for **Example:** Rutuja wants to distribute her public key in a secure manner.
- She can present her public key to certificate authority (CA), obtain a certificate and then publish the certificate.
- Now, one who wants the public key of Rutuja, can obtain the certificate and also verify that the certificate has originated from CA. (i.e. the certificate is valid and original).
- One can also transmit a certificate to convey the key to those who requested it.
- Figure 4.5 shows distribution of public key using certificates.

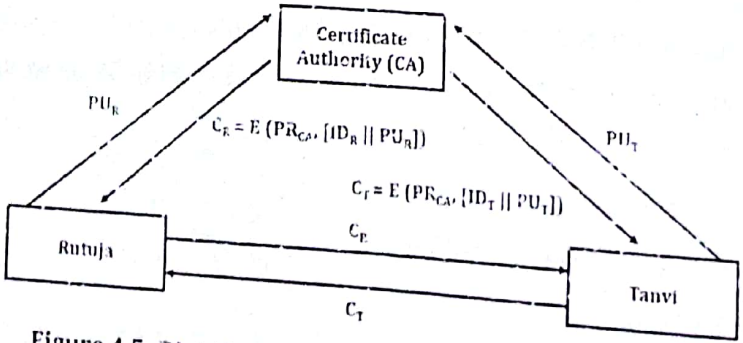


Figure 4.5: Distribution of public key using certificates.

Where,

PU_R = Public key of Rutuja.

PU_T = Public key of Tanvi.

C_R = Certificate issued for Rutuja.

C_T = Certificate issued for Tanvi.

CHAPTER - 5: CRYPTOGRAPHIC HASH FUNCTIONS

Q1] What is a digital signature? Explain any digital signature algorithm in detail.

[10M – May16 & 5M – Dec16]

Ans:

DIGITAL SIGNATURE:

1. Digital Signature is a **type of electronic signature.**
2. It encrypts documents with digital codes that are particularly difficult to duplicate.
3. A digital signature takes the concept of traditional paper-based signing and turns it into an electronic "fingerprint."
4. This "fingerprint," or coded message, is unique to both the document and the signer and binds them together.
5. It is used to **validate the authenticity and integrity of a message**, software or digital document.
6. Digital signature technique is based on public key cryptography with a difference.
7. In public key cryptography a pair of keys are used, one public key and one private key.
8. The public key is often used for message encryption, and the private key is often used for decrypting the message.
9. However in case of digital signature, message is encrypted with the private key and decrypted with the public key.
10. Only a specific person with the corresponding private key can encrypt the message or in other words sign the message.
11. However any party who has the signatory's public key can encrypt the message, in other words can verify the message.
12. Figure 5.1 shows the processes of Digital Signature.

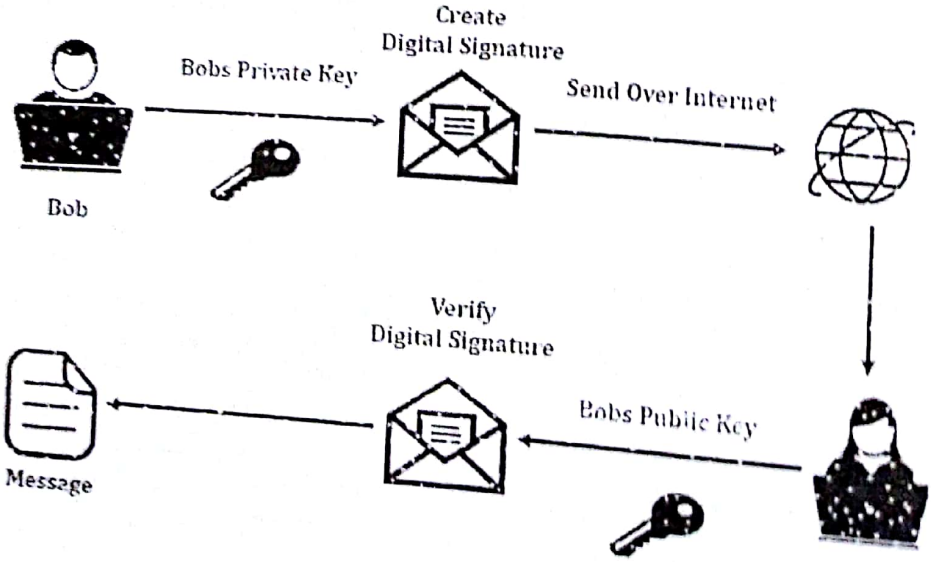


Figure 5.1: Digital Signature Process.

DSA:

1. DSA Stands for **Digital Signature Algorithm**.
2. DSA is a United States Federal Government standard for digital signatures.
3. It is used with **Digital Signature Standard (DSS)**.
4. The first part of the DSA algorithm is the public key and private key generation.
5. The second part of the DSA algorithm is the signature generation and signature verification.

Key Generation:

- Choose a prime number q, which is called the prime divisor.
- Choose another primer number p, such that p - 1 mod q = 0. Where p is called the prime modulus.
- Choose an integer g, such that

$$1 < g < p,$$

$$g^q \bmod p = 1,$$

$$g = h^{((p-1)/q)} \bmod p.$$

- Choose a secret key x by some random method, where $0 < x < q$.
- Compute public key $y = g^x \bmod p$.
- Package the public key as {p, q, g, y}.
- Package the private key as {x}.

Signature Generation:

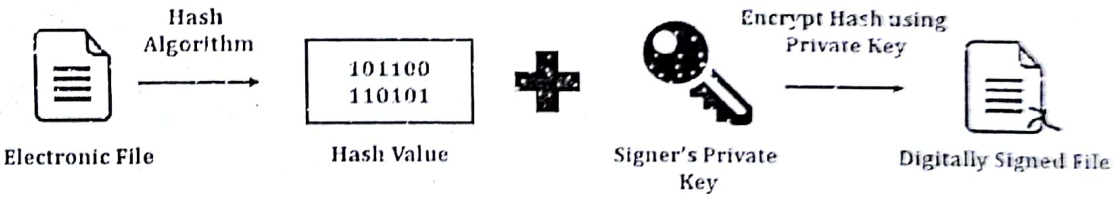


Figure 5.2: Signature Generation.

To generate a message signature, the sender can follow these steps:

- Let 'h' be the hashing function & 'm' the message.
- Generate a random number k, such that $0 < k < q$.
- Compute $r = (g^k \bmod p) \bmod q$.
- In the unlikely case that If r = 0, start again with a different random k.
- Calculate $s = k^{-1} (H(m) + xr) \bmod q$
- In the unlikely case that If s = 0, start again with a different random k.
- Package the digital signature as {r, s}.

Signature Verification:

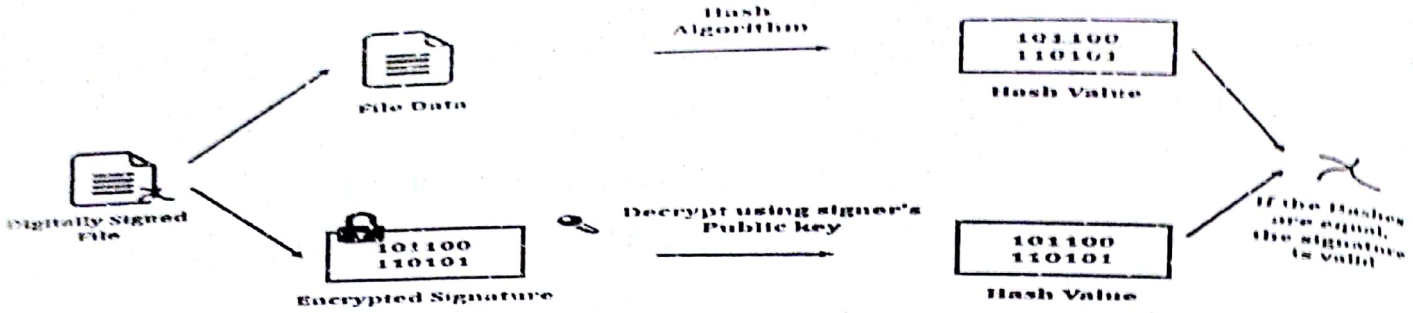


Figure 5.3: Signature Verification.

To verify a message signature, the receiver of the message and the digital signature can follow these steps:

- Let 'h' be the hashing function & 'm' the message.
- Reject the signature if $0 < r < q$ or $0 < s < q$ is not satisfied.
- Calculate $w = s^{-1} \bmod q$.
- Compute $u_1 = h(m) * w \bmod q$.
- Compute $u_2 = r * w \bmod q$.
- Compute $v = (((g^{u1})*(y^{u2})) \bmod p) \bmod q$.
- If v == r, the digital signature is valid.

Q2] Why are Digital Signatures & Digital certificates required? What is the significance of Dual Signature?

Ans:

[10M – May17]

DIGITAL SIGNATURE:

Refer Digital Signature part from Q1.

Why Digital Signatures are required:

- To provide Authenticity, Integrity and Non-repudiation to electronic documents.
- To use the Internet as the safe and secure medium for e-Commerce and e- Governance.

DIGITAL CERTIFICATES:

1. Digital Certificate (DC) is a digital file.
2. It certifies the identity of an individual or institution, or even a router seeking access to computer - based information.
3. It is issued by a **Certification Authority (CA).**
4. A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI).

5. A digital certificate may also be referred to as a **public key certificate.**

Why Digital Certificates are required:

- Digital Certificates can be used to identify a person or a device.
- Once identification is established, the Certificate is most frequently used to prove one person's, or device's identity to another person or device.
- Because of the RSA system, they both know each other.
- The Digital Certificate can now be used for signing and/or encrypting email or for providing **two-factor strong authentication.**

SIGNIFICANCE OF DUAL SIGNATURE:

1. **Dual signature** is a significant modernization of SET protocol.
2. The function of the dual signature is to **guarantee the authenticity and integrity of data.**
3. The purpose of the dual signature is to link two messages that are intended for two different recipients.
4. In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank.
5. The merchant does not need to know the customer's credit-card number, and the bank does not need to know the details of the customer's order.
6. The customer is afforded extra protection in terms of privacy by keeping these two items separate.
7. However, the two items must be linked in a way that can be used to resolve disputes if necessary.
8. The link is needed so that the customer can prove that this payment is intended for this order and not for some other goods or service.
9. To see the need for the link, suppose that the customers send the merchant two messages: a signed OI and a signed PI, and the merchant passes the Pi on to the bank.
10. If the merchant can capture another OI from this customer, the merchant could claim that this OI goes with the PI rather than the original OI
11. The linkage prevents this.
12. Figure 5.4 shows the use of a dual signature to meet the requirement of the preceding paragraph

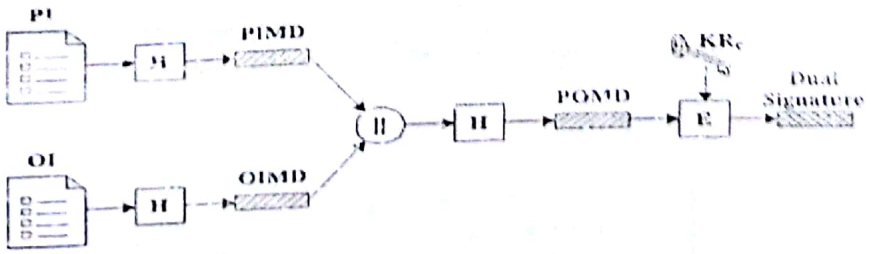


Figure 5.4: Use of a dual signature.

Where,

- PI = Payment Information.
- OI = Order Information.
- H = Hash Function.
- || = Concatenation
- PIMD = PI Message Digest
- OIMD = OI Message Digest
- POMD = Payment Order Message Digest
- E = Encryption (RSA)
- KR_c = Customer's private signature key

Q3] SHA-1 **[5M – May17]**

Ans:

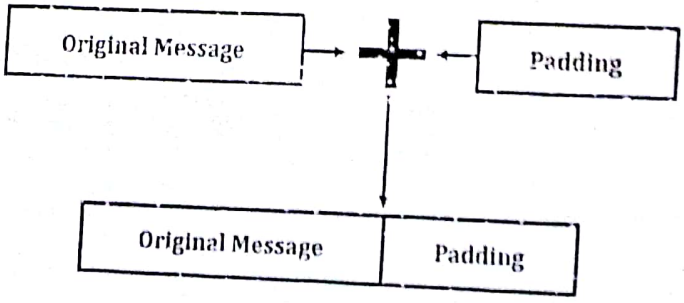
SHA-1:

1. SHA stands for **Secure Hash Algorithm.**
2. In cryptography, SHA-1 is a cryptographic hash function proposed by NIST.
3. There are three SHA algorithm named as SHA-0, SHA-1 and SHA-2.
4. SHA-1 is most widely used SHA hash function.
5. The input to SHA-1 is message of length 264 bits and its produces a 160 bits output.
6. It is similar to MD5 with following differences:
   a. It is more secure.
   b. It is little slower to execute than MD5.
   c. SHA-1 makes 5 passes whereas MD5 makes four passes.
7. SHA-1 pads the message in similar way as MD5.
8. Similar to MD5, SHA-1 also operates in stages.

ALGORITHM:

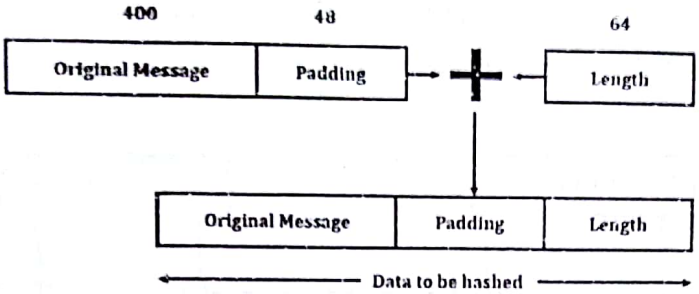
Step - 1: Append Padding Bits

- The message is padded so that its length is congruent to 448, module 512.
- Message + Padding bits + 64 should be a multiple of 512 bits.
- **Example:** If message is 400 + 64 = 464
- Hence padding = 512 – 464 = 48 padding bits.

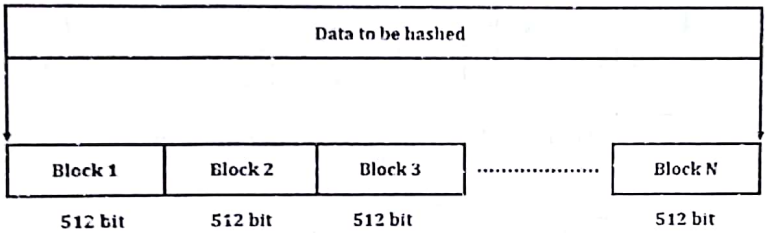


Step - 2: Append Length

- 64 bit length is appended.
- The resultant message has a length that is an exact multiple of 512 bits.



Step - 3: Divide the input into 512 bit blocks

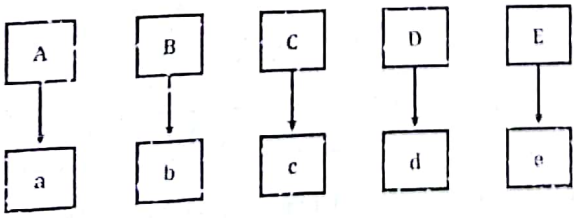


Step - 4: Initialize chaining variables

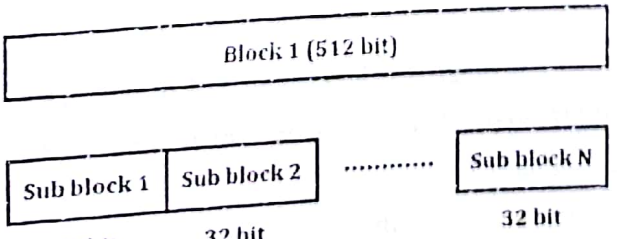
32 Bit	A	HEX	01	23	45	67
32 Bit	B	HEX	89	AB	CD	EF
32 Bit	C	HEX	FE	DC	BA	98
32 Bit	D	HEX	76	54	32	10
32 Bit	E	HEX	C3	D2	E1	F0

Step – 5: Process block

5.1: Copy chaining variable to five corresponding variables a, b, c, d and e.



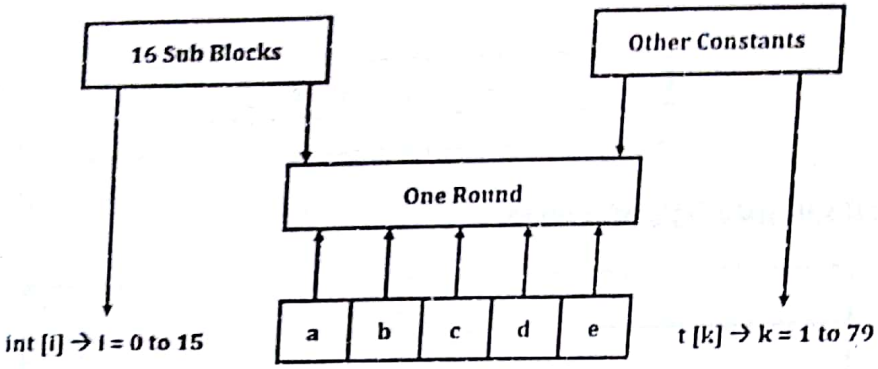
5.2: Divide current 512 bit block into 16 sub blocks.



5.3: We have four rounds

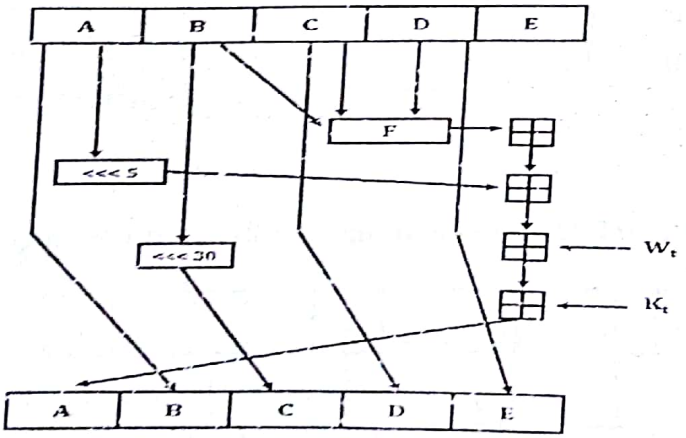
In each round consist of:

a) All 16 sub-block.
b) Variables a, b, c, d and e.
c) Some constant.



Process round	In each round process p
1	(b ^ c) V (b' ^ d)
2	b ⊕ c ⊕ d
3	(b ^ c) V (b ^ d) V (c ^ d)
4	b ⊕ c ⊕ d

Step – 6: SHA-1 operation



Q4] What are the properties of hash functions? What is the role of a hash function in security?

Ans: [5M – Dec17]

HASH FUNCTION:

1. A hash function is a mathematical function that converts a numerical input value into another compressed numerical value.
2. The input to the hash function is of **arbitrary length** but output is always of **fixed length**.
3. Values returned by a hash function are called **message digest** or simply **hash values**.

4. Hash functions are extremely useful and appear in almost all information security applications.

PROPERTIES OF HASH FUNCTIONS:

I) **Pre-Image Resistance:**

- This property means that it should be computationally hard to reverse a hash function.
- In other words, if a hash function h produced a hash value z, then it should be a difficult process to find any input value x that hashes to z.
- This property protects against an attacker who only has a hash value and is trying to find the input.

II) **Second Pre-Image Resistance:**

- This property means given an input and its hash, it should be hard to find a different input with the same hash.
- In other words, if a hash function h for an input x produces hash value h(x), then it should be difficult to find any other input value y such that h(y) = h(x).
- This property of hash function protects against an attacker who has an input value and its hash, and wants to substitute different value as legitimate value in place of original input value.

III) **Collision Resistance:**

- This property is also referred to as **collision free hash function.**
- This property means it should be hard to find two different inputs of any length that result in the same hash.
- In other words, for a hash function h, it is hard to find any two different inputs x and y such that h(x) = h(y).
- This property makes it very difficult for an attacker to find two input values with the same hash.

IV) **Other Properties:**

- **Compression:** Output length is small.
- **Efficiency:** h(x) easy to compute for any x.
- **One-way:** Given a value y, it should be infeasible to find an x such that h(x) = y
- **Weak collision resistance:** Given x and h(x), infeasible to find y != x such that h(y) = h(x)
- **Strong collision resistance:** Infeasible to find any x and y, with x != y such that h(x) = h(y)

ROLE:

I) **Password Storage:**

- Hash functions provide **protection to password storage.**
- Instead of storing password in clear, mostly all logon processes store the hash values of passwords in the file.

II) **Data Integrity Check:**

- Data integrity check is a most common application of the hash functions.
- It is used to generate the checksums on data files.
- It provides assurance to the user about correctness of the data.

Q5] What characteristics are needed in secure hash function? Explain the operati of secure hash algorithm on 512 bit block

[10M – May

Ans:

CHARACTERISTICS ARE NEEDED IN SECURE HASH FUNCTION:

Refer Q4 (Properties of Secure Hash Function Part)

OPERATION OF SECURE HASH ALGORITHM ON 512 BIT BLOCK (SHA – 1):

Refer Q3.

Q6] What is the need for message authentication? List various techniques used fo message authentication. Explain any one

[10M – May18

Ans:

NEED FOR MESSAGE AUTHENTICATION:

1. Message authentication ensures that the message has been sent by a genuine identity and not b an imposter.
2. Message authentication is used to verify:
   a. Received message is from alleged source.
   b. Message has not been altered.
   c. There is no change in message sequence.
   d. Message is not delayed or a replay.
3. Message authentication includes mechanism for non-repudiation by source.
4. Message authentication is typicaliy achieved by using **message authentication codes (MACs), authenticated encryption (AE)** or digital signatures.

MESSAGE AUTHENTICATION CODE (MAC):

1. MAC algorithm is a **symmetric key cryptographic technique.**
2. It is used to provide message authentication.
3. A MAC uses a keyed hash function that includes the symmetric key between the sender and receiver when creating the digest.
4. For establishing MAC process, the sender and receiver share a symmetric key K.

5. Essentially, a MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication.
6. The process of using MAC for authentication is shown in figure 5.5.

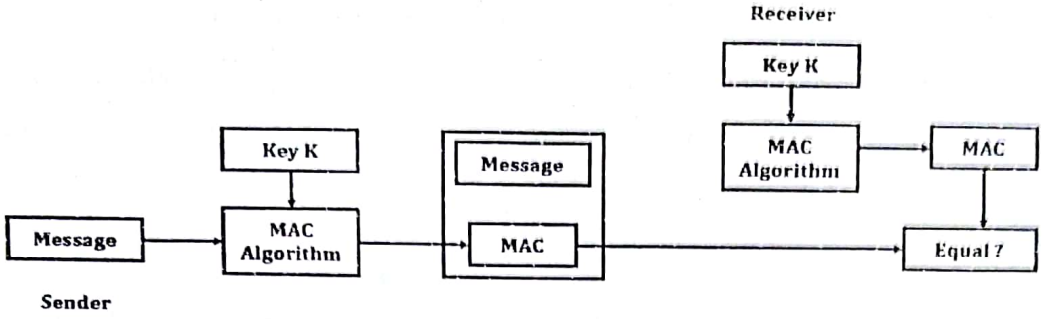


Figure 5.5: MAC Process.

WORKING:

- Figure 5.5 shows how a sender uses a keyed hash function to **authenticate his message** and how the receiver can verify the **authenticity of the message.**
- This system makes use of a symmetric key shared by sender and receiver.
- Sender use the symmetric key and a keyed hash function to generates a MAC.
- Sender then sends this MAC along with the original message to receiver.
- Receiver receives the message and the MAC and separates the message from the MAC.
- Receiver then applies the same keyed hash function to the message using the same symmetric key to get a fresh MAC.
- Receiver then compares the MAC sent by sender with the newly generated MAC.
- If they match, then the receiver accepts the message and assures himself that the message has been sent by the intended sender.
- If the computed MAC does not match the MAC sent by the sender, the receiver cannot determine whether it is the message that has been altered or it is the origin that has been falsified.
- As a bottom-line, a receiver safely assumes that the message is not the genuine.

Q7] Compare and contrast: KDC versus CA.

Ans: [5M – Dec16]

Table 5.1: Comparison between KDC versus CA.

KDC	CA
KDC Stands for Key Distribution Center.	CA Stands for Certificate Authority
It is **symmetric** key solution against active attacks.	It is **asymmetric** key solution against active attacks.
It is less secure.	It is more secure.

It has single point failure.	No single point failure.
KDC has to be online.	CA does not have to be online.
KDC can scale up to hundreds.	CA has better scalability
Everyone who register with KDC shares a secret key.	Everyone who register with CA obtains certificate for its public key.
It is more expensive.	It is less expensive.
It is performance sensitive.	It is not performance sensitive.
Preferred for LANs.	Preferred for WANs.

Q8] Differentiate between MD-5 and SHA.

Q9] MD-5 versus SHA

Ans: [Q8 | 5M – Dec15, Dec16 & May18] & [Q9 | 5M – Dec

Table 5.2: Comparison of MD-5 & SHA.

Points	MD-5	SHA
Message Digest Length	128 Bits.	160 Bits.
Security	Less Secure than SHA.	Considered more secure than MD-5
Speed	Faster, only 64 Iterations.	Slower than MD-5, Required Iterations.
Format	Little endian format used to store values.	Big endian format used to store va
Buffers Used	4 buffers of 32 bits each.	5 buffers of 32 bits each.
Attack required to find out original message	2^{128} bit operations required to break.	2^{160} bit operations required to bre
Collision	Collision attack exist	Collision ratio is less than MD-5
Pass	It requires 4 passes.	It requires 5 passes.
Rounds	64 Rounds.	20 Rounds.
Cryptanalytic Attack	Vulnerable to cryptanalysis attack.	Non-Vulnerable to cryptanalysis

CHAPTER - 6: AUTHENTICATION APPLICATIONS

Q1] Give the format of X.509 digital certificate and explain the use of a digital signature in it.

Ans: **[5M – Dec15]**

X.509:

1. X.509 is an important standard for a **Public Key Infrastructure (PKI).**
2. It is used to **manage Digital Certificates & Public Key Encryption.**
3. X.509 are the building blocks a PKI system that defines the standard formats for certificates and their use.
4. Figure 6.1 shows the format of X.509 Digital Certificate. (CA – Certificate Authority)

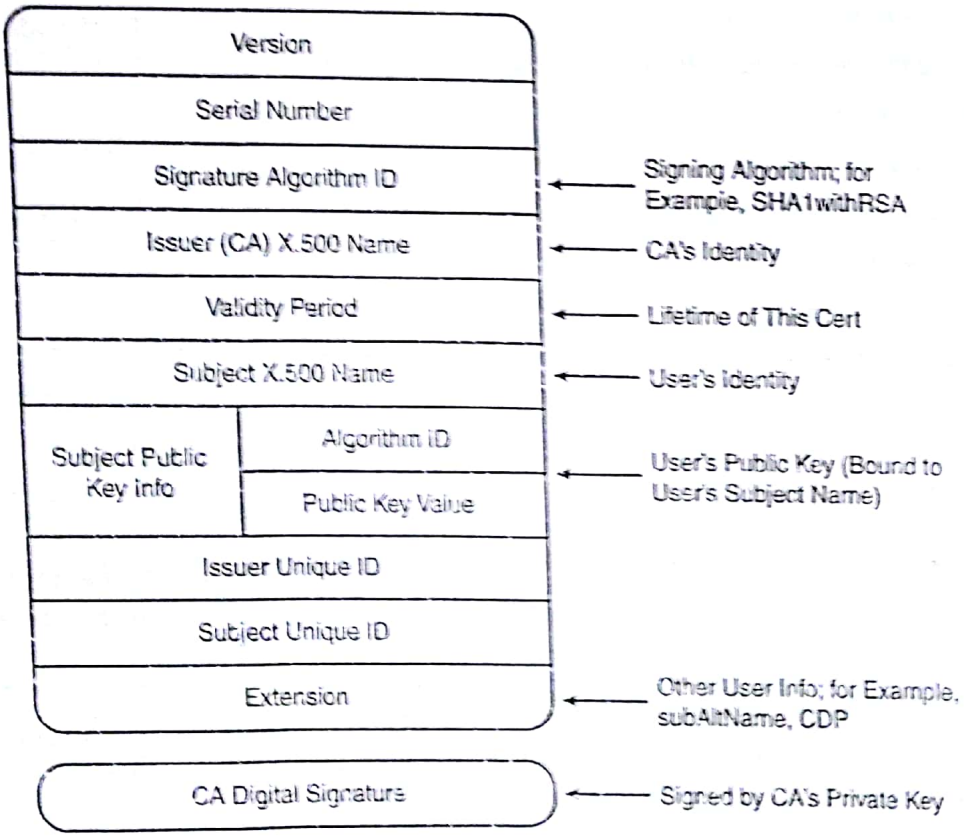


Figure 6.1: Format of X.509 Digital Certificate.

USE OF DIGITAL SIGNATURE:

- Digital Signature in X.509 Digital Certificate can be used to access secured zones of websites.
- It is used for verification & validation purpose.
- It ensures confidentiality of certificate.
- It can also be used to verify validity period & Unique ID.

Q2] **What is a digital certificate? How does it help to validate the authenticity of a user? Explain the X.509 certificate format**

[10M – Dec17]

Ans:

DIGITAL CERTIFICATE:

1. Digital Certificate (DC) is a digital file.
2. Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender.
3. It is issued by a Certificate Authority (CA) to verify the identity of the certificate holder.
4. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information.
5. Digital signature is used to attach public key with a particular individual or an entity.
6. Digital certificate contains:
   a. Name of certificate holder.
   b. Serial number which is used to uniquely identify a certificate, the individual or the entity identified by the certificate
   c. Expiration dates.
   d. Copy of certificate holder's public key.
   e. Digital Signature of the certificate issuing authority.

CERTIFICATE BASED AUTHENTICATION:

1. Certificate based authentication is based on the digital certificates of the user.
2. In Public Key Infrastructure (PKI), the digital certificates are used for secure digital transactions.
3. The digital certificates in PKI can also be re-used for user authentication as well.
4. This is a stronger mechanism as compared to password based authentication.
5. Figure 6.2 shows certificate based authentication process.

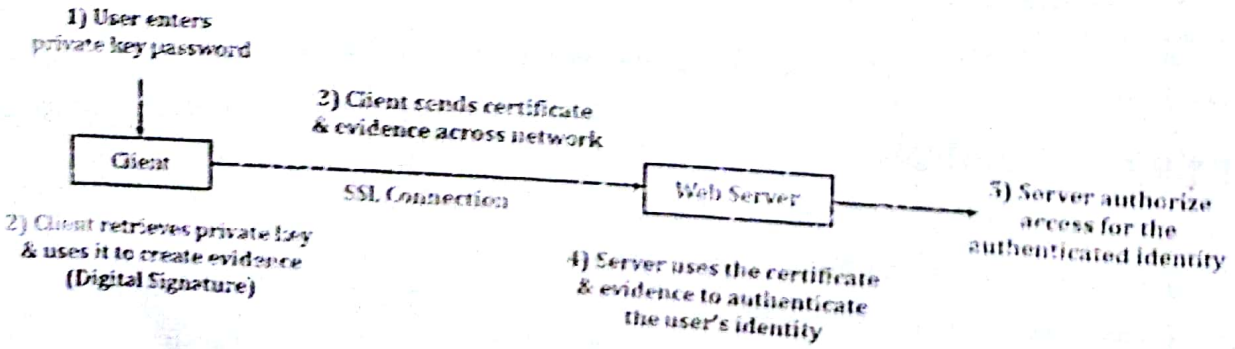


Figure 6.2: Certificate based authentication process.

WORKING:

1. The client software maintains a database of the private keys that correspond to the public keys published in any certificates issued for that client.
2. The client asks for the password to this database the first time the client needs to access it during a given session, such as the first time the user attempts to access an SSL-enabled server that requires certificate-based client authentication.
3. After entering this password once, the user does not need to enter it again for the rest of the session, even when accessing other SSL-enabled servers.
4. The client unlocks the private-key database, retrieves the private key for the user's certificate, and uses that private key to sign data randomly-generated from input from both the client and the server.
5. This data and the digital signature are evidence of the private key's validity.
6. The digital signature can be created only with that private key and can be validated with the corresponding public key against the signed data, which is unique to the **SSL session.**
7. The client sends both the user's certificate and the randomly-generated data across the network.
8. The server uses the certificate and the signed data to authenticate the user's identity.
9. The server may perform other authentication tasks, such as checking that the certificate presented by the client is stored in the user's entry in an LDAP directory.
10. The server then evaluates whether the identified user is permitted to access the requested resource.
11. If the result of the evaluation is positive, the server allows the client to access the requested resource.

X.509 CERTIFICATE FORMAT:

Refer Q1.

Q3] Email Security.

Ans: **[5M – May16]**

EMAIL SECURITY:

1. E-Mail Stands for **Electronic Mail.**
2. Electronic mail is most widely used application on the internet to send and receive messages to other users.
3. Due to this the security of email messages has become an extremely important issue.
4. The Simple Mail Transfer Protocol (SMTP) is used for email communication.
5. The three main email security protocols used are as follows:

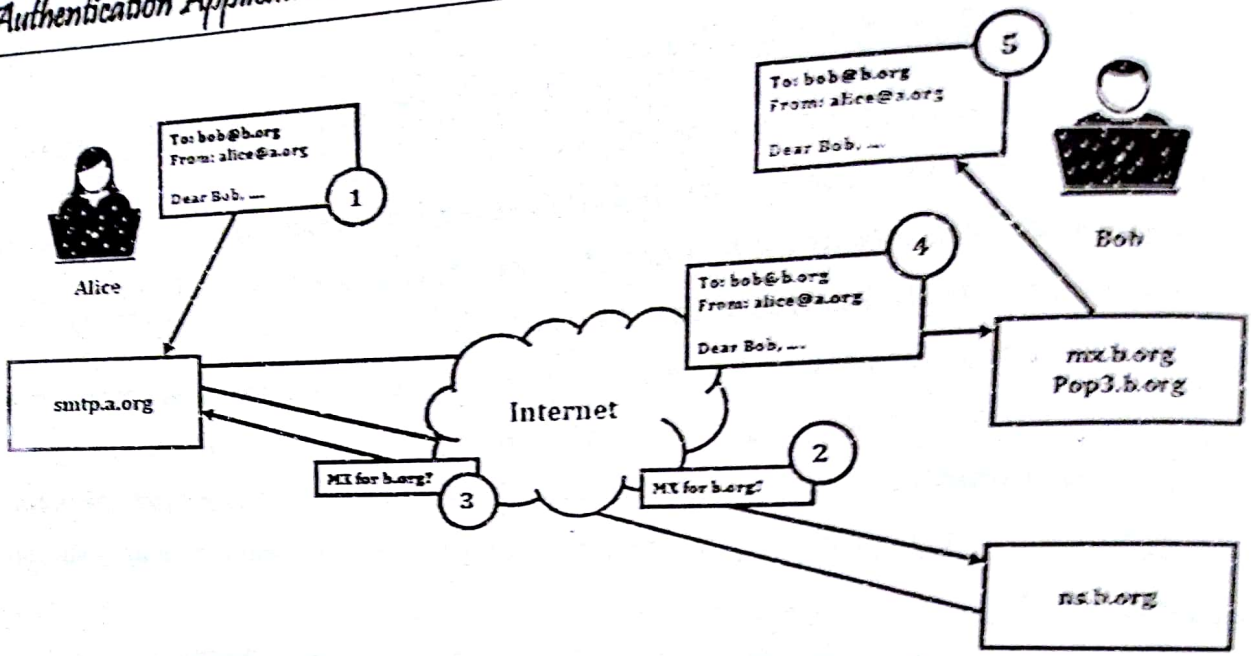


Figure 6.3: Email Security.

I) **Privacy Enhanced Mail (PEM):**

- Privacy Enhanced Mail is an **Internet Standard for Protecting Email.**
- It was adopted by Internet Architecture Board (IAB).
- PEM supports the three main functions of encryption, non-repudiation and message integrity.
- In PEM, Message is DES Encrypted.
- **Authentication** is provided using MD-5.

II) **Pretty Good Privacy (PGP):**

- Pretty Good Privacy (PGP) is widely used **Email cryptosystem.**
- PGP provides authentication through the use of Digital Signature.
- It provides **confidentiality** through the use of symmetric block encryption.
- It provides compression using Zip Algorithm.
- The most significant aspects of PGP are that it supports the basic requirements of cryptography which is quite simple to use and is free along with its source code and documentation.

III) **Secure Multipurpose Internet Mail Extensions (S/MIME):**

- MIME system extends the basic email system by permitting users to send binary files using the basic email system.
- S/MIME is a security enhancement to the MIME Internet Email format Standard.
- S/MIME is similar to PGP which provides digital signatures and encryption of email messages.

Q4] How does PGP achieve confidentiality and authentication in emails?

Q5] How is confidentiality achieved in emails using either S/MIME or PGP?

Ans:

[5M – Dec15 & Dec16]

PGP:

1. PGP Stands for **Pretty Good Privacy.**
2. It is an open-source, freely available software package for e-mail security.
3. It provides Authentication through the use of digital signature and confidentiality through the use of symmetric block encryption.
4. It also provides **Compression using the ZIP algorithm.**

PGP ACHIEVE CONFIDENTIALITY AND AUTHENTICATION IN EMAILS:

- Figure 6.4 shows the Confidentiality & Authentication in Emails using PGP.
- First, a signature is generated for the plaintext message and prepended to the message.
- Then the plaintext message plus signature is encrypted using CAST-128 (or IDEA or 3DES).
- Session key is then encrypted using RSA.
- In summary, when both services are used, the sender first signs the message with its own private key.
- Then the sender encrypts the message with a session key, and finally encrypts the session key with the recipient's public key.

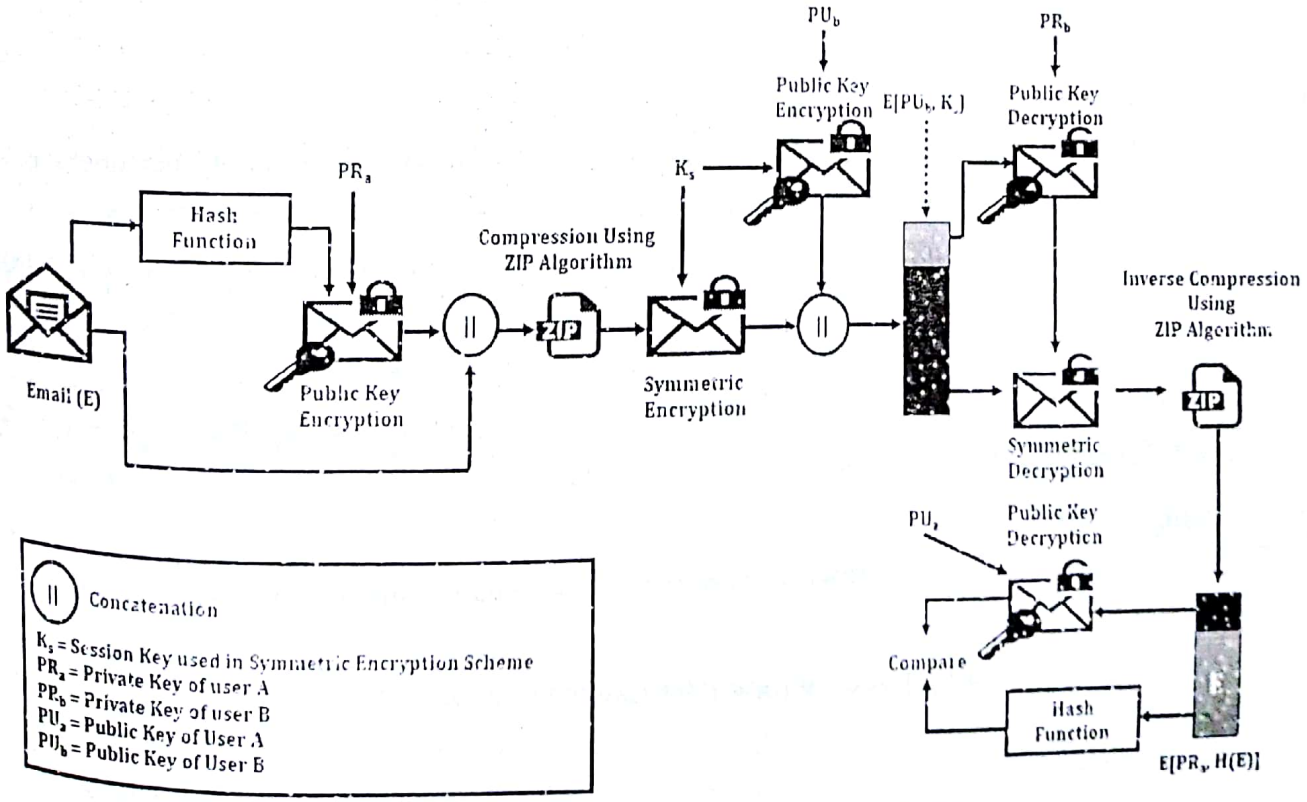
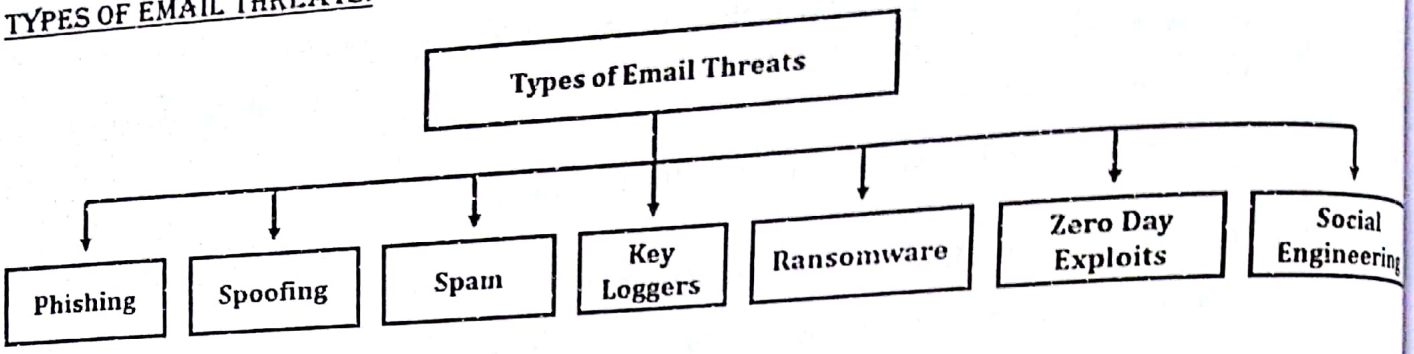


Figure 6.4: Authentication & Confidentiality in PGP.

Q6] What are the different threats to emails? Give an algorithm to secure emails being sent from user A to user B **[10M – May18]**

Ans:

TYPES OF EMAIL THREATS:



I) **Phishing:**

- Phishing is an example of social engineering techniques used to deceive users, and exploits weaknesses in web security.
- Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons.
- A phishing attack usually consists of an authentic-looking sender and a socially engineered message.
- Many email recipients believe the message is from a trusted individual and will open infected attachments or click on malicious links.

II) **Spoofing:**

- A spoofing attack is a situation in which a person or program successfully masquerades as another by falsifying data, to gain an illegitimate advantage.
- Because email protocols lack effective mechanisms for authenticating email addresses, hackers are able to use addresses and domains that are very similar to legitimate ones, deceiving victims into believing that fraudulent emails are from a trusted individual.
- Criminals may spoof an individual mailbox sagarnarkar@topperssolutions.com to sagarnarkaar@topperssolutions.com.

III) **Spam:**

- Despite a number of ways to filter out unwanted email, spam remains a significant challenge for organizations.
- While ordinary spam is simply considered a nuisance, spam is also frequently used to deliver malware.
- Ransomware, for example, is most commonly delivered via spam, and it behooves all organizations to carefully evaluate spam for dangerous intent.

IV) **Key Loggers:**

- In the most damaging data breaches, the criminals behind the attacks nearly always utilize stolen user credentials.
- One effective method criminals use to obtain IDs and passwords is a key logger, often delivered by email when victims inadvertently click on a malicious attachment or link.
- Read Password Stealing Malware Remains Key Tool for Cybercriminals to learn more about key loggers.

V) **Ransomware:**

- Ransom malware, or ransomware, is a type of malware.
- It prevents users from accessing their system or personal files and demands ransom payment in order to regain access.

VI) **Zero-Day Exploits:**

- A zero-day vulnerability refers to a security weakness that is unknown to the software developer.
- The security hole is exploited by hackers before the vendor has created a fix.
- Zero-day attacks are frequently delivered via malicious emails, and hackers use them to gain unauthorized access and steal sensitive information.

VII) **Social Engineering:**

- Cybercriminals use social engineering to build trust before stealing user logon credentials or confidential data.
- In a social engineering attack, a computer criminal poses as a trusted individual (IT support, human resource, outside contractor, etc.) and engages in a conversation to gain access to a company's network.
- The attacker deceives the victim into divulging IDs, passwords, and sensitive information, or dupes them into performing a fraudulent transaction.

ALGORITHM TO SECURE EMAILS BEING SENT FROM USER A TO USER B (PGP):

Refer Q4.

Q7] Why is the segmentation and reassembly function in PGP (Pretty Good Privacy) needed

[5M – May18]

Ans:

SEGMENTATION & ASSEMBLY IN PGP:

1. E-mail facilities are often restricted to a maximum message length.
2. For example, many of the facilities accessible throughout the Internet impose a maximum length of 50,000 octets.

3. Any message longer than that must be broken up into smaller segments, each of which is mailed separately.
4. To accommodate this restriction, PGP automatically subdivides a message that is too large into segments that are small enough to send via e-mail.
5. The segmentation is done after all the other processing, including the radix-64 conversion.
6. Thus the session key component and signature component appear only once, at the beginning of the first segment.
7. At the receiving end, PGP must strip off all e-mail headers and reassemble the entire original block before performing the steps illustrated in figure 6.5.

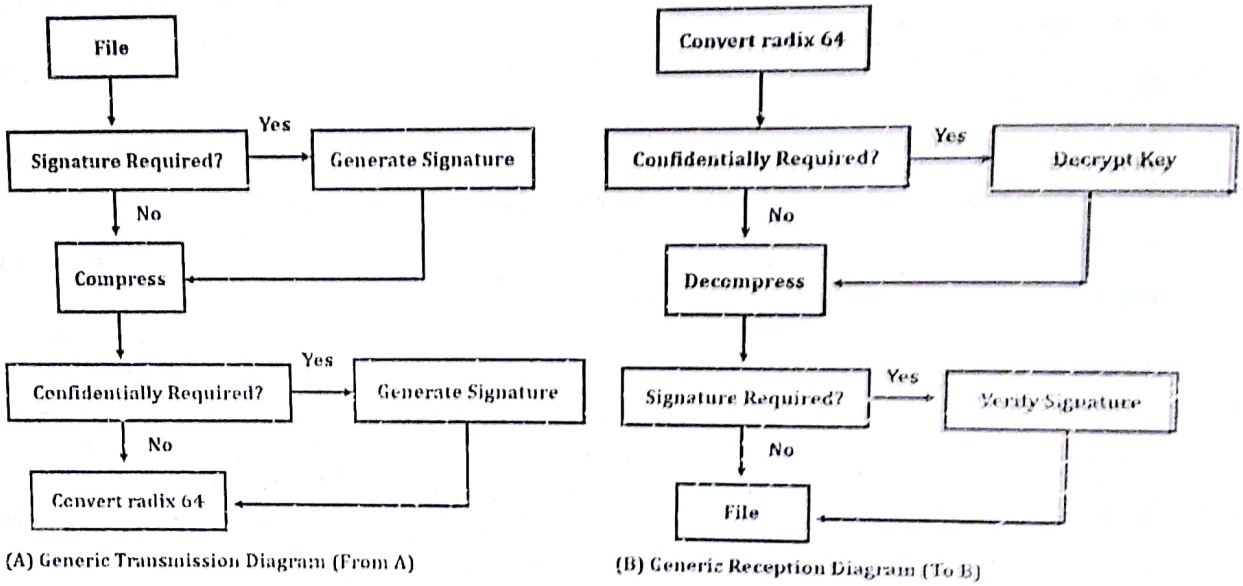


Figure 6.5: Transmission and Reception of PGP messages.

Q8] Explain key rings in PGP

Ans:

[5M – May17]

PGP:

1. PGP Stands for **Pretty Good Privacy**.
2. It is an open-source, freely available software package for e-mail security.
3. It provides Authentication through the use of digital signature and confidentiality through the use of symmetric block encryption.
4. It also provides **Compression** using the **ZIP algorithm**.

KEY RINGS IN PGP:

1. PGP uses key rings to identify the key pairs that a user owns or trusts.
2. Private-key ring contains public/private key pairs of keys he owns.
3. Public-key ring contains public keys of others he trusts.

4. Each PGP user has a pair of key rings: Public key ring and private key ring.

i) **Public-key ring:**

- PGP allows multiple public/private key pairs for each user.
- It stores other's public keys known at this node.
- Public keys can be obtained in various ways.

Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
T_i	$KU_i \bmod 2^{64}$	KU_i	Trust_flag$_i$	User$_i$	Trust_flag$_i$		
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.

Owner trust: Trust value for the key owner; assigned by the user when the user enters a new public key.

Signatures: Signatures attached to the key.

Signature trusts: Trust value for the owner of this signature attached to the key; "unknown" value is assigned if the owner is not known

Key legitimacy: The extent to which PGP will trust the key.

ii) **Private-key ring:**

- It stores the public/private key pairs owned by that node.
- Private keys are encrypted using a key based on the user's passphrase (SHA hash code of the passphrase)

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
T_i	$KU_i \bmod 2^{64}$	KU_i	$E_{H(P_i)}[KR_i]$	User$_i$
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.

Q9] Explain the working of Kerberos.

Q10] Explain Kerberos protocol that supports authentication in distributed system

[Q9 | 10M – May16] & [Q10 | 10M – May18]

Ans:

KERBEROS:

1. In Greek mythology, Kerberos is a three-headed dog that guards the entrance to the Hades.
2. Whereas In security, Kerberos is a **network authentication protocol.**
3. It is designed to provide strong authentication for Client/Server Applications by using Secret-Key (Symmetric Key) Cryptography.
4. Kerberos originated at MIT (Massachusetts Institute of Technology) which was designed for smaller scale use.
5. Kerberos is used for authentication and to establish a session key that can be used for confidentiality and integrity.

WORKING OF KERBEROS:

Figure 6.6 shows the working of Kerberos.

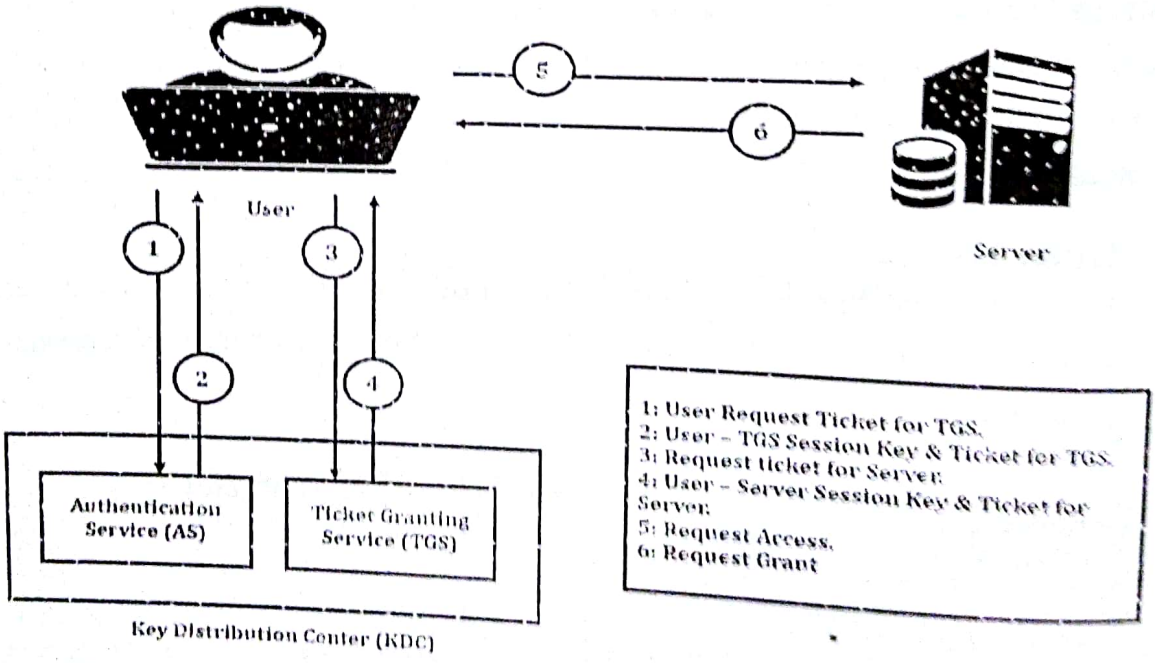


Figure 6.6: Working of Kerberos.

- Any symmetric cipher can be used with Kerberos however the crypto algorithm widely used is the Data Encryption Standard (DES).
- There are four parties involved in the Kerberos protocol:

User: The one who uses the client workstation.

Server: The server provides services for the user.

Authentication Service (AS):

- It is part of Key Distribution Center in the Kerberos protocol.
  - Each user registers with the AS and is granted a user identity and a password.
- The AS verifies the user, issues a session key to be used between User and TGS and sends a ticket to TGS.

Ticket Granting Service (TGS): Issues a ticket for the Server. It provides the session key (KAB) between User and Server.

The Three steps involved in Kerberos protocol are:

I) **Login:**

- User uses a public workstation and enters its name which is sent to the AS in plain text.
- In response, the AS first creates a package of the username and a randomly generated session key (KS).
- It encrypts this package with the symmetric key that the AS shares with the Ticket Granting Server (TGS).
- The TGT can be opened only by the TGS since it possess the corresponding symmetric key for decryption.
- The AS then combines the TGT with the session key (KS) and encrypts the two together using a symmetric key derived from the password of User (KA).
- After the message is received User's workstation asks for the password.
- When User enters it the workstation generates the symmetric key (KA) derived from the password and uses it to extract the session key (KS) and the TGT.

II) **Obtaining a service granting ticket (SGT):**

- After a successful login, User wants to make use of the server for communication.
- For this User needs a ticket to communicate with Server.
- At this juncture User's workstation creates a message intended for the ticket granting server (TGS) which contains the TGT, ID of Server and the current timestamp encrypted with the same session key (KS).
- Once the TGS is satisfied of the credentials of User, the TGS creates a session key KAB for User to have a secure communication with Server.
- TGS sends it twice to User, once combined with Server's Id and encrypted with KS and a second time combined with User's Id and encrypted with Server's secret key (KAB).

iii) **User contacts Server for access:**

- User can now send **KAB** to Server in order to enter into a session.
- Since this exchange is also desired to be secure, User can simply forward KAB encrypted with Server's secret key to Server.
- This will ensure that only Server can access KAB.
- Server now adds 1 to the timestamp sent by User, encrypts the result wit KAB and sends it to User.
- Since User and Server know KAB, User can open this packet and verify that the timestamp incremented by Server was indeed the one sent to Server in the first place.
- Now User and Server can communicate securely using the shared secret key KAB to encrypt messages.
- If User wants to communicate with another server, than User will need another shared key from the TGS and specify the name in the message.

Q11] S/MIME

Ans: **[5M – May17]**

S/MIME:

1. S/MIME Stands for **Secure/Multipurpose Internet Mail Extensions.**
2. It is a standard for **public key encryption** and signing of MIME data.
3. It was originally developed by RSA Data Security Inc.
4. S/MIME enables email security features by providing encryption, authentication, message integrity and other related services.
5. It ensures that an email message is sent by a legitimate sender and provides encryption for incoming and outgoing messages.
6. To enable S/MIME based communication, the sender and receiver must be integrated with public key and signatures issued from a certificate authority (CA).
7. A digital signature is used to validate a sender's identity, whereas a public key provides encryption and decryption services.
8. A very secure way of e-mail encryption is the S/MIME protocol.
9. X.509 certificates are used by S/MIME and can be created by the administrator or PKI trust center.
10. The user doesn't need to have any technical knowledge to use S/MIME.
11. Figure 6.7 shows S/MIME Encryption Process.

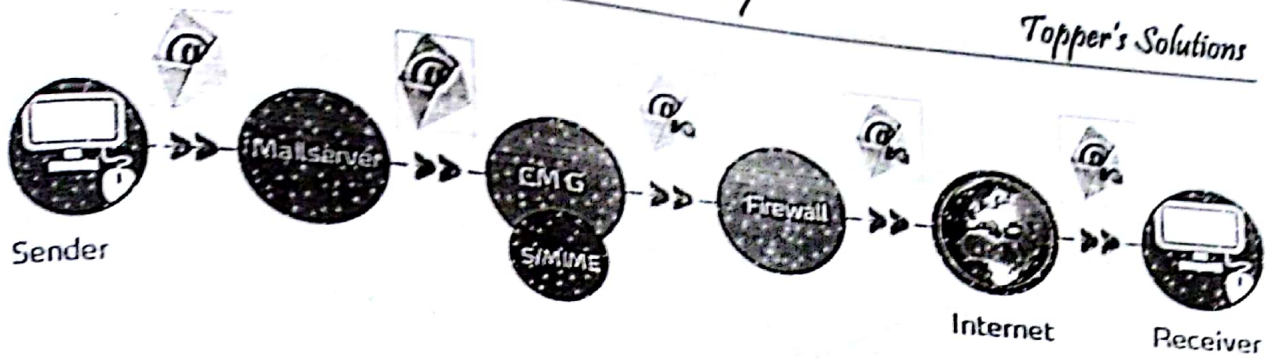


Figure 6.7: S/MIME Encryption Process.

Q12] What is a nonce in key distribution scenario? Explain the key distribution scenario if A wishes to establish logical connection with B. A and B both have a master key which they share with itself and key distribution center

Ans:

[10M – May18]

NONCE IN KEY DISTRIBUTION:

1. A nonce is an **arbitrary number** that can be used just once.
2. It is often a random or pseudo-random number issued in an authentication protocol.
3. It ensure that old communications cannot be reused in **replay attacks.**
4. Nonce can also be useful as initialization vectors and in cryptographic hash functions.
5. In key distribution scenario, nonce may be a timestamp, a counter, or a random number.
6. The minimum requirement is that it differs with each request.

KEY DISTRIBUTION:

1. Key Distribution Scenario is the important aspect of the subject information and network security.
2. The key distribution concept can be deployed in a number of ways.
3. Two parties A and B can have various key distribution alternatives:
   a. A can select key and physically deliver to B.
   b. Third party can select & deliver key to A & B.
   c. If A & B have communicated previously can use previous key to encrypt a new key.
   d. If A & B have secure communications with a third party C, C can relay key between A & B
4. The Key Distribution Scenario assumes that each user shares a unique master key with the key distribution center (KDC).
5. A typical Key Distribution Scenario is illustrated in figure 6.8.

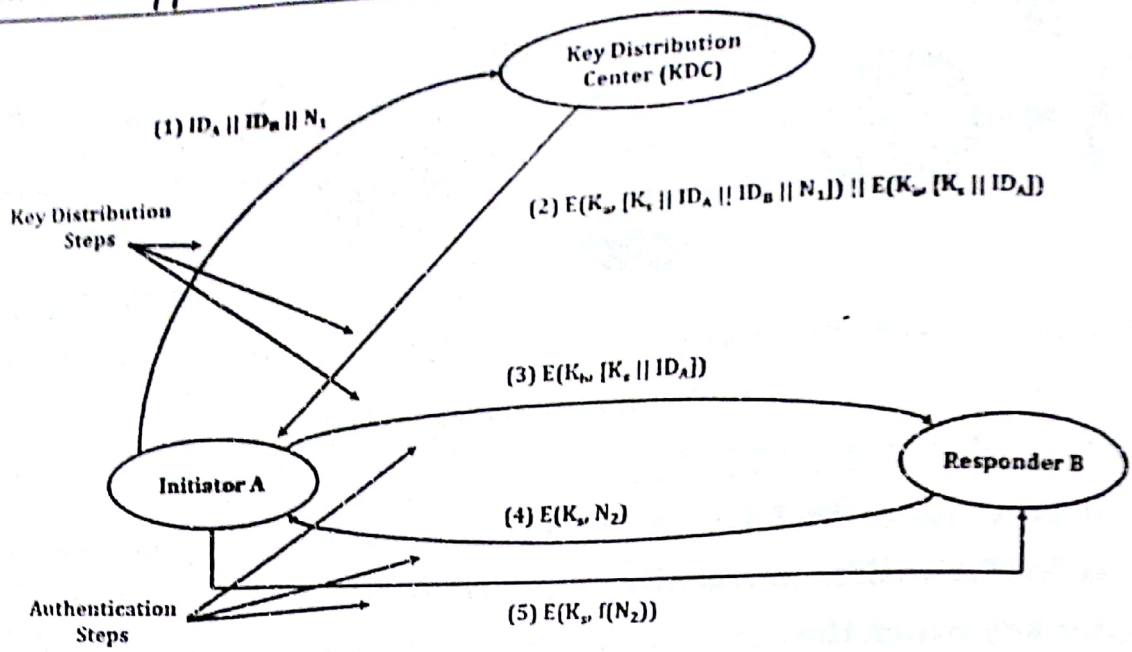


Figure 6.8: Key Distribution Scenario.

STEPS:

1. A issues a request to the KDC for a session key.
   - Nonce is also sent.
   - Nonce includes identities of communicating parties and a unique value.
2. KDC sends a response encrypted with A's secret key K_a
   - It includes one-time session key K_S
   - Original request message, including the nonce.
   - Message also includes K_S and ID of A encrypted with KB intended for B.
3. A stores K_S and forwards information for B i.e., $E(K_B, [K_S||ID_A])$
4. B sends a nonce to A encrypted with K_S
5. A responds by performing some function on nonce like incrementing.
6. The last two steps assure B that the message it received was not a replay.

KEY DISTRIBUTION ENTITIES:

I) **Key Distribution Center:**

- It provides one time session key to valid users for encryption.

II) **Front end Processor:**

- It carries out the end to end encryption.
- obtains session key from the KDC on behalf of its host.

CHAPTER - 7: SECURITY & FIREWALLS

Q1] What is a firewall? What are the firewall design principle?

Ans:

[5M – May16]

FIREWALL:

1. Firewall is the device or set of devices located at the network gateway server.
2. It can be **hardware, software or combination of both.**
3. It protects private networks from outside networks.
4. It is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.
5. The rules are nothing but the **firewall security policy.**
6. This policies specifies which traffic is authorized to pass in each direction.
7. Firewall examines each packet to determine whether to permit or deny network transmission.
8. The purpose of firewall is to filter traffic and keep malicious or unsafe information outside of a protected network.
9. Firewall is like a secretary of network.
10. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet or Wide Area Network that is assumed not to be secure or trusted as shown in figure 7.1.

Figure 7.1: Firewall.

FIREWALL CHARACTERISTICS:

I) **Service control:** Specifies what type of services can be accessed, depending on set of rules.

II) **Direction control:** Specifies the direction of initialization and flow of particular service.

III) **User control:** Specifies which particular user is allowed to access a service.

IV) **Behavior control:** Specifies behavior of the service.

FIREWALL DESIGN PRINCIPLE:

- All traffic from inside to outside and vice versa must pass through the firewall.
- Only authorized traffic as defined by the local security policy will be allowed to pass.
- To Establish a Secure Control Link.
- To protect the premises network from Internet based attacks.

Q2] What are firewalls? Explain the different types of firewalls and mention the layer in which they operate.

Q3] What are the types of firewalls? How are firewalls different from IDS?

[Q2 | 10M – Dec16] & [Q3 | 10M – May17]

Ans:

FIREWALL:

Refer Q1.

TYPES OF FIREWALLS:

1) Packet Filtering Firewall:

- A packet filtering firewall is also called as **screening router firewall.**
- It is simplest and most effective type of firewall.
- It filters the packet based on following information:
  - Source and destination IP address.
  - Source and destination Port address.
  - IP Protocol field.
- Packet filtering firewall examines packets up to the **network layer** and can only filter packets based on the information that is available at the network layer.
- A packet filter receives packets and passes them through a set of rules, if they match the rules then accept or reject.

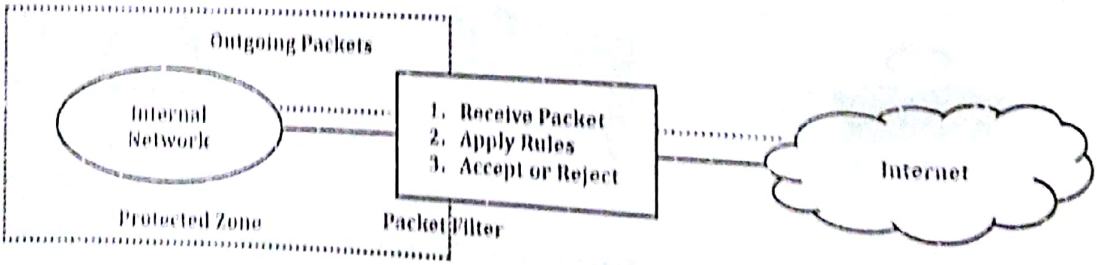


Figure 7.2: Packet Filtering Firewall.

Advantages:

- Efficiency
- Simplicity, fast speed of packet processing.
- Low cost.
- Low impact on network performance.

Disadvantages:

- They can be complex to configure.
- Have limited logging capabilities.

Application: In the area as a first line defense and in SOHO networks.

ii) Stateful Inspection Firewall:

- Unlike packet filtering firewall, Stateful firewall keeps track of state of a connection which may be initiation, data transfer or termination.
- A drawback of packet filters is that they are stateless and they have no memory of previous packets which makes them vulnerable to spoofing attacks.
- Attacker may modify the attack by splitting it into multiple packets, which goes undetected in packet filter.
- Stateful inspection firewall examines a group of packets at the same time.
- Stateful firewall operates at **network, transport & session layer** of OSI Model.

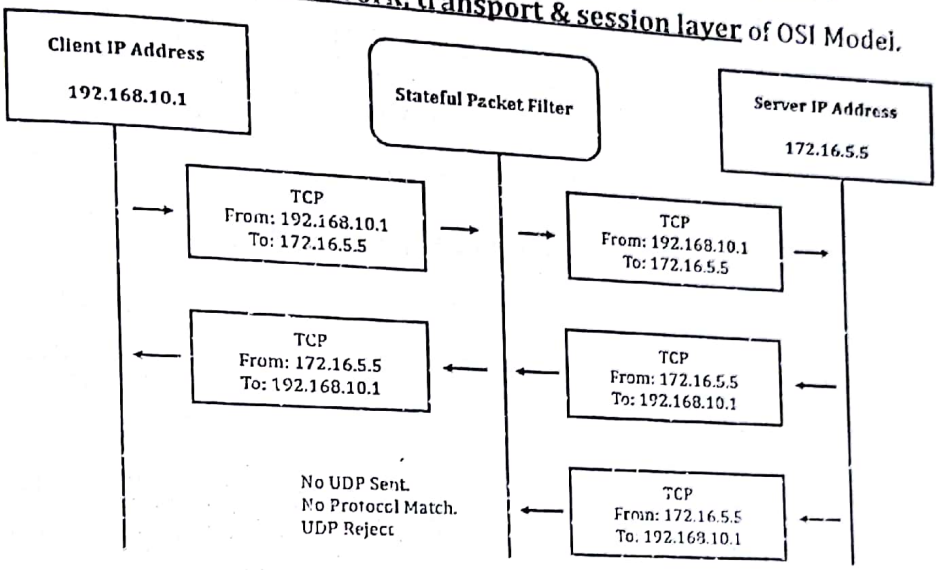


Figure 7.3: Stateful Inspection Firewall.

Advantages:

- Prevent more kinds of DoS attack than packet filter.
- Have more robust logging.

Disadvantages:

- Slower than packet filtering firewall.
- It does not prevent application layer attacks.

iii) Application Proxies Firewall:

- A proxy means acting on your behalf of something.
- An application proxy firewall processes incoming packets all the way up to the application layer.
- This firewall contains a proxy agent that acts as an intermediary between two hosts that want to communicate with each other.
- Application proxies never allow a direct connection between the two hosts and it is transparent to them.
- Each proxy agent authenticates each individual network user; with the authentication having several forms such as, user ID and password, biometrics, token matching etc.

- It also verifies the data inside the packet.
- It work on the application layer of the OSI Model.

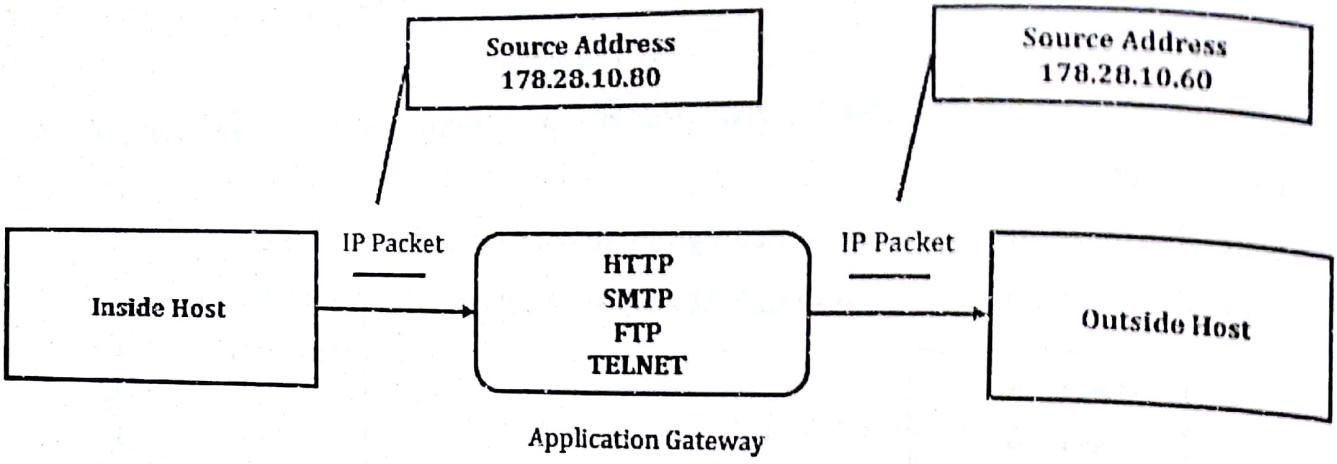


Figure 7.4: Application Proxy Firewall.

Advantages:

- It has complete view of connections and application data.
- It provides detailed logging.

Disadvantages:

- Requires special client software.
- Process intensive. They requires lot of CPU cycles and memory to process every packet that they see.

IV) **Personal Firewall:**

- It is software application used to protect a single internet connected computer from intruders.
- Personal firewall protection is useful for users with 'always-on' connections such as DSL or cable modem.
- These users are students, home users, individual workers, small businessmen etc.
- Using a separate firewall system would be expensive. To tackle this problem personal firewall are used.
- It is an application program which runs on a work station to block unwanted traffic from network.
- Personal firewall can be used with antivirus software to become more effective and efficient.
- **Example:** Norton Personal firewall from Symantec, McAfee personal firewall etc.

HOW ARE FIREWALLS DIFFERENT FROM IDS?

Refer Q4.

Q4] Differentiate between Firewall and IDS.

Ans:

[5M – Dec15 & May18]

Table 7.1: Comparison between Firewall & IDS.

Firewall	IDS
Firewall is device or set of devices located at the network gateway server.	IDS is a software or hardware device installed on the network or host.
Firewall is used to protect private networks from outside networks.	IDS is used to detect and report intrusion attempts to the network.
Firewall can block connection.	IDS cannot block connection.
It does not gives early warning of an intrusion.	It gives early warning of an intrusion.
Firewall is more likely to be attacked then IDS.	IDS is less likely to be attacked then Firewall.
It is not aware of traffic in the internal network.	It is aware of traffic in the internal network.
Types: 1. Packet Filtering Firewall. 2. Stateful-inspection Firewall. 3. Network Address Translation Firewall. 4. Application Based Firewall 5. Hybrid Firewalls.	**Types:** 1. Network IDS. 2. Host IDS. 3. Protocol Based IDS. 4. Anomaly Based IDS. 5. Misuse Based IDS. 6. Hybrid IDs.
Strength: It provides Protection from vulnerable services.	**Strength:** It can detect password cracking & denial of services.
Limitation: Firewall cannot give protection against all attack that does not pass through firewall	**Limitation:** IDS Detect attack only after they have entered the network, and do nothing to stop attacks.
Diagram: Refer Figure 7.1	**Diagram:** Refer Figure 7.5

Q5] Explain the significance of an Instruction Detection System for securing a network. Compare signature based and anomaly based IDS.

Q6] What are the different components of an Intrusion Detection System? Compare the working of signature based IDS with anomaly based IDS

[Q5 | 10M – May16] & [Q6 | 10M – Dec17]

Ans:

IDS:

1. IDS stand for **Intrusion Detection System.**
2. It is the device which gives early warning of an intrusion.
3. So that the defensive action can be taken to prevent or minimize damage.
4. IDS detect unusual pattern of activity, which may be malicious or suspicious.

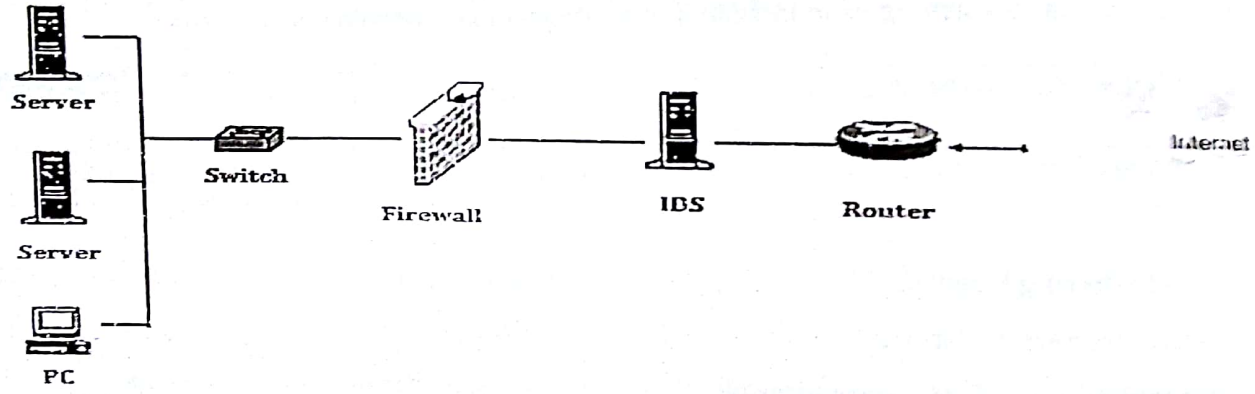


Figure 7.5: IDS.

CHARACTERISTICS:

1. It must run continuously without human supervision.
2. It should not be in a black box.
3. It must resist subversion.
4. It must be fault tolerant.

IDS SIGNIFICANCE:

1. IDS is used for Monitoring and analyzing both user and system activities.
2. It helps in assessing system and file integrity.
3. IDS detect attack which may harm the system by continuously monitoring it.
4. It provides cross platform protection.
5. It is used to track user policy violations.
6. IDS perform Analysis of abnormal activity patterns in order to secure a network.

COMPONENTS OF AN IDS:

Figure 7.6 shows the components of IDS.

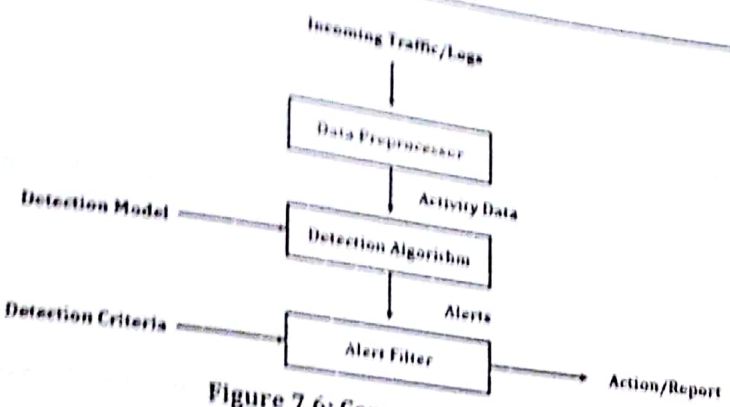


Figure 7.6: Components of IDS.

I) **Incoming traffic/log data:**
   a. **Packets:** Headers contain routing information, content may (and is more and more) also be important for detecting intrusions.
   b. **Logs:** A chronological set of records of system activity.

II) **Data pre-processor:** It collects and formats the data to be analyzed by the detection algorithm.

III) **Detection algorithm:** It is based on the detection model, detects the difference between "normal" and intrusive traffic.

IV) **Alert filter:** It is based on the decision criteria and the detected intrusive activities, estimates their severity and alerts the operator/manages responsive activities (usually blocking).

COMPARISON BETWEEN SIGNATURE BASED AND ANOMALY BASED IDS:

Table 7.2: Comparison between signature based and anomaly based IDS.

Signature Based IDS	Anomaly Based IDS
It is based on **simple pattern matching**.	It is based on **behavior of user**.
It maintain database of signature.	It does not maintain database of signature.
It is less efficient as compared to Anomaly Based IDS.	It is more efficient as compared to Signature Based IDS.
It is able to detect known attacks.	It is able to prevent new unknown attacks.
Signature Based IDS monitors the packets on the network and compare them against a database of signatures.	Anomaly Based IDS monitors the system activity and classifies them as either normal or anomalous based on heuristics rather than signature.
Strength: Precise if Signature are correctly generated.	**Strength:** It has the potential to detect new or unknown attacks.
Weakness: Requires prior knowledge about the signature.	**Weakness:** Often results in false alarms due to the difficulty in modelling the "norm"

Q7] **Viruses and their types.**

Q8] **What are the different types of viruses and worms? How do they propagate?**

Ans: **[Q7 | 5M – Dec15] & [Q8 | 10M – Dec16 & Dec17]**

VIRUS:

1. A computer virus is a type of **malicious software program.**
2. It is a program or piece of code that is loaded onto the computer without user's knowledge and runs against wishes of the user.
3. Viruses can also replicate themselves.
4. All computer viruses are man-made.
5. Viruses can automatically copied and pasted from memory to memory over & over.
6. It can cause program to operate incorrectly or corrupt a computer's memory.
7. Virus can spread itself by infecting files on a network file system that is accessed by other computers.
8. For **Example:** A virus might attach itself to a program such as Excel. Now each time the Excel runs, the virus runs too.

TYPES OF VIRUSES:

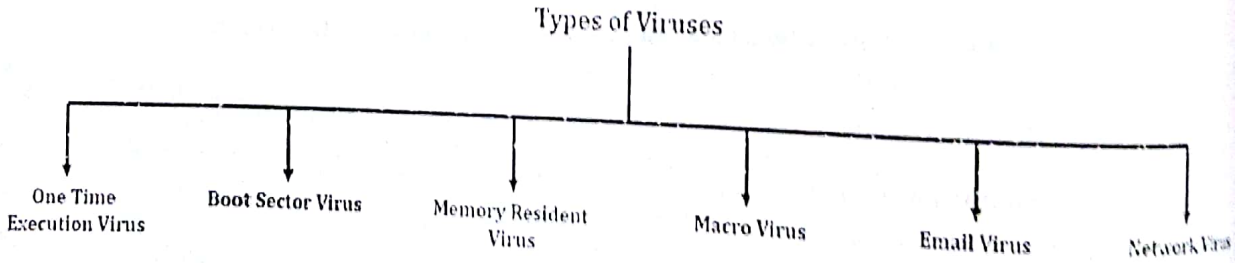


Figure 7.7: Types of Viruses.

I) **One Time Execution Virus:**

- This type of virus executes only once.
- In one execution, Virus spreads its copy in order to cause malicious effect.
- **For Example:** A virus that comes as an e-mail attachment. Once it is opened, it gets executed and spread itself.

II) **Boot Sector Virus:**

- This type of virus infects the boot sector on floppy disks, hard disks and other bootable media like CD or DVD.
- Example of Boot Sector Virus are Form & Stoned.

III) **Memory Resident Virus:**

- This type of virus lodges in main memory as part of a resident system program.
- From that point on, the virus infects every program that executes.

IV) **Macro Virus:**

- Macros are the blocks of the code written to automate frequently performed tasks and embedded in a program file.
- Macro virus is platform independent.
- Virtually all of the macro viruses infect Microsoft Word documents.
- Examples of Macro virus are Relax, Babbles & Melissa.

V) **E-Mail Virus:**

- This type of virus is transferred through Email.
- Generally this is a macro virus which multiplies by sending itself to other contacts, in hopes that they will activate the virus as well.

VI) **Network Virus:**

- This type of virus are uniquely created to quickly spread throughout the local area network and generally across the internet as well.
- It typical moves within shared resources like drivers and folders.

WORMS:

1. A worm is a piece of malicious code that can spread from one computer to another without requiring a host file to infect.
2. Worm is a program that replicates itself and makes use of a PC's network connectivity to transfer a copy of itself to other computers within that network.
3. It is capable of doing this without any input from the user.
4. Worms are distinct from viruses in that they do not require a host program to run, but like viruses, they almost always cause damage to the infected computer.
5. Thus, they are **self-propagating**.

TYPES OF WORMS:

I) **Email Worms:**

- An email worms uses a PC's email client to spread itself.
- It will either send a link within the email that, when clicked, will infect the computer, or it will send an attachment that, when opened, will start the infection.
- A well-known example of this type of worm is the "ILOVEYOU" worm, which infected millions of computers worldwide in 2000.

II) **Internet Worms:**

- Internet worms are **completely autonomous programs.**
- They use an infected machine to scan the internet for other vulnerable machines.
- When a vulnerable machine is located, the worm will infect it and begin the process again.

III) **File-sharing Networks Worms:**

- File-sharing worms take advantage of the fact that file-sharers do not know exactly what they are downloading.
- The worm will copy itself into a shared folder with an unassuming name.
- When another user on the network downloads files from the shared folder, they will unwittingly download the worm, which then copies itself and repeats the process.
- In 2004, a worm called "**Phatbot**" infected millions of computers in this way, and had the ability to steal personal information, including credit card details, and send spam on an unprecedented scale.

IV) **Instant Message and Chat Room Worms:**

- These work in a similar way to email worms.
- The infected worm will use the contact list of the user's chat-room profile or instant-message program to send links to infected websites.
- These are not as effective as email worms as the recipient needs to accept the message and click the link.
- They tend to effect only the users of the particular program

---

Q9] With the help of examples explain non-malicious programming errors.

Ans: **[5M – Dec15]**

NON-MALICIOUS PROGRAMMING ERRORS:

1. Being Human, Programmers & Other Developers make many mistakes.
2. Most of mistakes made are unintentional & non malicious.
3. Many such errors will not lead to more serious vulnerabilities but few will put many security professionals in trouble.
4. There are three broad classes of non-malicious programming errors that have security effects and they are as follows.

I) **Buffer Overflows:**

- A buffer is a space in which data can be held.
- A buffer resides in memory.
- Because memory is finite, a buffer's capacity is finite.

- For this reason, in many programming languages the programmer must declare the buffer's maximum size so that the complier can set aside that amount of space.
- Example of Buffer Overflow in C Language:
  - Char Sample [5]
  - The complier sets aside 5 bytes to store this buffer, one byte for each of the 5 elements of the array, sample [0] through sample [4].
  - Now we execute the statement: Sample [5] = 'A';
  - The subscript is out of bounds and results in buffer overflow because it does not fall between 0 and 4.

II) Incomplete Mediation:

- Incomplete Mediation means **Incomplete Checking**.
- Incomplete Mediation is easy to exploit and attackers use it to cause security problems.
- In above example, buffer overflow will occur if the length of the input is greater than the length of buffer.
- To prevent such a buffer overflow, the program validates the input by checking the length of input before attempting to write it to buffer.
- Failure to do so is an example of Incomplete Mediation.

Example:

Consider the following URL

http://www.ToppersSolutions.com/index.asp?parm1=(555)8184567andparm2=2014Dec20

- Parm1 & Parm2 are the parameters for Telephone number and a Date respectively.
- It is possible for the attacker to change this parameters in the URL as Parm2=1100Feb20.
- The receiving program may give data type error, or it may execute and give wrong result.

III) Time-of-check to Time-of-use Errors:

- The Time-of-check to Time-of-use (TOCTTOU) Errors is performed by "bait & switch" strategy.
- It is also known as Race Condition Errors or serialization or synchronization flaw.
- Time-of-check to Time-of-use errors exploits the time lag between the time we check and the time we use.
- **Non Computing Example:**
  - Shopkeeper shows buyer real Rolex watch (bait)
  - After buyer pays, shopkeeper switches real Rolex watch to a forged one.
- **Computing Example:**
  - Change of a resource (e.g. Data) between time access checked and time access used.

Q10] What are the various ways for memory and address protection.

Q11] What are the various ways for memory and address protection in Operating systems? How is authentication achieved in O.S?

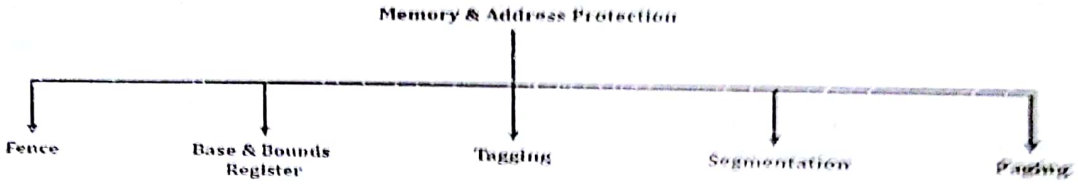
[Q10 | 5M – May16 & 10M – Dec17] & [Q11 | 10M – Dec16]

Ans:

MEMORY & ADDRESS PROTECTION:

1. It is a way to control memory access rights on a computer.
2. Memory protection includes protection for the memory that the OS itself uses as well as the memory of user processes.
3. The main purpose of memory & address protection is to prevent a process from accessing memory that has not been allocated to it.
4. This prevents a bug or malware within a process from affecting other processes, or the operating system itself.

METHODS:



I) **Fence:**

- A fence or fence address is simplest form of memory protection.
- It is designed for single user systems.
- A fence is a particular address that users and their processes cannot cross.
- Only the OS can operate on one side of the fence and users are restricted to the other side.

II) **Base and Bounds Registers:**

- This type of protection can be used in multi- user environment where one users program needs to be protected from the other.
- Each user has a base register which is the lower address and a Bound register which is the upper address limit.
- The base and bounds register approach implicitly assumes that the user or process space is contiguous in memory.
- The OS must determine what protection to apply to a specific memory location.

III) **Tagging:**

- Problem of Base & Bounds Register is that it can allow another module to access all or none of its data.

- This problem is solved using Tagging.
- Tagging specifies the protection for each individual address.
- In this method of protection every word of machine memory has one or more extra bits to identify the access rights to that word.
- Only privileged instructions can set these access bits.

IV) Segmentation:

- This method divides the memory into logical units such as individual procedures or the data in one array.
- Once they are divided, appropriate access control can be enforced on each segment.
- A benefit of segmentation is that any segment can be placed in any memory location provided the location is large enough to hold it.

V) Paging:

- Paging discards the disadvantage of segmentation.
- In paging all segments are of a fixed size called as pages and the memory divided is known as page frames.
- The advantages of paging over segmentation include no fragmentation & improved efficiency.
- The disadvantages are that there is, in general, no logical unity to pages, which makes it more difficult to determine the proper access control to apply to a given page.

HOW AUTHENTICATION ACHIEVED IN O.S:

1. Authentication refers to identifying each user of the system.
2. It is the responsibility of the Operating System to create a protection system which ensures that a user who is running a particular program is authentic.
3. Operating Systems generally authenticates users using following three ways:
   a. **Username / Password:** User need to enter a registered username and password with Operating system to login into the system.
   b. **User card/key:** User need to punch card in card slot, or enter key generated by key generator in option provided by operating system to login into the system.
   c. **User attribute - fingerprint/ eye retina pattern/ signature:** User need to pass his/her attribute via designated input device used by operating system to login into the system.

Q12] Define authentication and non-repudiation and show with examples how each one can be achieved. [10M – Dec16]

Ans:

AUTHENTICATION:

1. Authentication refers to **identifying each user of the system.**
2. Authentication is process of identifying an individual, usually based on a username and password.
3. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.
4. **For Example:** If the sender claims herself as Snehal, the authentication would be to determine whether the sender is really Snehal or not.
5. Operating Systems generally authenticates users using following three ways:
   a. **Username / Password:** User need to enter a registered username and password with Operating system to login into the system.
   b. **User card/key:** User need to punch card in card slot, or enter key generated by key generator in option provided by operating system to login into the system.
   c. **User attribute - fingerprint/ eye retina pattern/ signature:** User need to pass his/her attribute via designated input device used by operating system to login into the system.
6. Figure 7.8 shows basic authentication process.

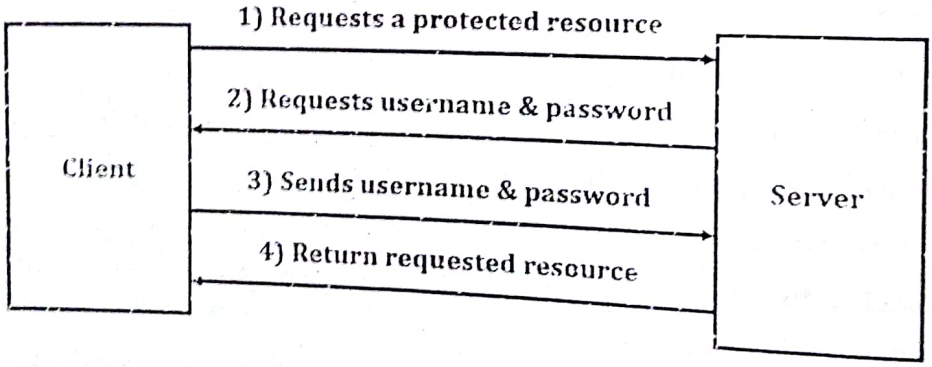


Figure 7.8: Authentication Process.

NON-REPUDIATION:

1. Non-repudiation is the assurance that **someone cannot deny something.**
2. Non-repudiation does not allow the sender or receiver of a message to refuse the claim of not sending or receiving that message.
3. In reference to security, non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message.
4. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

5. Non-repudiation can be obtained through the use of:
   a. **Digital signatures:** Function as a unique identifier for an individual, much like a written signature.
   b. **Confirmation services:** The message transfer agent can create digital receipts to indicate that messages were sent and/or received.
   c. **Timestamps:** Timestamps contain the date and time a document was composed and proves that a document existed at a certain time.
6. Figure 7.9 shows non-repudiation process.

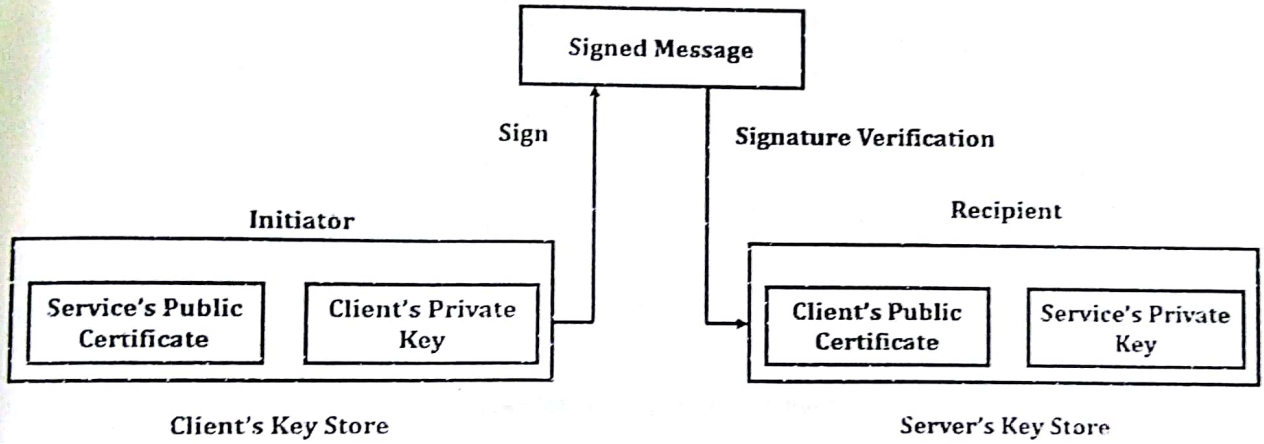


Figure 7.9: Non-repudiation Scenario.

--- EXTRA QUESTION ---

Q1] Malware

Ans:

1. Malware stands for malicious software.
2. It consists of programming with malicious intent to harm the system.
3. Malware is nothing but a software that do malicious things without the victim's knowledge.
4. Malware can be subdivided into many categories as shown in figure 7.10

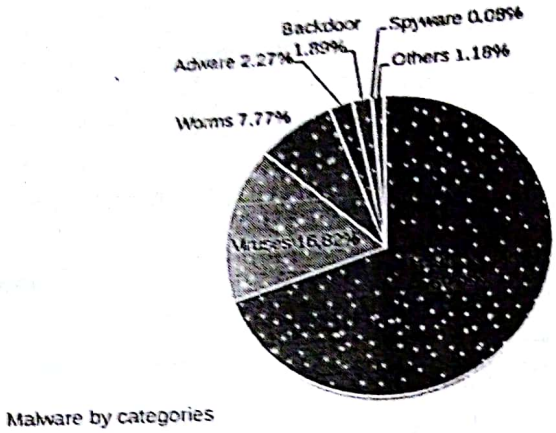


Figure 7.10: Types of Malware.

I) **Logic Bomb:**

- It is a piece of code that detonates or sets off when specific condition is triggered.
- The condition may be a day, date, time, a particular 'if loop', time interval, or count.

II) **Virus:**

- It is a computer program which replicates itself and spreads from one computer to another.
- A virus can spread itself by infecting files on a network file system that is accessed by other computer.
- **Example:** An email virus attaches itself to an email that is send from one user to another.

III) **Worm:**

- It spreads itself through network to infect other computers.
- It does not need outside assistance as required by virus.
- **Example:** Code red worm may be crash the operating system and other devices connected under the same network.

IV) **Trojan horse:**

- It is the malware that invites the user to run it, which may contain harmful or malicious payload
- The payload may lead to many undesirable effects.
- **Example:** An innocent looking game could do something malicious while the victim is playing.

V) **Trapdoor:** It is method of bypassing normal authentication procedure i.e. it allows unauthorized access to a system.

VI) **Rabbit:**

- It is a malware which creates many instances of them in order to exhaust the system resources. Unlike worms, it does not spread over network.
- It can exhaust system resources.

VII) **Spyware:**

- It is the type of malware that can be installed on computer and which collects information about users without their knowledge.
- It monitors user's computing.

CHAPTER - 8: IP SECURITY

Q1] What is a Denial of service attack? What are the different ways in which an attacker can mount a DOS attack on a system?

Q2] Denial of service attacks.

Q3] What are Denial of Service attacks? Explain any three types of DOS attacks in detail.

Ans: **[Q1 | 10M – Dec15], [Q2 | 5M – May16] & [Q3 | 10M – May17]**

DENIAL OF SERVICE:

1. Denial of Service (DoS) is also called as **availability attack.**
2. DoS makes a computer or its resources unavailable to its intended user.
3. In DoS, an attacker may prevent you from accessing email, website, online accounts or other services that rely on affected computer.
4. The basic purpose of a DoS attack is simply to flood a network or change in the configurations of routers on the network.
5. These attacks sometimes have a specific target.
6. For **Example:**
   a. All message sent to specific recipient may be suppressed.
   b. An entire network may be disrupted either by disabling the network or by flooding it with messages.

METHODS:

The different ways in which attackers can mount DoS attacks are:

1) **SYN Flood Attack:**

➢ SYN Flood Attack uses TCP protocol suite, where a 3-way handshaking of network connection is done with SYN and ACK message as shown in figure 8.1.

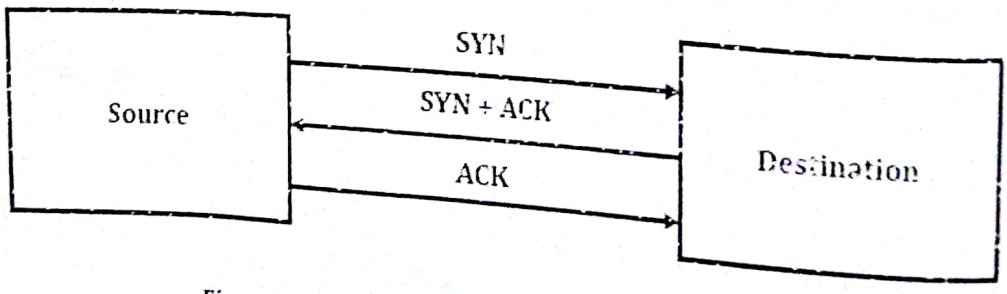


Figure 8.1: SYN Flood Attack 3 Way Handshaking.

- To initiate TCP connection, the system that wishes to communicate, sends a SYN message to the target system.
- If the target system is ready to communicate, it sends SYN + ACK message to source machine.
- The source system then responds with an ACK message to complete the communication.
- In SYN flood attack, attacker denies service to the target by sending many SYN message and not replying with ACK.
- This fills up the buffer space for SYN message on the target machine, which prevents other systems on the network from communicating with target system.

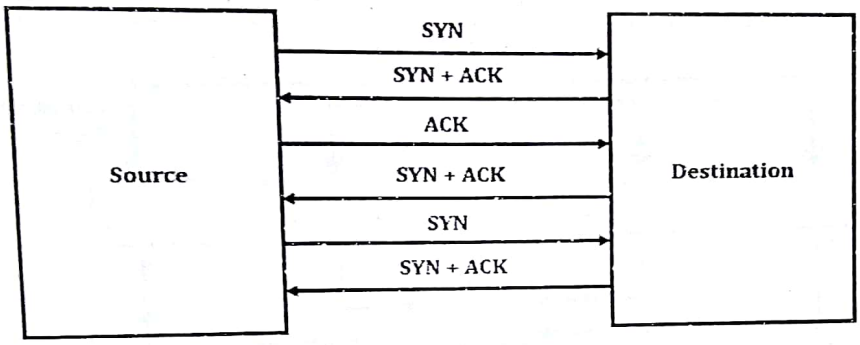


Figure 8.2: SYN Flood Attack.

II) **Ping of death:**

- The ping of death simply sends ping packets that are larger than 65.535 bytes to the victim.
- This DoS attack is as follows: **ping –l 86600 victim.org**
- This attack saturates the victim's bandwidth, if attacker is on let's saying 100 MB connection and victim is on 10 MB connection.
- But the attack would not succeed if attacker is on 10 MB connection and victim is on 100 MB connection.

III) **Teardrop Attack:**

- Teardrop Attack is conducted by targeting TCP/IP fragmentation reassembly code.
- This attack causes fragmentation packets to overlap one another on the host receipt.
- The host attempt to reconstruct them during the process but fails.
- For **Example:** you need to send 3000 bytes of data from one system to another. The data is divided and sent into smaller packets as given below:
  - Packet 1 carries bytes 1 – 1000
  - Packet 2 carries bytes 1001 – 2000
  - Packet 3 carries bytes 2001 – 3000
- Teardrop attack overlaps the bytes with each other.
- Bytes 1 – 1500, bytes 1000 – 2000 and bytes 1500 – 2500

IV) **Smurf Attack:**

- It is a variation of a ping attack.
- This attacker floods a target system via spoofed broadcast ping message.
- The attacker sends a ping request to a third party's broadcast address on the network address.
- Every system within third party's broadcast domain then sends ping response to the victim.

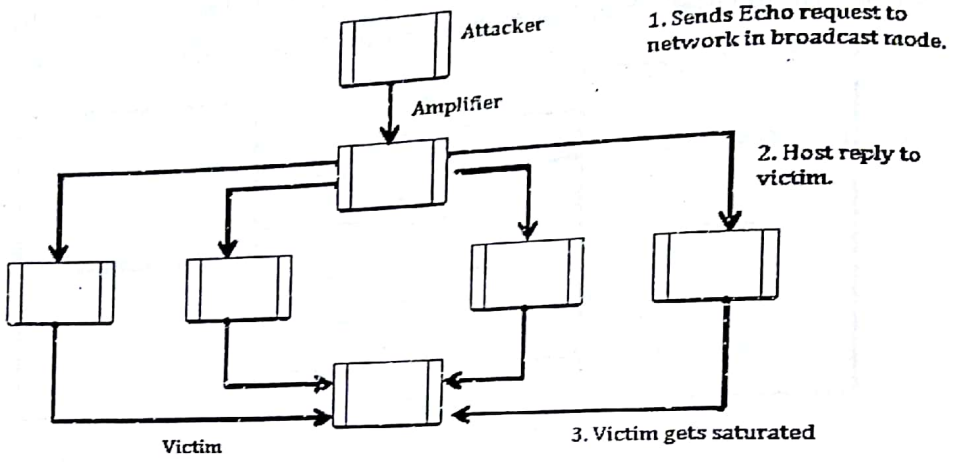


Figure 8.3: Smurf Attack.

V) **Echo Chargen:**

- Echo chargen takes place between two hosts.
- Echo services repeat anything sent to it.
- Chargen service generates a continuous stream of data.
- If they are used together, they create an infinite loop and results in denial of service.
- For example an attacker starts this chargen process on host A which sends echo packets to host B.
- Host B replies to stream of packets generated by host A, by echoing them back to host A.
- This creates an endless loop between A and B.

Q4] What is access control? How does the Bell La Padula model achieve access control?

Ans:

ACCESS CONTROL:

[10M – May16]

1. Access control is a security technique.
2. It can be used to regulate who or what can view or use resources in a computing environment.
3. The act of accessing may mean consuming, entering, or using.
4. Permission to access a resource is called authorization.
5. Access Control includes Access Control Matrix & Access Control List.

I) Access Control Matrix:

- Access Control Matrix gives a classic view of authorization.
- Authorization is used to restrict the actions of authenticated users.
- Access control matrix has all relevant information needed by the operating system to made a decision about which users are allowed to do what with the various system resources.
- Access Control Matrix consists of subjects and objects.
- Subjects (users) are the index of rows.
- Objects (resources) are the index of columns.
- Figure 8.4 shows the example of Access Control Matrix, where UNIX-style notation such as execute (x), read (r), and write (w) privileges are used.

	OS	Accounting Program	Accounting Data	Insurance Data	Payroll Data
Bob	rx	rx	r	---	---
Alice	rx	rx	r	rw	rw
Sam	rwx	rwx	r	rw	rw
Accounting Program	rx	rx	rw	rw	rw

Figure 8.4: Example of Access Control Matrix.

II) Access Control List:

- Access control matrix has all relevant information.
- This could be 1000's of users and 1000's of resources.
- Then matrix with 1,000,000's of entries.
- The problem is how to manage such a large matrix.
- This can be done by portioning the Access Control Matrix into more manageable pieces.
- There are two ways to split the Access Control Matrix:
  - **Using Access Control List:** Access Control List stores access control matrix by column.

	OS	Accounting Program	Accounting Data	Insurance Data	Payroll Data
Bob	rx	rx	r	---	---
Alice	rx	rx	r	rw	rw
Sam	rwx	rwx	r	rw	rw
Accounting Program	rx	rx	rw	rw	rw

- **Using Capabilities:** Capabilities stores access control matrix by row.

	OS	Accounting Program	Accounting Data	Insurance Data	Payroll Data
Bob	rx	rx	r	...	...
Alice	rx	rx	r	rw	rw
Sam	rwx	rwx	r	rw	rw
Accounting Program	rx	rx	rw	rw	rw

BELL-LA PADULA MODEL:

1. Bell La Padula model is known as BLP Security Model.
2. BLP security model was designed to express essential requirements for Multi-Level Security.
3. BLP deals with **confidentiality.**
4. It is used to prevent unauthorized reading.
5. Bell La Padula Model Supplements the Access Matrix to provide Access Control & Information Flow.
6. Assume that O is an object, S is a subject.
7. Object O has a classification.
8. Subject S has a clearance.
9. Security level denoted L(O) and L(S)
10. BLP consists of:
    a. **Simple Security Condition:** S can read O if and only if $L(O) \leq L(S)$
    b. **Property (Star Property):** S can write O if and only if $L(S) \leq L(O)$
11. No read up & no write down as shown in figure 8.5

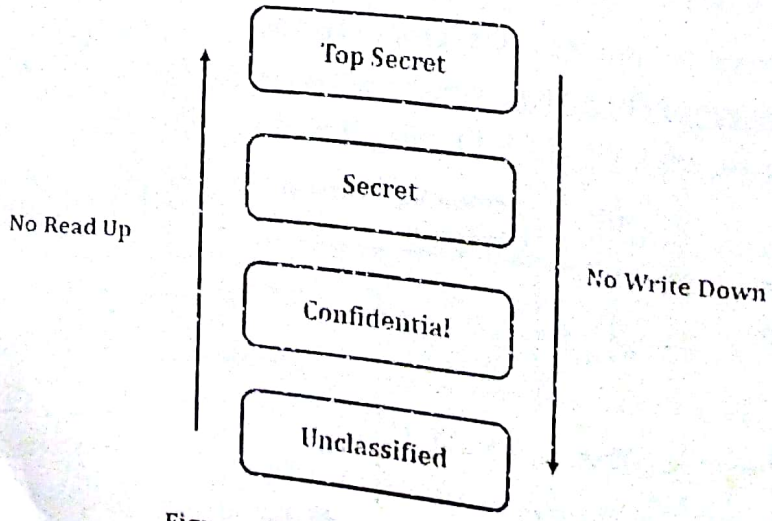


Figure 8.5: Bell-La Padula Model.

Q5] SSL Handshake Protocol.

Q6] List the functions of the different protocols of SSL. Explain the handshake protocol

[Q5 | 5M – May16] & [Q6 | 5M – Dec15]

Ans:

SSL:

1. SSL stands for **Secure Socket Layer (SSL).**
2. It is also known as Transport Layer Security (TLS).
3. SSL is layered on top of TCP.
4. It is a protocol developed by Netscape to protect communication between web browser and server.
5. URLs that require SSL connection start with https.
6. SSL ensures that all data passed between web server and browser remains private and secure.

FUNCTIONS OF THE DIFFERENT PROTOCOLS OF SSL:

1. SSL Protocols Authenticates the End Points usually the servers.
2. It hides the data during transmission.
3. It provides a way to validate or identify the website by creating the information file and making the accessing possible.
4. It creates an encrypted connection that provides the sending of the data from one source to another using the SSL.
5. SSL provides a way to ensure that the security is being provided to the transaction and the data in use.
6. The lock is used to display the browsers connection is closed or opened on the secure channel of SSL or TLS.

HANDSHAKE PROTOCOL:

1. Handshake Protocol is the first sub layer protocol used in client and server to communicate using an SSL-Enabled Connection.
2. This is similar to how Alice & Bob would shake hands with each other with a hello before they start conversing.
3. The Handshake Protocol is made up of four phases which pass message between the client and server.
4. Figure 8.6 shows the handshake protocol operation.

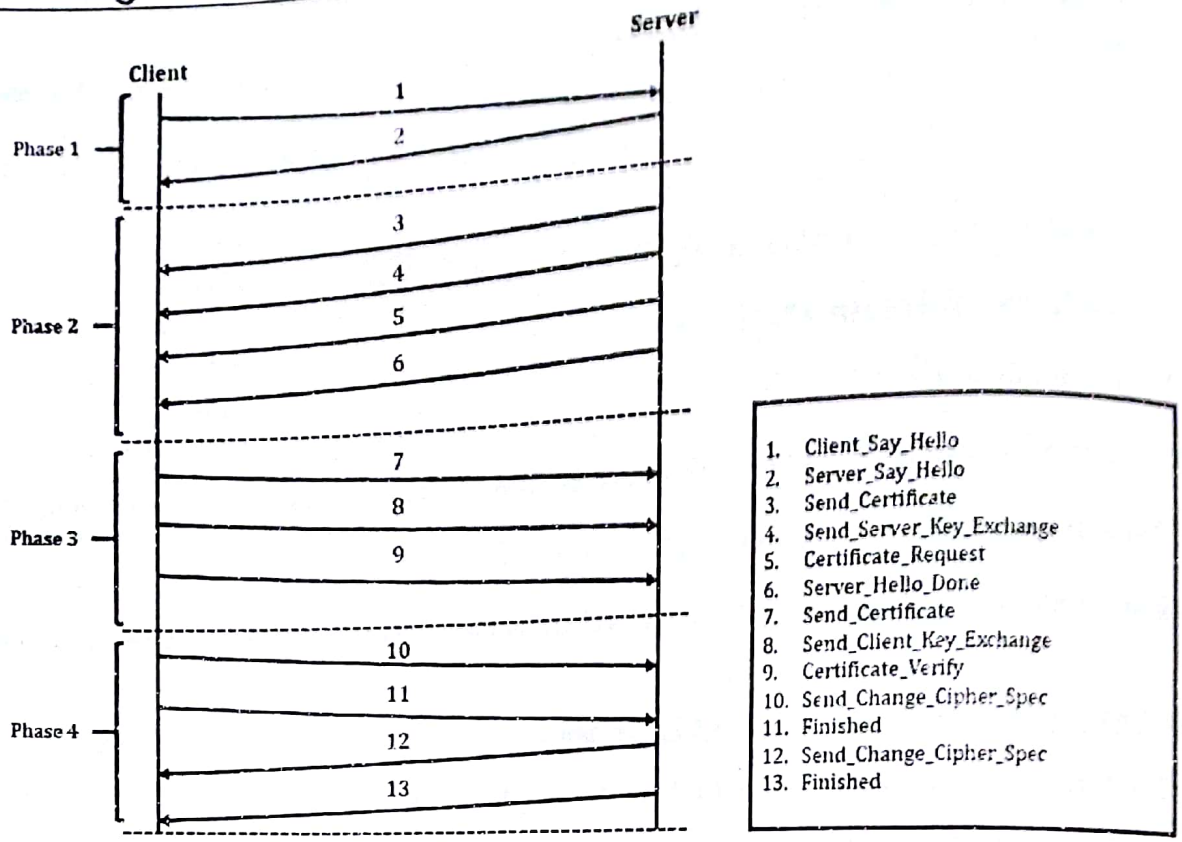


Figure 8.6: Handshake Protocol Operation.

I) **Establish Security Capabilities:**

- This initiates logical connections and establishes capabilities associated with that connection.
- This consists of two messages that are the client hello and server hello.
- The client sends the client hello message to server and receives a server hello message from the server as a reply.

II) **Server Authentication and Key Exchange:**

- The server initiates this phase and is the sole sender of all messages.
- While client is the sole recipient of all messages.
- This phase contains the following four steps:
  - **Certificate:** Server sends its digital certificate to the client for authentication.
  - **Server Exchange Key:** If server does not send a certificate then it sends its public key.
  - **Certificate Request:** The server request for the client's digital certificate.
  - **Server Hello Done:** This message indicates to the client that its portion of hello message is complete.

III) **Client Authentication and Key Exchange:**

- The client initiates this phase and is the sole sender of all messages.
- While server is the sole recipient of all messages.
- This phase contains the following three steps:

- **Certificate:** This is an optional and used only if the server requested for client's digital certificate.
- **Client Exchange Key:** the client sends a symmetric key to the server.
- **Certificate Verify:** This is needed only if the server demands client authentication.

iv) **Finish:**

- The client initiates this phase of the Handshake which the server ends.
- The client sends change cipher specs and finished message to the server.
- On receiving them the server sends change cipher specs and finishes messages.

Q7] What are the different protocols in SSL? How do the client and server establish an SSL connection

Ans: **[5M – Dec17]**

SSL:

1. SSL stands for **Secure Socket Layer (SSL).**
2. SSL ensures that all data passed between web server and browser remains private and secure.

SSL PROTOCOLS:

I) **SSL Handshake Protocol:**

- SSL Handshake Protocol is the most complex part of SSL.
- It is invoked before any application data is transmitted.
- It creates SSL sessions between the client and the server.

II) **ChangeCipherSpec Protocol:**

- It is simplest part of SSL protocol
- It comprises of a single message exchanged between two communicating entities, the client and the server.
- As each entity sends the ChangeCipherSpec message, it changes its side of the connection into the secure state as agreed upon.
- The cipher parameters pending state is copied into the current state.
- Exchange of this Message indicates all future data exchanges are encrypted and integrity is protected.

III) **SSL Alert Protocol:**

- This protocol is used to report errors – such as unexpected message, bad record MAC, security parameters negotiation failed, etc.

- It is also used for other purposes – such as notify closure of the TCP connection, notify receipt of bad or unknown certificate, etc.

HOW CLIENT AND SERVER ESTABLISH AN SSL CONNECTION PROTOCOL?

Refer Q5 (SSL Handshake Protocol Section).

Q8] IPSec Protocols for security

Q9] Explain IPSec protocol in detail. Also write applications and advantages of IPSec

Ans: **[Q8 | 5M – May16] & [Q9 | 10M – May18]**

IPSEC PROTOCOL:

1. IPSec Stands for **Internet Protocol Security.**
2. It is a protocol suite for **securing Internet Protocol Communication.**
3. It uses cryptographic security services to protect communications over Internet Protocol (IP) networks.
4. IPSec is implemented at the IP Layer, so it affects all upper layers (i.e. TCP & UDP)
5. It provides Authentication, Confidentiality & Key Management.
6. Using IPSec, it is possible to communicate securely across a LAN, across public/private WAN and across the internet.
7. IPSec is used to provide an en-to-end security services.
8. IPSec is usually installed in networking device such as router or firewall.
9. Figure 8.7 shows IPSec Scenario.

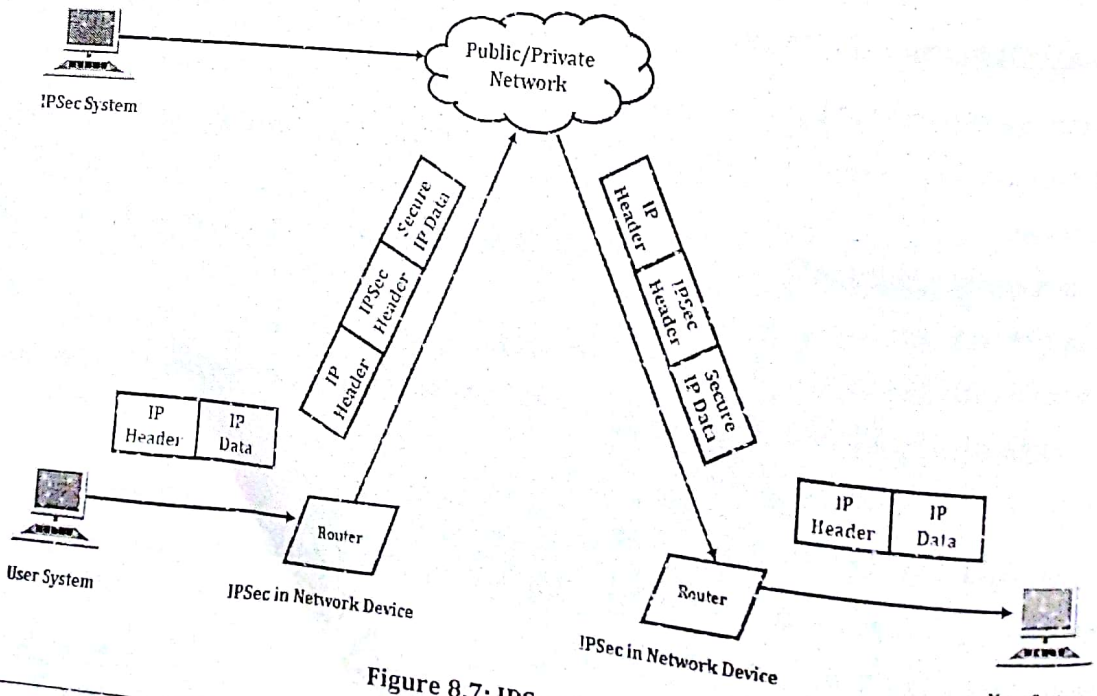


Figure 8.7: IPSec Scenario.

SERVICES PROVIDED BY IPSEC:

- Access Control.
- Connectionless Integrity.
- Confidentiality.
- Data Origin Authentication.
- Rejection of Replayed Packets.

GOALS OF IPSEC:

- To provide system security solutions.
- To have single security policy.
- Both endpoints must agree to bypass or protect traffic.

ADVANTAGES:

- IPSec provides security without any modifications to user computers.
- It can work independent of applications.
- In a firewall/router, it provides strong security to all traffic crossing the perimeter.
- It is below transport layer, hence transparent to applications.
- It can be transparent to end users.
- IPsec allows per flow or per connection based security.
- It provides seamless security to application and transport layers (ULPs).

APPLICATIONS:

- IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.
- Examples of its use include:
  - Secure branch office connectivity over the Internet.
  - Secure remote access over the Internet.
- Using IPSec all distributed applications can be secured. **Example:**
  - Remote logon.
  - Client/server.
  - E-mail.
  - File transfer.
  - Web access
- It is used for establishing extranet & intranet connectivity with partners.
- Enhancing electronic commerce security.

Q10] **IPSec offers security at n/w layer. What is the need of SSL? Explain the services of SSL protocol?** [10M – May17]

Ans:

IPSEC PROTOCOL:

Refer Q8.

NEED OF SSL:

I) **To Encrypt Information:**

- The major purpose of an SSL certificate is to **encrypt information** so that it can only be read and understood by the intended parties.
- Information submitted on Internet forms often passes through more than one computer before reaching its final destination, and the more "stops" it has to make, the higher the chance that a third party could obtain access.
- An SSL certificate inserts random characters into the original information, rendering it incomprehensible to anyone without the proper encryption key.

II) **To Provide Authentication:**

- To make sure that the Information on website, including customer information, goes to the correct server without being intercepted
- This requires authentication.
- When obtaining an SSL certificate, another type of protection called a **server certificate** is also issued.
- This certificate acts as a mediator between browsers and SSL servers to show that the SSL certificate provider can be trusted.

III) **Guards Against Phishing:**

- SSL also acts as a guard against **phishing**
- When users don't see the signs of security on a site, they're more likely to navigate away without entering any information.

IV) **To Accept Payments:**

- An SSL certificate with the proper encryption of at least 128-bit is needed.
- PCI standards verify that the SSL certificate is from a trusted source, uses the right strength of encryption and provides a private connection on any page that requires customers to enter personal information.
- Without a certificate that meets these standards, a site won't be able to take credit card payments

SERVICES OF SSL PROTOCOL:

1. **Fragmentation:** Divides the data into blocks of 214 bytes or less.
2. **Compression:** Lossless compression methods are used for compressing fragmented data.
3. **Message Integrity:** To preserve the integrity of data SSL uses a keyed-hash function to create a MAC.
4. **Confidentiality:** Original data and the MAC are encrypted using symmetric key cryptography.
5. Protects against Man-in-the-middle attack.
6. Simple and well designed.

Q11] How is security achieved in the transport and tunnel modes of IPSec? Describe the role of AH and ESP.

Ans: **[10M – Dec16]**

1. IPsec Communication has two modes of functioning: transport and tunnel modes.
2. These modes can be used in combination or used individually depending upon the type of communication desired.

TRANSPORT MODE

- Transport mode is used for **host-to-host communication.**
- It only encrypts and optically authenticates IP Payload and not the IP header as shown in figure 8.8.

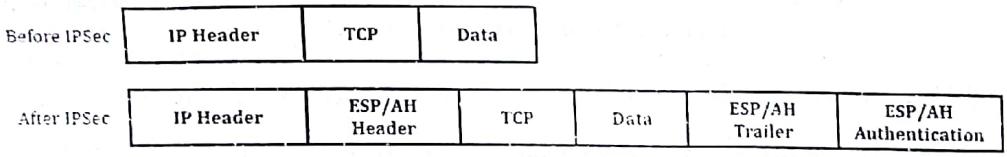


Figure 8.8: Transport Mode.

- That means, transport mode does not protect entire IP packet.
- Transport mode is efficient, but since it does not encrypts IP header, IP header is visible to attacker.

TUNNEL MODE.

1. Tunnel mode is used for **network to network communication, host to network communication and host to host communication.**
2. In this mode, entire IP packet is encrypted and optionally authenticated.

3. It takes the original IP packet with its IP header, uses IPSec to encrypt it and then adds new IP header to encrypted payload.
4. Refer 8.9 figure for tunnel mode.

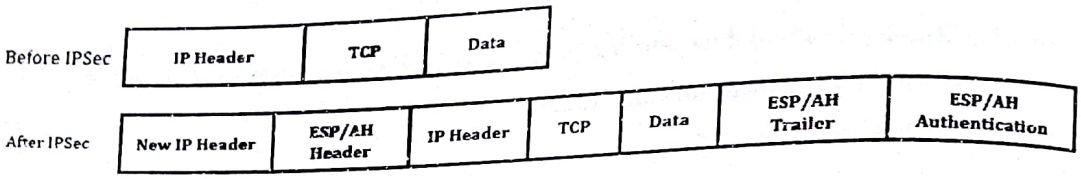


Figure 8.9: Tunnel Mode.

AH:

1. AH stands for **Authentication Header**.
2. The AH protocol provides service of data integrity and authentication of IP packets.
3. It also protects against replay attacks by using sliding window and discarding old packets.
4. It is based on use of MAC.
5. The packet format of AH is shown in figure 8.10.

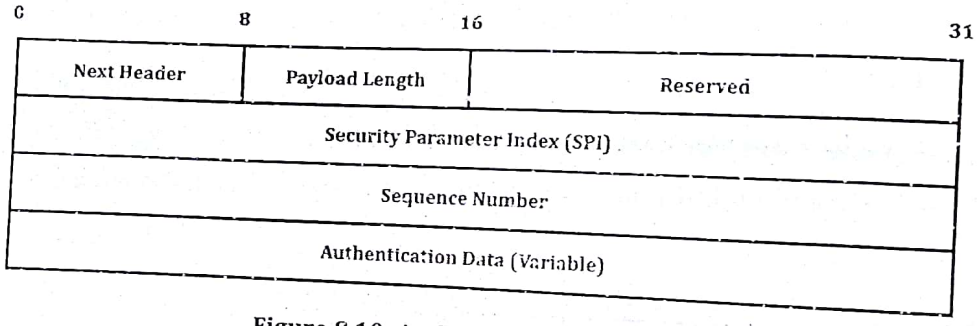


Figure 8.10: Authentication Header.

Next Header (8 bit): It identifies the type of header immediately following AH header.

Payload Length (8 bit): It is length of authentication header.

Reserved (16 bit): It is reserved for future use.

Security Parameter Index (SPI) (32 bit): It identifies a security association.

Sequence Number (8 bit): It is used as counter.

Authentication Data (Variable): A variable length field that contains the integrity check value.

ESP:

1. ESP stands for **Encapsulating Security Payload**.
2. It is the key protocol use in IPSec.
3. It is used to provide confidentiality, data origin authentication, connection less integrity, an anti-replay service and limited flow confidentiality.

The packet format for ESP is shown in figure 8.11.

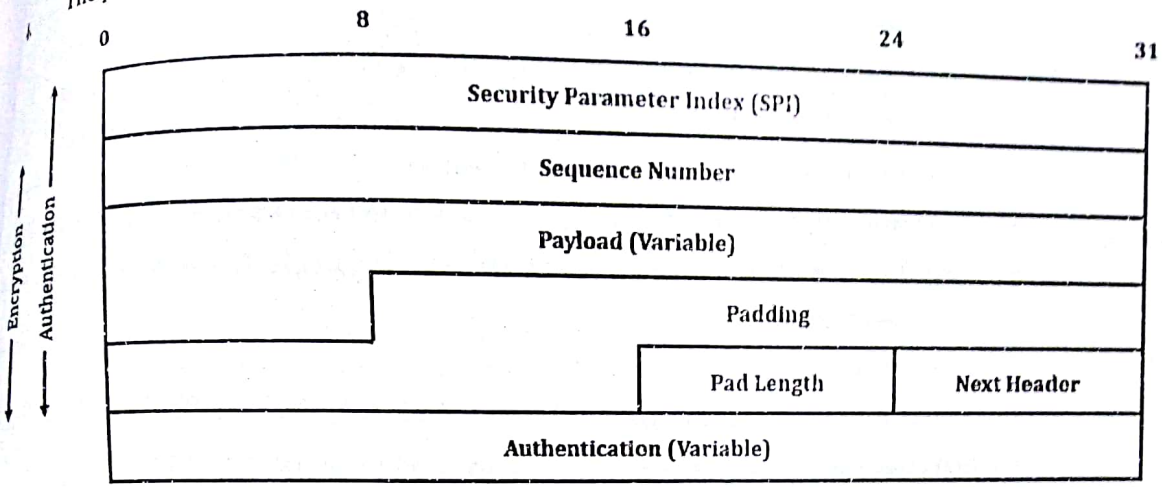


Figure 8.11: ESP Packet Header.

Security Parameter Index (SPI) (32 bit): It identifies a security association.

Sequence Number (32 bit): It is used as counter to provide anti-replay function.

Payload (Variable): IP Packet protected by encryption.

Padding (0 – 255 bytes): It is used for various reasons.

Pad length (8 bit): It indicates number of pad bytes.

Next Header: It identifies type of data contained in payload data field by identifying the first header in that payload.

Authentication Data (Variable): A variable length value which contains the integrity check value.

Padding: It is used as padding bit.

Q12] How is security achieved in the transport and tunnel modes of IPSec? What are security associations?

[10M – Dec17]

Ans:

SECURITY IN TRANSPORT & TUNNEL MODE OF IPSEC:

Refer Q11.

SECURITY ASSOCIATIONS:

1. One of the most important concepts in IPSec is called a Security Association (SA).
2. Security Association are defined in RFC 1825.
3. SAs are the combination of a given Security Parameter Index (SPI) and Destination Address.

4. SAs are one way.
5. A minimum of **two SAs** are required for a single IPSec connection.
6. SAs contain parameters including:
   - Authentication algorithm and algorithm mode.
   - Encryption algorithm and algorithm mode.
   - Key(s) used with the authentication/encryption algorithm(s)
   - Lifetime of the key.
   - Lifetime of the SA
   - Source Address(es) of the SA.
   - Sensitivity level (i.e. Secret or Unclassified)

Example:

1. A security is a very complex set of pieces of information.
2. However, we can show the simplest case in which Alice wants to have an association with Bob for use in a two-way communication.
3. Alice can have an outbound association (for datagrams to Bob) and an inbound association (for datagrams from Bob).
4. Bob can have the same.
5. In this case, the security associations are reduced to two small tables for both Alice and Bob as shown in figure 8.12.

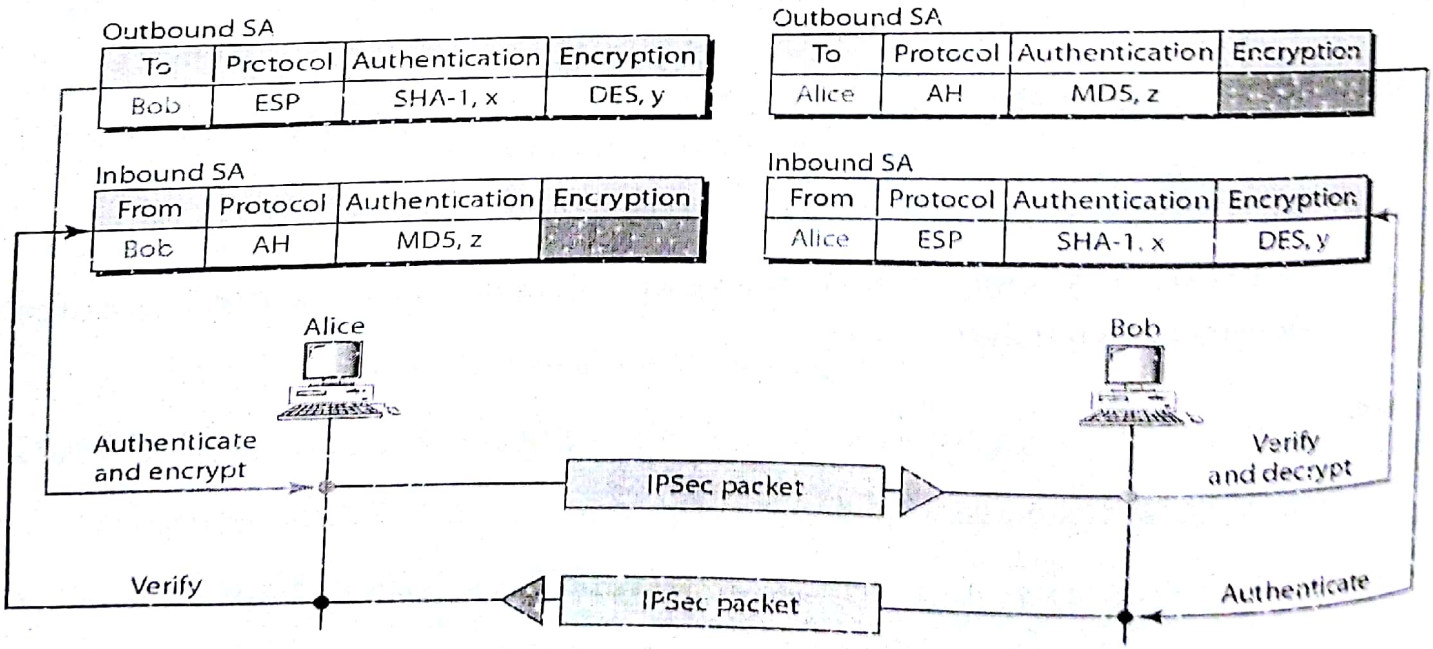


Figure 8.12: Example of Security Associations.

6. The figure 8.12 shows that when Alice needs to send a datagram to Bob, she uses the ESP Protocol of IPSec.
7. Authentication is done by using SHA-1 with key X.
8. The encryption is done by using DES with key Y.

When Bob needs to send a datagram to Alice, he uses the AH Protocol of IPSec.

Authentication is done by using MD5 with key z.

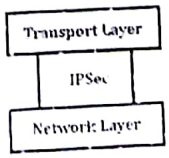
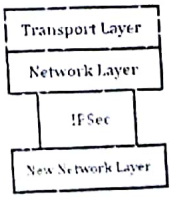
Note that the inbound association for Bob is the same as the outbound association for Alice, and vice versa.

Q3] Differentiate between the transport mode and tunnel mode of IP Sec and explain how authentication and confidentiality are achieved using IP Sec.

Ans: **[10M – Dec15]**

COMPARISON OF TRANSPORT & TUNNEL MODE OF IPSEC:

Table 8.1: Differentiate between the transport mode and tunnel mode of IP Sec.

Points	Transport Mode	Tunnel Mode
Protection Provided	It protects IP Payload only.	It protects entire IP Packet.
Authentication Header (AH)	Authenticates only IP payload and selected portions of the IP header.	Authenticates entire inner IP packet and selected portions of the outer IP header.
Encapsulation Security Payload (ESP)	It encrypts IP Payload and optionally authenticates it.	It encrypts and optionally authenticates the entire inner IP packet.
Purpose	It is used when we need host-to-host protection of data.	It is used when one or both ends of a security association are a security gateway.
Protection Mode	It provides protection primarily for upper layer protocols.	It provides protection to the entire IP Packets.
Payload Message Service Specification (MSS)	Less.	Comparatively higher.
Place in TCP/IP Model	In this mode, IPSec is placed between transport and network layer. 	In this mode, IPSec is placed between network layer and new network layer. 
NAT Traversal	Not supported.	Supported.
VPN Scenarios	Site-to-site VPN Scenarios.	Client-to-site VPN Scenarios.

Use	It is used for end-to-end communication between two hosts.	It is used between two routers, between a host and a router or between a router and a host.

AUTHENTICATION IN IPSEC:

- IPsec authentication algorithms use a shared key to verify the identity of the sending IPsec device.
- The IPsec protocol suite defines two authentication algorithms: MD5 and SHA-1.
- The Services Router uses an HMAC variant of MD5 and SHA-1 algorithms that provide an additional level of hashing.
- In an IPsec-enabled network, the Services Router that sends an IP packet computes a MD5 or SHA-1 digital signature, and adds this digital signature to the packet.
- The Services Router that receives the packet computes the digital signature and compares it with the signature stored in the packet's header.
- If the digital signatures match, the packet is authenticated.

CONFIDENTIALITY IN IPSEC:

- Confidentiality means encryption of data.
- Encryption encodes data into a secure format so that it cannot be deciphered by unauthorized users.
- Like authentication algorithms, encryption algorithms use a shared key to verify the authenticity of the IPSec devices.
- The Services Router uses the following encryption algorithms:
  - Data Encryption Standard-cipher block chaining (DES-CBC)
  - Triple Data Encryption Standard-cipher block chaining (3DES-CBC)
  - Advanced Encryption Standard (AES)

Q.4] Explain software flaws with example. [5M – May16]

Ans:

SOFTWARE FLAWS:

1. A software flaws is an error, bug, failure or fault in a computer program or system.
2. Most software flaws arise from mistakes and errors made in either a program's source code or its design, or in components and operating systems used by such programs.
3. According to National Institute of Standards and Technology (NIST), there are as many as twenty flaws per thousand lines of software code.
4. Software Flaws can result in Denial of Service, Unauthorized Disclosure and Unauthorized Modification of Data.
5. Following are some standard terminologies suggested by IEEE:
   i. **Error:** Human Action that produces an incorrect Result.
   ii. **Fault:** It is an incorrect step, process, command or data definition in a computer program.
   iii. **Failure:** A failure is the inability of the system to perform its required behavior.

Classification of Software Flaws:

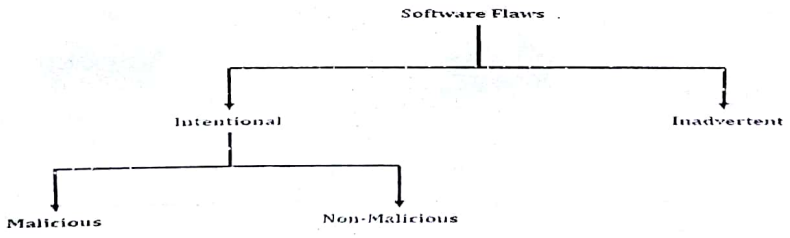


Figure 8.13: Classification of Software Flaws.

Example:

Consider the below programming code.

```
Char Array [10];
For (i = 0; i < 10; ++i)
{
        Array [i] = 'A';
        Array [10] = 'B';
}
```

- This Program has an Error.
- This Error might cause a Fault.
- If a Fault occurs, it might lead to Failure.
- We use the term Flaw for all the above case.

Q15] Buffer overflow attack. [5M - Dec15]

Ans:

BUFFER OVERFLOW ATTACK:

1. A buffer is a space in which data can be held.
2. A buffer resides in memory.
3. Because memory is finite, a buffer's capacity is finite.
4. Buffer overflow is the result of stuffing more data into a buffer than it can handle.
5. **For Example:** If you try to pour four gallons of water into three gallons capacity jug, some water is going to spill out.
6. It is also called as buffer overrun or smashing the stack.
7. It is the basis of many software vulnerabilities.
8. Assume a Web form that asks the user to enter data, such as name, age and date of birth.
9. The entered information is then sent to a server and the server writes the data entered to a buffer that can hold N characters.
10. If the server software does not verify that the length of the data is at most N characters, then a buffer overflow might occur.

EXAMPLE OF BUFFER OVERFLOW IN C LANGUAGE:

```
Int main ()
{
Char Sample [5]
Sample [5] = 'A';
}
```

- Char Sample [5]: The complier sets aside 5 bytes to store this buffer, one byte for each of the 5 elements of the array, sample [0] through sample [4].
- Now we execute the statement: Sample [5] = 'A';
- The subscript is out of bounds and results in buffer overflow because it does not fall between 0 and 4.
- The buffer overflow might overwrite the user data or code, or it could overwrite system data or code, or it might overwrite unused space.

[06] Compare packet sniffing and packet spoofing. Explain session hijacking attack.

[10M – May16]

ans:

PACKET SNIFFING:

1. Packet Sniffing is a technique of monitoring every packet that crosses the network.
2. It is a form of wiretap applied to computer.
3. Packet Sniffing is widely used by hackers and crackers to gather information illegally about networks they intend to break into.
4. The software or device used to do this is called a **Packet Sniffer.**
5. A Packet Sniffer is a utility that sniffs without modifying the network's packets in any ways.
6. There are two ways in which a Packet Sniffer can be set:
   a. **Unfiltered:** It captures all packets.
   b. **Filtered:** It captures only the packets with specific data items.
7. Packet Sniffing is difficult to detect, but it can be done. But the difficulty of the solution means that in practice, it is rarely done.
8. Figure 8.14 shows example of Packet Sniffing.

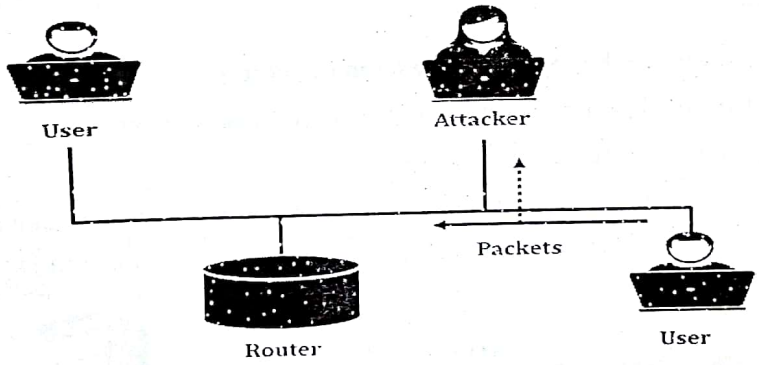


Figure 8.14: Packet Sniffing Example.

PACKET SPOOFING:

1. Packet Spoofing is also known as **IP Spoofing.**
2. It is the creation of Internet Protocol (IP) packets with a false source IP address, for the purpose of hiding the identity of the sender or impersonating another computing system.
3. One technique which a sender may use to maintain anonymity is to use a proxy server
4. As shown below in figure 8.15, attacker creates an IP packet and sends to the server which is known as SYN request.
5. The difference in the IP packet and normal packet is that the attacker puts the own source address as another computers IP address in the newly created IP packet.
6. The server responds back with a SYN-ACK response which travels to the forged IP address.

7. The attacker somehow gets this SYN-ACK response send by the server and acknowledges it so as to complete a connection with server.
8. Once this is done the attacker can try various commands on the server computer.
9. The most common methods include IP address spoofing attacks, ARP spoofing attacks, and DNS server spoofing attacks.

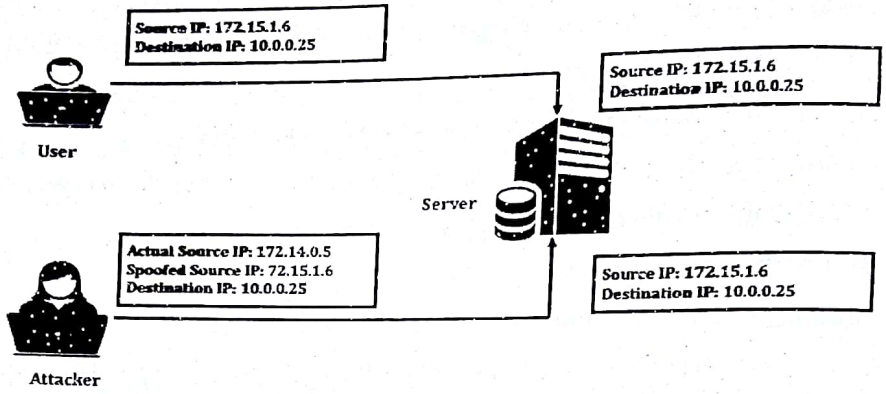


Figure 8.15: Packet Spoofing Example.

SESSION HIJACKING:

1. Session Hijacking is also known as TCP session hijacking.
2. It is a method of taking over a secure/unsecure web user session by secretly obtaining the session ID and masquerading as an authorized user.
3. Once the user's session ID has been accessed, the attacker can masquerade as that user and do anything the user is authorized to do on the network as shown in figure 8.16.

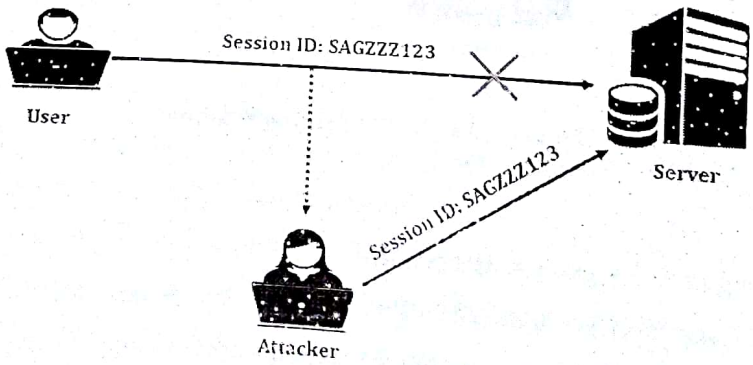


Figure 8.16 Session Hijacking Example.

4. The session ID is stored within a cookie or URL.
5. HTTP cookies are used for authenticating, session tracking, state maintenance and maintaining user information.
6. Session hijacking takes advantage of this practice by intruding in real time during a session.
7. The intrusion may or may not be detectable.

8. If a website does not respond in a normal way to user input or stops responding then session hijacking may be the reason.

Q17] IP spoofing.

Ans: **[5M – Dec15]**

Refer Q16 Packet Spoofing Part.

Q18] Session Hijacking and Spoofing.

Ans: **[5M – May17]**

Refer Q16 Session Hijacking and Packet Spoofing Part.

Q19] Define the following examples:

(i) Salami attack.

(ii) Session Hijacking.

Ans: **[5M – Dec15]**

SALAMI ATTACK:

1. Salami Attack is the series of small attacks which results in large attack.
2. It works on "**Collect & Round Off**" Trick.
3. A salami attack is when small attacks add up to one major attack that can go undetected.
4. It also known as salami slicing or penny shaving.

Example:

- Consider the example of banking system.
- The bank pays 9% interest on accounts deposited in the bank.
- In first month, let's say an account holder gets Rs. 102.25 and in second month he/she gets Rs. 198.54
- But because the bank deals only in Rupees, rounding is performed based on value of residue.
- If residue is half of rupees or more, round up is performed otherwise round down is performed.
- Attacker tries to steal this 0.25 or 0.6 or some other fraction of a rupee in paise and add to its own account.
- Even if the value is negligible for one account holder or transaction, a bank makes a few lakh transactions every day and an attacker may collect these fractional paise from all accounts or transaction to add significant amount his account.

SESSION HIJACKING:

Refer Q16 Session Hijacking part.

Q20] Explain briefly with examples, how the following attacks occur:

i) Salami attack

ii) Denial of Service attack

iii) Session hijacking attack

iv) Cross-site scripting attack.

Ans: **[10M – Dec16]**

SALAMI ATTACK:

Refer Q19 Salami attack part.

DENIAL OF SERVICE ATTACK:

Refer Q1.

SESSION HIJACKING:

Refer Q19 Session Hijacking part.

CROSS-SITE SCRIPTING ATTACK:

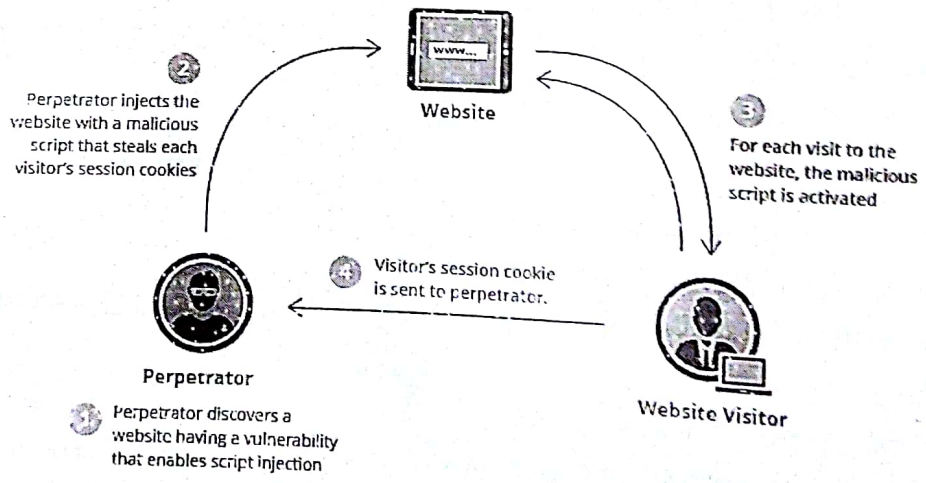


Figure 8.17: Working of XSS

1. Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications.
2. XSS enables attackers to inject client-side scripts into web pages viewed by other users.

3. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.
4. The scripts referred here are **malicious code.**
5. In XSS, the attacker does not directly target the user.
6. Firstly the attacker injects the malicious code into the Web App where the user visits and then the malicious code is delivered to the victim's browser.
7. The figure 8.18 shows the working of XSS.

Q21] Explain briefly with examples, how the following attacks occur: [10M]

(a) Phishing attack.

(b) Denial of Service attack.

(c) SQL injection attack.

(d) Cross-site scripting attack

Ans:

[10M – Dec17]

PHISHING ATTACK:

1. Phishing is an example of **social engineering techniques.**
2. It is used to deceive users.
3. It exploits weaknesses in web security.
4. Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons.
5. Phishing is typically carried out by **email spoofing** or **instant messaging.**
6. A phishing attack usually consists of an authentic-looking sender and a socially engineered message.
7. Many email recipients believe the message is from a trusted individual and will open infected attachments or click on malicious links.

Example:

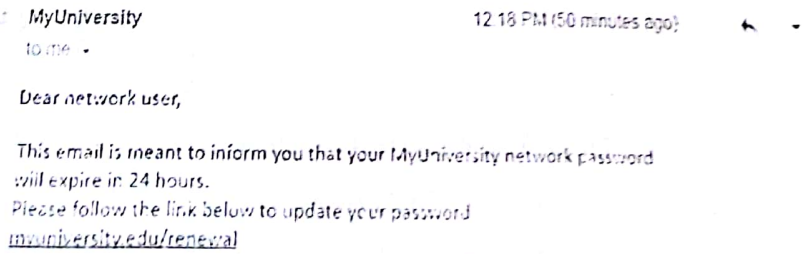


Figure 8.18: Phishing Attack Example.

A spoofed email as shown in figure 8.18 from myuniversity.edu is mass-distributed to as many faculty members as possible.

2. The email claims that the user's password is about to expire.
3. Instructions are given to go to myuniversity.edu/renewal to renew their password within 24 hours.
4. The user is redirected to myuniversity.edurenewal.com, a bogus page appearing exactly like the real renewal page, where both new and existing passwords are requested.
5. The attacker, monitoring the page, hijacks the original password to gain access to secured areas on the university network.
6. The user is sent to the actual password renewal page.
7. However, while being redirected, a malicious script activates in the background to hijack the user's session cookie.
8. This results in a reflected XSS attack, giving the perpetrator privileged access to the university network.

DENIAL OF SERVICE ATTACK:

Refer Q1.

SQL INJECTION ATTACK:

1. SQL injection is a **code injection technique.**
2. It is used to attack **data-driven applications.**
3. SQL injection is a set of SQL commands that are placed in a URL string or in data structures in order to retrieve a response that we want from the databases that are connected with the web applications.
4. This type of attacks generally takes place on webpages developed using PHP or ASP.NET.
5. An SQL injection attack can be done with the following intentions:
   - To dump the whole database of a system.
   - To modify the content of the databases.
   - To perform different queries that are not allowed by the application.

Example:

1. A typical eStore's SQL database query may look like the following:

```
SELECT ItemName, ItemDescription
FROM Item
WHERE ItemNumber = ItemNumber
```

2. From this, the web application builds a string query that is sent to the database as a single SQL statement.
3. A user-provided input http://www.estore.com/items/items.asp?itemid=999 can then generates the following SQL Query.

```
SELECT ItemName, ItemDescription
FROM Item
WHERE ItemNumber = 999
```

4. The above-mentioned input, which pulls information for a specific product, can be altered to read http://www.estore.com/items/items.asp?itemid=999 or 1=1.
5. As a result, the corresponding SQL query looks like this:

```
SELECT ItemName, ItemDescription
FROM Items
WHERE ItemNumber = 999 OR 1=1
```

6. And since the statement 1 = 1 is always true, the query returns all of the product names and descriptions in the database, even those that you may not be eligible to access.

CROSS-SITE SCRIPTING ATTACK:

Refer Q20.

Q22] Why E-commerce transactions need security? Which tasks are performed by payment gateway in E-commerce transaction? Explain the SET (Secure Electronic Transaction) protocol

Ans: **[10M – May18]**

IMPORTANCE OF INTERNET SECURITY:

1. Security is an essential part of any transaction that takes place over the internet.
2. Customers will lose his/her faith in e-business if its security is compromised.
3. Following are the essential requirements for safe e-payments/transactions:
   - **Confidentiality:** Information should not be accessible to an unauthorized person. It should not be intercepted during the transmission.
   - **Integrity:** Information should not be altered during its transmission over the network.
   - **Availability:** Information should be available wherever and whenever required within a time limit specified.
   - **Authenticity:** There should be a mechanism to authenticate a user before giving him/her an access to the required information.
   - **Non-Repudiability:** It is the protection against the denial of payment. Once a sender sends a message, the sender should not be able to deny sending the message. Similarly, the recipient of message should not be able to deny the receipt.
   - **Encryption:** Information should be encrypted and decrypted only by an authorized user.
   - **Auditability:** Data should be recorded in such a way that it can be audited for integrity requirements.

TASKS ARE PERFORMED BY PAYMENT GATEWAY IN E-COMMERCE TRANSACTION:

1. A payment gateway is a merchant service provided by an e-commerce application service provider.
2. Payment gateways facilitate transactions by transferring key information between payment portals such as web-enabled mobile devices/websites and the front end processor/bank.
3. When a customer places an order from an online store, the payment gateway performs several tasks to finalize the transaction.

I) Encryption:

- The web browser encrypts the data to be sent between it and the vendor's web server.
- The gateway then sends the transaction data to the payment processor utilized by the vendor's acquiring bank.

II) Authorization Request:

- The payment processor sends the transaction data to a card association.
- The card's issuing bank views the authorization request and "approves" or "denies."

III) Filling the Order:

- The processor then forwards an authorization pertaining to the merchant and consumer to the payment gateway.
- Once the gateway obtains this response, it transmits it to the website/interface to process the payment.
- Here, it is interpreted and an appropriate response is generated.
- This seemingly complicated and lengthy process typically takes only a few seconds at most.
- At this point, the merchant fills the order.

IV) Clearing Transactions:

- The steps outlined above are repeated in an effort to "clear" the authorization via a consummation of the transaction.
- However, the clearing is only triggered once the merchant has actually completed the transaction

SECURE ELECTRONIC TRANSACTION (SET) PROTOCOL:

1. Secure Electronic Transaction (SET) is a communications protocol standard
2. It is used for securing credit card transactions over networks, specifically, the Internet.
3. It is a secure protocol developed by MasterCard and Visa in collaboration
4. SET protocol restricts revealing of credit card details to merchants thus keeping hackers and thieves at bay.
5. SET protocol includes Certification Authorities for making use of standard Digital Certificates like **X.509 Certificate.**

PARTICIPANTS IN SET:

- **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.

SET FUNCTIONALITIES:

- Provide Authentication.
- Provide Message Confidentiality.
- Provide Message Integrity.

SET WORKING:

Both cardholders and merchants must register with CA (certificate authority) first, before they can buy or sell on the Internet. Once registration is done, cardholder and merchant can start to do transactions, which involve 9 basic steps in this protocol, which is simplified.

1. Customer browses website and decides on what to purchase
2. Customer sends order and payment information, which includes 2 parts in one message:
   a. **Purchase Order:** This part is for merchant.
   b. **Card Information:** This part is for merchant's bank only.
3. Merchant forwards card information (part b) to their bank.
4. Merchant's bank checks with Issuer for payment authorization.
5. Issuer send authorization to Merchant's bank.
6. Merchant's bank send authorization to merchant.
7. Merchant completes the order and sends confirmation to the customer.
8. Merchant captures the transaction from their bank.
9. Issuer prints credit card bill (invoice) to customer.

MISCELLANEOUS

Q1] Timing and Storage Covert Channel.

Ans: [5M – May17]

COVERT CHANNEL:

1. Covert Channel is type of **computer security attack.**
2. It transfers information in a way that violates a security policy.
3. Covert channels have been defined by Lampson in 1973 as a communication channel, not designed for any kind of information transfer.
4. Consider there is group of students preparing for exam, where questions are of objective type.
5. For each question there are four choice of answer: a, b, c, d and right answer has to be selected.
6. Now one who is clever in the group decides to help others.
7. So he/she any reveal the answer by acting in accordance to a predetermined protocol like coughing for answer "a", sighing for answer "b" and so on.
8. Covert channel is hidden communication in open channel.

TIMING COVERT CHANNEL:

1. Timing Covert Channel are **memoryless channel.**
2. In a covert timing channel, the information transmitted from the sender must be sensed by the receiver immediately, otherwise it will be lost.
3. The task of identifying and handling covert timing channel in a secure system is more difficult than storage covert channel.
4. Examples of timing channel are:
   a. I/O Scheduling Control.
   b. Memory Resource Management Channel.
5. Figure 9.1 represents example of covert timing channel.

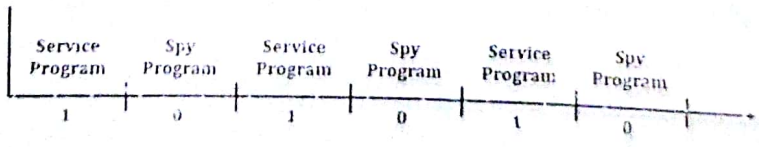


Figure 9.1 (a) Normal Scheduling

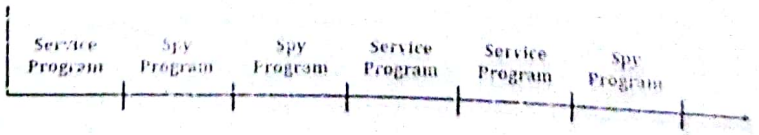


Figure 9.1 (b) Service program communicating 101

Figure 9.1: Example of Timing Covert Channel.

6. In Figure 9.1, the scheduling of service program and spy's program is shown.
7. A service program makes use of timing channel either by using certain amount of time or by not using it.
8. In multi programmed system, time is divided into blocks and allocated to one process and another alternatively.
9. The processing time is rejected by a process if it is waiting for an event to occur and is idle.
10. A block is used by a process to signal 1 and it is rejected to signal 0.
11. Figure 9.1 (a) shows first situation of normal scheduling, where service program and spy program are used alternately.
12. In figure 9.2 (b), the second situation is showed where service program communicates 101 string to spy program.

STORAGE COVERT CHANNEL:

1. A storage covert channel transfers information through the writing of bits by one program and reading those bits by another.
2. Examples of storage covert channel are:
   a. File Lock Channel.
   b. Printer Attachment Channel.
3. Figure 9.2 shows the example of storage covert channel.

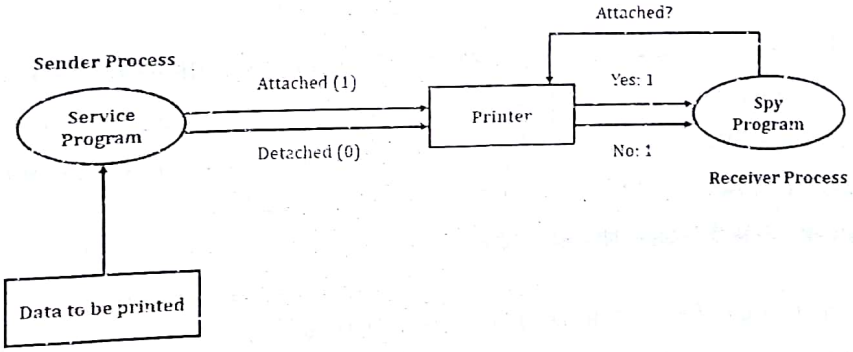


Figure 9.2: Printer Attachment Covert Channel.

4. When physical printers or other I/O devices are shared resources in a system, a sending process 'S' at a high security level could potentially transfer information to a receiving process 'R' at a lower security level by creating contention for the device.
5. The sender and receiver must have some way to synchronize.
6. To send a 1, the sender process simply checks to see if the printer is attached and attaches if it is not.
7. To send a 0, the sender process checks to see if the printer is attached and detaches if it is attached.
8. The receiver process attempts to attach the printer, receiving a 0 if successful and a 1 otherwise.
9. The receiver process then detaches the printer if the attach call was successful.

Mumbai University – Dec 2015

Q1] (a) Define the following examples: [10]

(i) Substitution cipher.

(ii) Poly-alphabetic cipher.

(iii) Salami attack.

(iv) Session Hijacking.

Ans: [Chapter - 2 | Page No. 11 & Chapter – 8 | Page No. 117]

(b) With the help of examples explain non-malicious programming errors. [05]

Ans: [Chapter – 7 | Page No. 88]

(c) Define the goals of security and specify mechanisms to archive each goal. [05]

Ans: [Chapter – 1 | Page No. 2]

Q2] (a) In an RSA system the public key (e, n) of user A is defined as (7, 119). Calculate Φ_n and private key d. what is the cipher text when you encrypt message m=10, using the public key? [10]

Ans: [Chapter – 4 | Page No. 40]

(b) Give the format of X 509 digital certificate and explain the use of a digital signature in it. [05]

Ans: [Chapter – 6 | Page No. 65]

(c) Encrypt "The key is hidden under the door" using play fair cipher with keyword "domestic" [05]

Ans: [Chapter – 2 | Page No. 14]

Q3] (a) Explain how a key is shared between two parties using Diffie-Hellman by exchange algorithm. What is the drawback of this algorithm? [10]

Ans: [Chapter – 4 | Page No. 47]

(b) Differentiate between i) MD-5 and SHA ii) Firewall and IDS. [10]

Ans: [Chapter – 5 & 7 | Page No. 64 & 83]

Q4] (a) Explain working of DES detailing the Fiestel structure. [10]

Ans: [Chapter – 3 | Page No. 26]

(b) What is a Denial of service attack? What are the different ways in which an attacker can mount a DOS attack on a system? [10]

Ans: [Chapter – 8 | Page No. 96]

Q5] (a) List the functions of the different protocols of SSL. Explain the handshake protocol. [05]

Ans: [Chapter – 8 | Page No. 101]

(b) How does PGP achieve confidentially and authentication in emails? [05]

Ans: [Chapter – 6 | Page No. 69]

(c) Differentiate between the transport mode and tunnel mode of IP Sec and explain how authentication and confidentiality are achieved using IP Sec. [10]

Ans: [Chapter – 8 | Page No. 111]

Q6] Write in brief about (any four): [20]

(a) Operating System Security.

Ans: [Chapter - 1| Page No. 1]

(b) Buffer overflow attack.

Ans: [Chapter – 8 | Page No. 114]

(c) IP spoofing.

Ans: [Chapter – 8 | Page No. 117]

(d) Viruses and their types.

Ans: [Chapter – 7 | Page No. 86]

(e) Key generation in IDEA.

Ans: [Chapter – 3 | Page No. 21]

Mumbai University – May 2016

Q1] (a) Explain software flaws with example. **[05]**

Ans: [Chapter – 8 | Page No. 113]

(b) List with example the different mechanisms to achieve security. **[05]**

Ans: [Chapter – 1 | Page No. 2]

(c) Explain with example, keyed and keyless transposition ciphers **[05]**

Ans: [Chapter – 2 | Page No. 12]

(d) Elaborate the steps of key generation using RSA Algorithm. **[05]**

Ans: [Chapter – 4 | Page No. 39]

Q2] (a) A and B decide to use Diffie Hellman Algorithm to share a key. They chose P = 23 and G = 5 as the public parameters. Their secret keys are 6 and 15 respectively. Compute the secret key that they share. **[10]**

Ans: [Chapter – 4 | Page No. 49]

(b) Explain working of DES. **[10]**

Ans: [Chapter – 3 | Page No. 26]

Q3] (a) What is access control? How does the Bell La Padula model achieve access control. **[10]**

Ans: [Chapter – 8 | Page No. 98]

(b) What is a digital signature? Explain any digital signature algorithm in detail. **[10]**

Ans: [Chapter – 5 | Page No. 54]

Q4] (a) Compare packet sniffing and packet spoofing. Explain session hijacking attack. **[10]**

Ans: [Chapter – 8 | Page No. 115]

(b) Explain working of Kerberos. [10]

Ans: [Chapter – 6 | Page No. 74]

Q5] (a) What is a firewall? What are the firewall design principle? [05]

Ans: [Chapter – 7 | Page No. 79]

(b) What are the various ways for memory and address protection. [05]

Ans: [Chapter – 7 | Page No. 90]

(c) Explain the significance of an instruction Detection System for securing a network. Compare signature based and anomaly based IDS. [10]

Ans: [Chapter – 7 | Page No. 84]

Q6] Write in brief about (any four): [20]

(a) Email Security.

Ans: [Chapter – 6 | Page No. 67]

(b) SSL handshake protocol.

Ans: [Chapter – 8 | Page No. 101]

(c) IPSec Protocols for security.

Ans: [Chapter – 8 | Page No. 104]

(d) Denial of service attacks.

Ans: [Chapter – 8 | Page No. 96]

(e) IDEA.

Ans: [Chapter – 3 | Page No. 21]

Mumbai University – Dec 2016

Q1] (a) What are block ciphers? Explain with examples the CBC and ECB modes of block ciphers. [05]

Ans: [Chapter – 3 | Page No. 33]

(b) Encrypt the string "This is an easy task" using a playfair cipher with key "monarchy". [05]

Ans: [Chapter – 2 | Page No. 128]

(c) Define authentication and non-repudiation and show with examples how each one can be achieved. [05]

Ans: [Chapter – 7 | Page No. 92]

(d) Describe triple DES with two DES keys. Is man in the middle attack possible on triple DES? [05]

Ans: [Chapter – 3 | Page No. 31]

Q2] (a) A and B decide to use Diffie Hellman algorithm to share key. They choose p=23 and g=5 as the public parameters. Their secret keys are 6 and 15 respectively. Compute the secret key that they share. [10]

Ans: [Chapter – 4 | Page No. 49]

(b) Compare DES and IDEA. Explain the round key generation scheme in both these algorithms. **[10]**

Ans: [Chapter – 3 | Page No. 32]

Q3] (a) What are the different types of viruses and worms? How do they propagate? **[10]**

Ans: [Chapter – 7 | Page No. 86]

(b) What are the various ways for memory and address protection in Operating systems? How is authentication achieved in O.S? **[10]**

Ans: [Chapter – 7 | Page No. 90]

Q4] (a) Explain briefly with examples, how the following attacks occur: **[10]**

i) Salami attack

ii) Denial of Service attack

iii) Session hijacking attack

iv) Cross-cite scripting attack

Ans: [Chapter – 8 | Page No. 118]

(b) How is security achieved in the transport and tunnel modes of IPSec? Describe the role of AH and ESP. **[10]**

Ans: [Chapter – 8 | Page No. 107]

Q5] (a) How is confidentiality achieved in emails using either S/MIME or PGP? **[05]**

Ans: [Chapter – 6 | Page No. 69]

(b) A and B wish to use RSA to communicate securely. A chooses public key (e, n) as (7, 247) and B chooses public key (e, n) as (5, 221). Calculate their private keys. What will be the cipher text sent by A to B if A wishes to send message m = 5 securely to B? **[10]**

Ans: [Chapter – 4 | Page No. 41]

(c) What is a digital signature? Explain any digital signature algorithm. **[05]**

Ans: [Chapter – 5 | Page No. 54]

Q6] (a) Compare and contrast (any two): **[10]**

i) Block and stream ciphers

ii) MD-5 versus SHA

iii) KDC versus CA

Ans: [Chapter – 2 & 5 | Page No. 19, 64 & 63]

(b) What are firewalls? Explain the different types of firewalls and mention the layer in which they operate. **[10]**

Ans: [Chapter – 7 | Page No. 80]

Mumbai University – May 2017

Q1] (a) Use the Play fair cipher with the keyword: "MEDICINE" to encipher the message "The greatest wealth is health". [05]

Ans: [Chapter – 2 | Page No. 17]

(b) Explain key rings in PGP. [05]

Ans: [Chapter - 6 | Page No. 72]

(c) Briefly define idea behind RSA and also explain [10]

1) What is the one way function in this system?

2) What is the trap door in this?

3) Give Public key and Private Key.

4) Describe security in this system.

Ans: [Chapter – 4 | Page No. 39]

Q2] (a) Explain DES, detailing the Fiestel structure and S-block design [10]

Ans: [Chapter – 3 | Page No. 26]

(b) Consider a Voter data management system in E-voting system with sensitive and non-sensitive attributes.

1) Show with sample queries how attacks (Direct, inference) are possible on such data sets.

2) Suggest 2 different ways to mitigate the problem. [10]

Ans: [Not Included]

Q3] (a) Explain Diffie-Hellman Key exchange algorithm with suitable example. Also explain the problem of MIM attack in it. [10]

Ans: [Chapter – 4 | Page No. 48]

(b) What are Denial of Service attacks? Explain any three types of DOS attacks in detail. [10]

Ans: [Chapter – 8 | Page No. 96]

Q4] (a) IPSec offers security at n/w layer. What is the need of SSL? Explain the services of SSL protocol? [10]

Ans: [Chapter – 8 | Page No. 106]

(b) What are the types of firewalls? How are firewails different from IDS [10]

Ans: [Chapter – 7 | Page No. 80]

Q5] (a) What are the various ways in which public key distribution is implemented. Explain the working of public key certificates clearly detailing the role of certificate authority. [10]

Ans: [Chapter – 4 | Page No. 50]

(b) Why are Digital Signatures & Digital certificates required? What is the significance of Dual Signature? [10]

Ans: [Chapter – 5 | Page No. 56]

Q6] Attempt any 4 [20]

(a) SHA-1 [05]

Ans: [Chapter – 5 | Page No. 58]

(b) Timing and Storage Covert Channel.

Ans: [Miscellaneous | Page No. 124]

(c) Session Hijacking and Spoofing.

Ans: [Chapter – 8 | Page No. 117]

(d) Blowfish.

Ans: [Chapter – 3 | Page No. 23]

(f) S/MIME

Ans: [Chapter – 6 | Page No. 76]

Mumbai University – Dec 2017

Q1] (a) Encrypt the message "Cryptography is fun" with a multiplicative cipher with key = 15. Decrypt to get back original plaintext. [05]

Ans: [Chapter – 3 | Page No. 34]

(b) With the help of suitable examples compare and contrast monoalphabetic ciphers and polyalphabetic ciphers? [05]

Ans: [Chapter – 2 | Page No. 11]

(c) What are the properties of hash functions? What is the role of a hash function in security? [05]

Ans: [Chapter – 5 | Page No. 60]

(d) What are the different protocols in SSL? How do the client and server establish an SSL connection. [05]

Ans: [Chapter – 8 | Page No. 103]

Q2] (a) What is a digital certificate? How does it help to validate the authenticity of a user? Explain the X.509 certificate format. [10]

Ans: [Chapter – 6 | Page No. 66]

(b) With reference to DES comment on the following: [10]

(i) Block size and key size.

(ii) Need for expansion permutation.

(iii) Avalanche and completeness effects.

(iv) Weak keys and semi-weak keys.

(v) Role of S-box.

Ans: [Chapter – 3 | Page No. 29]

Q3] (a) What are the different types of viruses and worms? How do they propagate? [10]

Ans: [Chapter – 7 | Page No. 86]

(b) What are the various ways for memory and address protection in Operating System? [10]

Ans: [Chapter – 7 | Page No. 90]

Q4] (a) Explain briefly with examples, how the following attacks occur: [10]

i) Phishing attack.

ii) Denial of Service attack.

iii) SQL injection attack.

iv) Cross-site scripting attack

Ans: [Miscellaneous | Page No. 119]

(b) How is security achieved in the transport and tunnel modes of IPSec? What are security associations? [10]

Ans: [Chapter – 8 | Page No. 107]

Q5] (a) What are the different threats to emails? Give an algorithm to secure emails being sent from user A to user B. [10]

Ans: [Chapter – 6 | Page No. 70]

(b) A and B wish to use RSA to communicate securely. A chooses public key as (7, 119) and B chooses public key as (13, 221). Calculate their private keys. A wishes to send message m = 10 to B. What will be the ciphertext? With what key will A encrypt the message "m" if A needs to authenticate itself to B. [10]

Ans: [Chapter – 4 | Page No. 43]

Q6] (a) Compare and contrast (any two): [10]

(i) Block and stream ciphers.

Ans: [Chapter – 2 | Page No. 19]

(ii) MD-5 versus SHA

Ans: [Chapter – 5 | Page No. 64]

(iii) Key generation in IDEA and Blowfish

Ans: [Chapter – 3 | Page No. 24]

(b) What are the different components of an Intrusion Detection System? Compare the working of signature based IDS with anomaly based IDS. [10]

Ans: [Chapter – 7 | Page No. 84]

Mumbai University – May 2018

Q1] (a) What is the purpose of S-boxes in DES? Explain the avalanche effect? [05]
Ans: [Chapter – 3 | Page No. 29]
(b) Give examples of replay attacks. List three general approaches for dealing with replay attacks. [05]
Ans: [Chapter – 1 | Page No. 4]
(c) Why is the segmentation and reassembly function in PGP (Pretty Good Privacy) needed? [05]
Ans: [Chapter – 6 | Page No. 71]
(d) List and explain various types of attacks on encrypted message. [05]
Ans: [Chapter – 1 | Page No. 5]

Q2] (a) What is the need for message authentication? List various techniques used for message authentication. Explain any one. [10]
Ans: [Chapter – 5 | Page No. 62]
(b) Explain Kerberos protocol that supports authentication in distributed system. [10]
Ans: [Chapter – 6 | Page No. 74]

Q3] (a) What characteristics are needed in secure hash function? Explain the operation of secure hash algorithm on 512 bit block. [10]
Ans: [Chapter – 5 | Page No. 62]
(b) What is a nonce in key distribution scenario? Explain the key distribution scenario if A wishes to establish logical connection with B. A and B both have a master key which they share with itself and key distribution center. [10]
Ans: [Chapter – 6 | Page No. 77]

Q4] (a) Why E-commerce transactions need security? Which tasks are performed by payment gateway in E-commerce transaction? Explain the SET (Secure Electronic Transaction) protocol. [10]
Ans: [Miscellaneous | Page No. 121]

(b) In RSA system the public key of a given user e = 7 & n= 187 [10]
1) What is the private key of this user?
2) If the intercepted CT=11 and sent to a user whose public key e=7 & n=187. What is the PT?
3) Elaborate various kinds of attacks on RSA algorithm?

Ans: [Chapter – 4 | Page No. 46]

Q5] *(a) How can we achieve web security? Explain with example.* [10]
Ans: [Not Included]
(b) Use Hill cipher to encrypt the text "short". The key to be used is "hill". [10]
Ans: [Chapter – 3 | Page No. 36]

Q6] *(a) Explain IPSec protocol in detail. Also write applications and advantages of IPSec.* [10]
Ans: [Chapter – 8 | Page No. 104]
(b) Differentiate between i) MD-5 and SHA ii) Firewall and IDS. [10]
Ans: [Chapter – 5 & 7 | Page No. 64 & 83]