PVP 23

Code: 23AM4601B, 23DS4601B

III B.Tech - II Semester - Regular Examinations - APRIL 2026

CRYPTOGRAPHY & NETWORK SECURITY

(Common for AIML, DS)

Duration: 3 hours Max. Marks: 70

Note: 1. This question paper contains two Parts A and B.
2. Part-A contains 10 short answer questions. Each Question carries 2 Marks.
3. Part-B contains 5 essay questions with an internal choice from each unit. Each Question carries 10 marks.
4. All parts of Question paper must be answered in one place.

BL – Blooms Level CO – Course Outcome

PART – A

		BL	CO
1.a)	Define confidentiality.	L2	CO1
1.b)	Define authentication.	L2	CO1
1.c)	Describe monoalphabetic cipher.	L2	CO1
1.d)	Define avalanche effect.	L2	CO1
1.e)	Describe AES.	L2	CO1
1.f)	Define Diffie-Hellman algorithm.	L2	CO1
1.g)	Describe digital certificate?	L2	CO1
1.h)	List applications of cryptographic hash functions.	L2	CO1
1.i)	Define Security Association (SA).	L2	CO1
1.j)	Define S/MIME.	L2	CO1

PART – B

			BL	CO	Max. Marks
		UNIT-I			
2	a)	Explain the concept of trusted systems and security models.	L2	CO1	5 M
	b)	Discuss passive attacks and active attacks with suitable examples.	L2	CO1	5 M
		OR			
3	a)	Explain confidentiality, integrity, and availability with examples.	L2	CO1	5 M
	b)	Describe security services provided in network security.	L2	CO1	5 M
		UNIT-II			
4	a)	Apply Caesar cipher for encryption and decryption with example.	L3	CO2	8 M
	b)	Describe AES MixColumns transformation.	L2	CO1	2 M
		OR			
5	a)	Make use of AES structure, explain number of rounds and key size.	L3	CO2	8 M
	b)	Describe block cipher design principles.	L2	CO1	2 M
		UNIT-III			
6	a)	Analyze the RSA algorithm with detailed steps.	L4	CO4	8 M
	b)	Describe digital signature verification.	L2	CO1	2 M

OR					
7	a)	Analyze the Elliptic Curve Cryptography and its working principle.	L4	CO4	8 M
	b)	Describe the applications of public key cryptography.	L2	CO1	2 M
UNIT-IV					
8	a)	Apply the role of hash functions in message authentication.	L3	CO3	5 M
	b)	Describe hash functions based on Cipher Block Chaining (CBC).	L2	CO1	5 M
OR					
9	a)	Apply the Elliptic Curve Digital Signature Algorithm.	L3	CO3	5 M
	b)	List attacks on digital signatures.	L2	CO1	5 M
UNIT-V					
10	a)	Explain IP Security policy and Security Association Database.	L2	CO1	3 M
	b)	Analyze the ESP packet format used in IPsec.	L4	CO4	7 M
OR					
11	a)	Explain email threats and comprehensive email security.	L2	CO1	3 M
	b)	Analyze the Internet mail architecture and email components.	L4	CO4	7 M

Code: 23AM4601B, 23DS4601B

PVP 23

III B.Tech-II Semester - Regular Examinations-April - 2026

CRYPTOGRAPHY & NETWORK SECURITY
(Common for AIML, DS)

Short Answer Key

PART – A

1.(a). Define confidentiality. ---------- 2M

Ans: Definition of confidentiality.

1.(b). Define authentication. ----------2M

Ans: Definition of Authentication.

1.(c). Describe monoalphabetic cipher ----------2M
Ans: Description about Monoalphabetic Cipher.

1.(d). Define avalanche effect. ----------2M
Ans: Definition of avalanche effect .

1.(e). Describe AES. ----------2M
Ans: Description about AES.

1.(f). Define Diffie-Hellman algorithm. ----------s--2M
Ans: Description about Diffie-Hellman algorithm.

1.(g). Describe digital certificate? ----------2M
Ans: Description about digital certificate.

1.(h). List applications of cryptographic hash functions. ----------2M
Ans: List the Three Applications.

1.(i). Define Security Association (SA). ----------2M
Ans: Definition of Security Association.

1.(j). Define S/MIME. ----------2M
Ans: Definition of S/MIME.

PART – B

UNIT-I

2. (a). Explain the concept of trusted systems and security models. ----------5M

Ans:

1.Trusted Systems ----------2M

2.Security Models----------3M

No security

Security through obscurity

Host security

Network security

2. (b).Discuss passive attacks and active attacks with suitable examples. ---------- -5M

Ans:

Passive Attacks----------2M

Active Attacks ----------3M

3.(a). Explain confidentiality, integrity, and availability with examples. ---------- 5M

Ans:

1. Confidentiality----------2M

2. Integrity----------2M

3. Availability----------1M

3.(b). Describe security services provided in network security. ----------5M

Ans:

Security services (Each service carry 1M)—5M(5*1)

Authentication

Access Control

Data Confidentiality

Data Integrity

Non-Repudiation

Availability

UNIT-II

4.(a). Apply Caesar cipher for encryption and decryption with example. ----------8M

Ans:

Caesar Cipher Description----------2M

Encryption----------2M

Decryption----------2M

Example----------2M

Note: Students choose their own Example.

4.(b).Describe AES MixColumns transformation.----------2M

Ans:

Mix Columns Description----------1M

Example----------1M

5.(a). Make use of AES structure, explain number of rounds and key size. ----------8M

Ans:

Advanced Encryption Standard (Aes) Algorithm ---------2M

Operation of AES ----------3M

Encryption Process ----------2M

Decryption Process ----------1M

5.(b). Describe block cipher design principles.----------2M

Ans: Each design principle carry 1M----------2M(2*1)

Number of Rounds

Design of Function F

Key Schedule Algorithm

UNIT-III

6.(a). Analyze the RSA algorithm with detailed steps.----------8M

Ans:

Description of the Algorithm ----------5M

Example of RSA algorithm----------2M

Analysis Diagram----------1M

Note: Students Choose their own Example.

6.(b). Describe digital signature verification ----------2M

Ans: Digital Signature Verification Description ---2M

7.(a). Analyze the Elliptic Curve Cryptography and its working principle. ----------8M

Ans: Analog of Diffie–Hellman Key Exchange ----------4M

Elliptic Curve Encryption/Decryption----------4M

7.(b). Describe the applications of public key cryptography----------2M

Ans: applications of public key cryptography ----------2M(2*1)

(Each application carry 1M)

public-key cryptosystems into three categories

Encryption/decryption

Digital signature

Key exchange

UNIT-IV

8.(a). Apply the role of hash functions in message authentication.----------5M

Ans:

Description----------1M

Message Authentication(Each one 1M)----------4M(4*1)

8.(b). Describe hash functions based on Cipher Block Chaining (CBC). ----------5M

Ans:

Description----------2M

Diagram----------3M

9.(a). Apply the Elliptic Curve Digital Signature Algorithm.----------5M

Ans:

Elliptic Curve Digital Signature Algorithm----------2M

Key Generation ----------1M

Digital Signature Generation and Authentication-----2M

9.(b). List attacks on digital signatures----------5M

Ans: Each attack carry 1M----------5M(5*1)

- Key-only attack
- Known message attack
- Generic chosen message attack

- Directed chosen message attack
- Adaptive chosen message attack

UNIT-V

10.(a). Explain IP Security policy and Security Association Database.----------3M

Ans:

IP Security Policy----------1M

Security Association Database----------2M

10.(b). Analyze the ESP packet format used in IPsec ----------7M

Ans:

ESP Format ----------3M

Transport and Tunnel Modes----------2M

11.(a). Explain email threats and comprehensive email security. ----------3M

Ans: Each one Carry ½ M----------2M(4*1/2)

email security threats can be classified as follows:

- Authenticity-related threats
- Integrity-related threats
- Confidentiality-related threats
- Availability-related threats

11.(b). Analyze the Internet mail architecture and email components.----------7M

Ans:

Email Components----------4M

- Message User Agent (MUA)
- Mail Submission Agent (MSA)
- Message Transfer Agent (MTA)
- Mail Delivery Agent (MDA)
- Message Store (MS)

Internet mail architecture ----------3M

Code: 23AM4601B, 23DS4601B

PVP 23

III B.Tech-II Semester - Regular Examinations-April - 2026

CRYPTOGRAPHY & NETWORK SECURITY
(Common for AIML, DS)

Answer Key

PART – A

1.(a). Define confidentiality. ---------- 2M

Ans: The principle of confidentiality specifies that only the sender and the intended recipient(s) should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access a message.

1.(b). Define authentication. ----------2M

Ans: Authentication mechanisms help establish proof of identities. The authentication process ensures that the origin of a electronic message or document is correctly identified.

1.(c). Describe monoalphabetic cipher ----------2M
Ans:

Monoalphabetic Ciphers

A monoalphabetic cipher is a classical substitution cipher in which each letter of the plaintext is replaced by a fixed corresponding letter of the ciphertext alphabet.

- One-to-one mapping
- Same substitution rule is used throughout the message
- Simple but vulnerable to frequency analysis

1.(d). Define avalanche effect. ----------2M
Ans:
The avalanche effect in Cryptography and Network Security is a property of secure cryptographic algorithms where a small change in the input (such as changing one bit of plaintext or key) causes a large and unpredictable change in the output (ciphertext or hash value).

1.(e). Describe AES. ----------2M
Ans:

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

The features of AES are as follows:

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

1.(f). Define Diffie-Hellman algorithm. ----------2M

Ans:

Diffie and Martin Hellman devised an amazing solution to the problem of key agreement, or key exchange in 1976. This solution is called as the Diffie-Hellman Key Exchange /Agreement Algorithm. The beauty of this scheme is that the two parties, who want to communicate securely, can agree-on a symmetric key using this technique.

It might come as a surprise, but Kl is actually equal to K2! This means that Kl =K2 = K is the symmetric key.

1.(g). Describe digital certificate? ----------2M

Ans:

- Another important application, which is similar to the message authentication application, is the digital signature.
- The hash value of a message is encrypted with a user's private key.
- Anyone who knows the user's public key can verify the integrity of the message that is associated with the digital signature.

1.(h). List applications of cryptographic hash functions. ----------2M

Ans:

- Message Authentication
- Digital Signatures
- Other Applications

1.(i). Define Security Association (SA). ----------2M

Ans:

Security Associations:IPSEC is designed to be able to use various security protocols, it uses Security Associations (SA) to specify the protocols to be used. SA is a database record which specifies security parameters controlling security operations.

1.(j). Define S/MIME. ----------2M

Ans:

Secure/Multipurpose Internet Mail Extension (S/MIME) is a security enhancement to the MIME Internet email format standard based on technology from RSA Data Security.

PART – B

UNIT-I

2. (a). Explain the concept of trusted systems and security models. ----------5M

Ans:

1.Trusted Systems: A trusted system is a computer system that can be trusted to a specified extent to enforce a specified security policy.

Trusted systems were initially of primary interest to the military. However, these days, the concept has spanned across various areas, most prominently in the banking and financial community, but the concept never caught on. Trusted systems often use the term reference monitor.

It is mainly responsible for all the decisions related to access controls. Naturally, following are the expectations from the reference monitor:

(a) It should be tamperproof

(b) It should always be invoked

(c) It should be small enough so that it can be independently tested

2.Security Models:

An organization can take several approaches to implement its security model. Let us summarize these approaches.

No security:

In this simplest case, the approach could be a decision to implement no security at all.

Security through obscurity:

In this model, a system is secure simply because nobody knows about its existence and contents. This approach cannot work for too long, as there are many ways an attacker can come to know about it.

Host security:

In this scheme, the security for each host is enforced individually. This is a very safe approach, but the trouble is that it cannot scale well. The complexity and diversity of modern sites/organizations makes the task even harder.

Network security:

Host security is tough to achieve as organizations grow and become more diverse. In this technique, the focus is to control network access to various hosts and their services, rather than individual host security. This is a very efficient and scalable model.

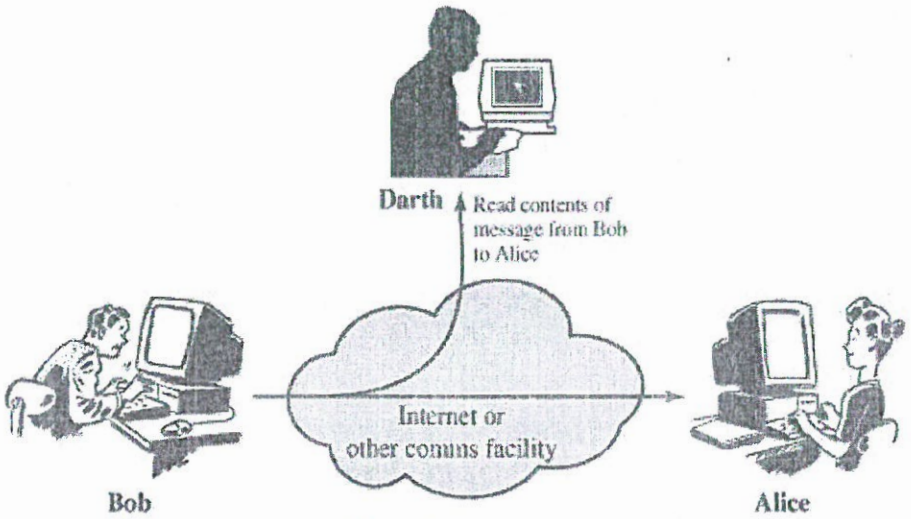
2. (b).Discuss passive attacks and active attacks with suitable examples. ---------- -5M

Ans:

Passive Attacks:

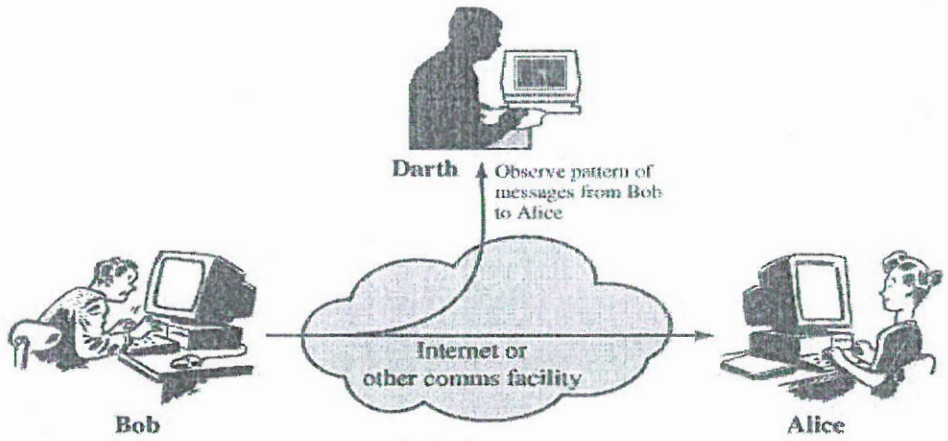
Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are the **release of message contents** and **traffic analysis**.

The **release of message contents** is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.



(a) Release of message contents

Traffic analysis: If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place.



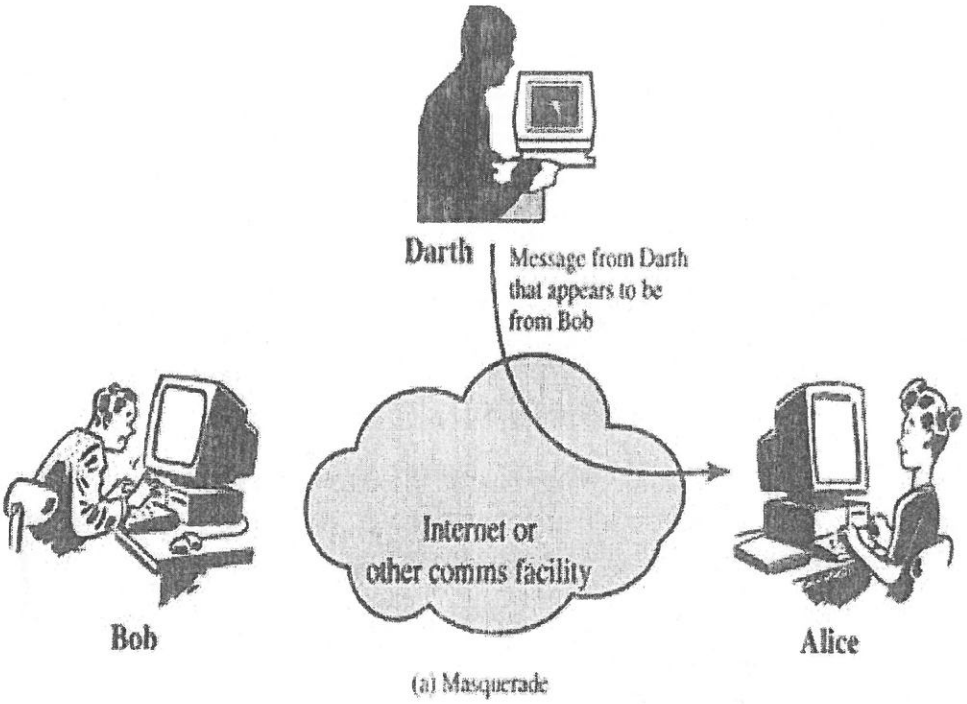
(b) Traffic analysis

Passive attacks are very difficult to detect, because they do not involve any alteration of the data.

Active Attacks

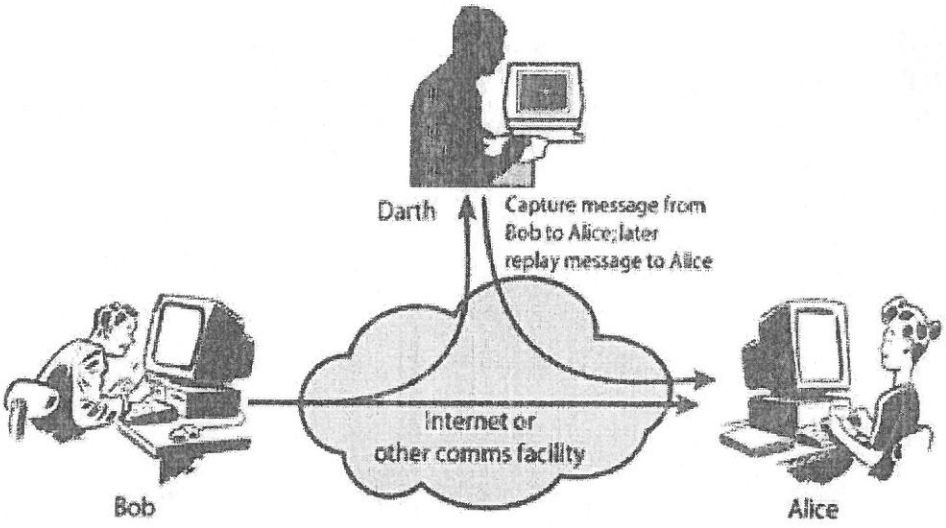
Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages and denial of service.

A **masquerade** takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack.

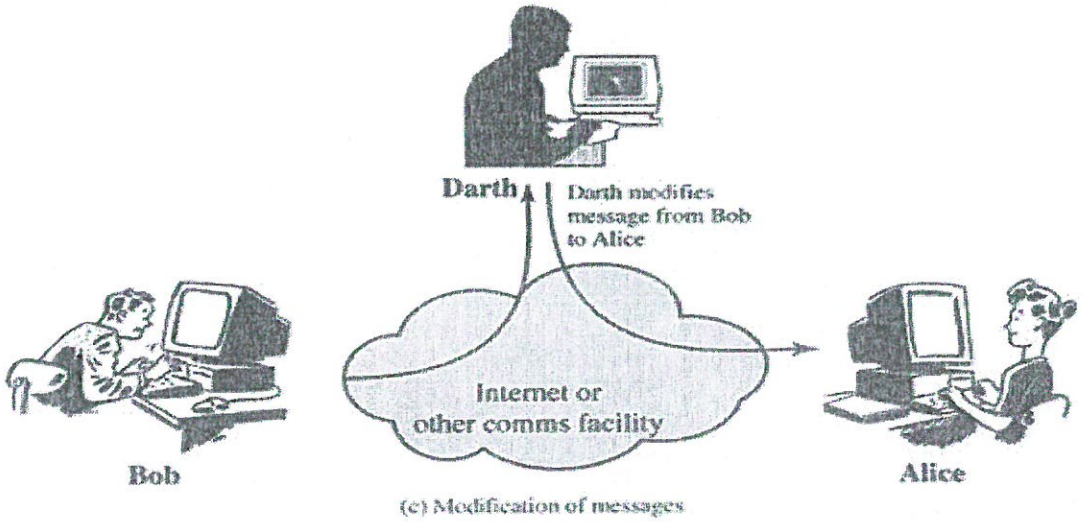


(a) Masquerade

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

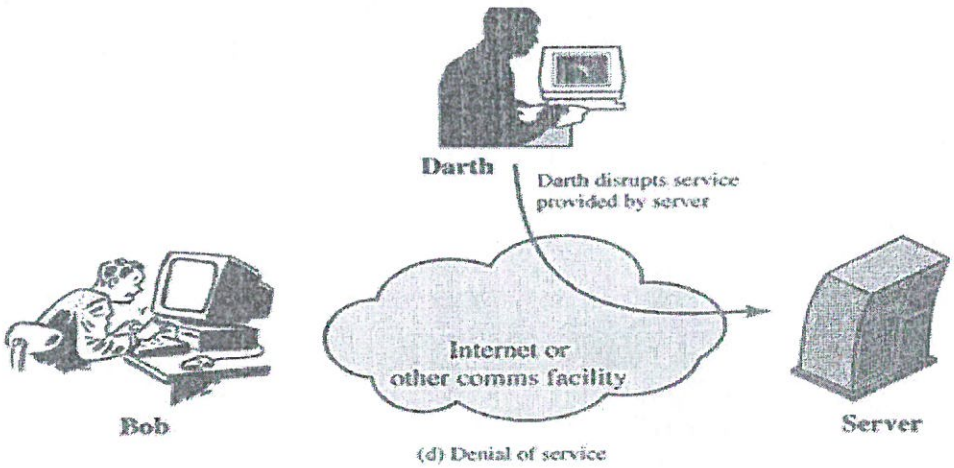


Modification of messages – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.



(c) Modification of messages

Denial of service – Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance.



(d) Denial of service

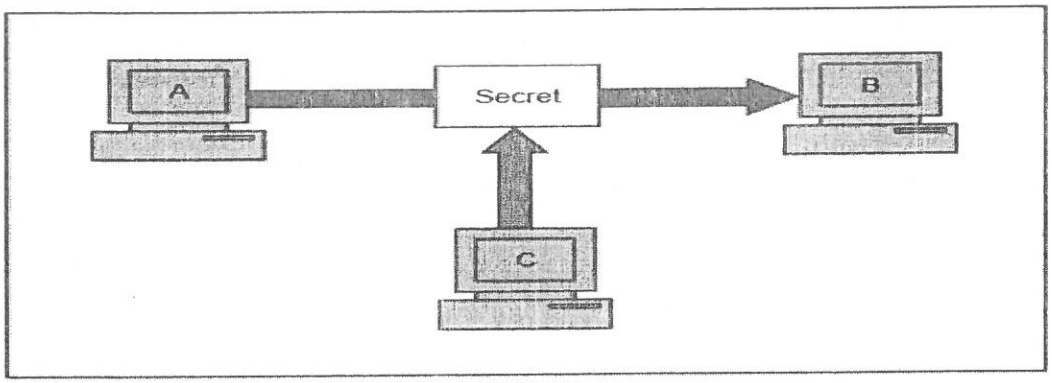
3.(a). Explain confidentiality, integrity, and availability with examples. ---------- 5M

Ans:

1. Confidentiality:

The principle of confidentiality specifies that only the sender and the intended recipient(s) should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access a message. Example of compromising the confidentiality of a message is shown in Fig. Here, the user of computer A sends a message to user of computer B. Another user C gets access to this message, which is not desired and therefore, defeats the purpose of confidentiality. Example of this could be a confidential email message sent by A to B, which is accessed by C without the permission or knowledge of A and B. This type of attack is called as interception.

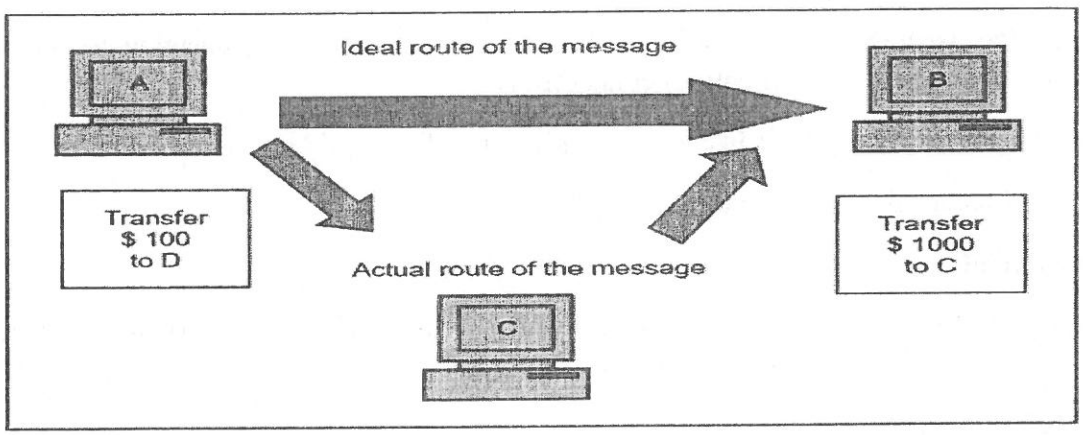
Interception causes loss of message confidentiality.



Loss of confidentiality

Integrity:

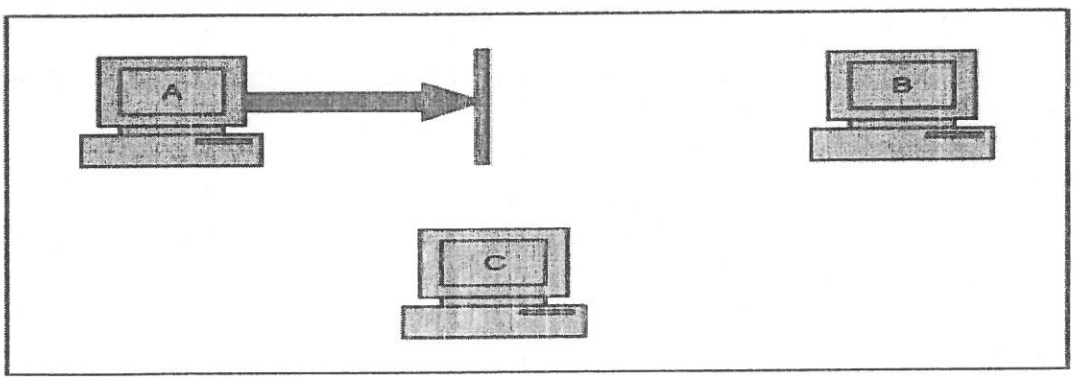
When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost. For example, suppose you write a check for Rs. 100 to pay for the goods bought from the US. However, when you see your next account statement, you are startled to see that the check resulted in a payment of Rs. 1000. This is the case for loss of message integrity.



Loss of integrity

Availability:

The principle of availability states that resources (i.e. information) should be available to authorized parties at all times. For example, due to the intentional actions of an unauthorized user C, an authorized user A may not be able to contact a server computer B.



Attack on availability

3.(b). Describe security services provided in network security. ----------5M

Ans:

Security services:

It is a processing or communication service that is provided by a system to give a specific kind of production to system resources. Security services implement security policies and are implemented by security mechanisms.

Authentication

This service assures that a communication is authentic. For a single message transmission, its function is to assure the recipient that the message is from intended source. For an ongoing interaction two aspects are involved. First, during connection initiation the service assures the authenticity of both parties. Second, the connection between the two hosts is not interfered allowing a third party to masquerade as one of the two parties. Two specific authentication services defines in X.800 are

1.Peer Entity Authentication

2.Data-Origin Authentication

1.Peer Entity Authentication: Used in association with a logical connection to provide confidence in the identity of the entities connected.

2.Data-Origin Authentication: In a connectionless transfer, provides assurance that

the source of received data is as claimed.

Access Control

In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links.

Data Confidentiality

The protection of data from unauthorized disclosure.

Connection Confidentiality: The protection of all user data on a connection.

Connectionless Confidentiality: The protection of all user data in a single data block.

Selective-Field Confidentiality: The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality: The protection of the information that might be derived from observation of traffic flows.

Data Integrity

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery

Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery

Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted, but provides only detection without recovery.

Selective-Field Connection Integrity

Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity

Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity

Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

Non-Repudiation

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin

Proof that the message was sent by the specified party.

Nonrepudiation, Destination

Proof that the message was received by the specified party

Availability:

Both X.800 and RFC 4949 define availability to be the property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.

UNIT-II

4.(a). Apply Caesar cipher for encryption and decryption with example. ----------8M

Ans:

CAESAR CIPHER

The earliest known use of a substitution cipher, and the simplest, was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

For example,

Plain text : meet me after the toga party

Cipher Text : PHHW PH DIWHU WKH WRJD SDUWB

Note that the alphabet is wrapped around, so that the letter following Z is A. We can define the transformation by listing all possibilities, as follows:

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

Let us assign a numerical equivalent to each letter:

A	b	c	d	e	F	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
N	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

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

$C = E(3, p) = (p + 3) \bmod 26$

A shift may be of any amount, so that the general Caesar algorithm is $C = E(k, p) = (p + k) \bmod 26$

where k takes on a value in the range 1 to 25.

The decryption algorithm is simply $p = D(k, C) = (C- k) \bmod 26$

If it is known that a given cipher text is a Caesar cipher, then a brute-force cryptanalysis is easily performed: Simply try all the 25 possible keys.

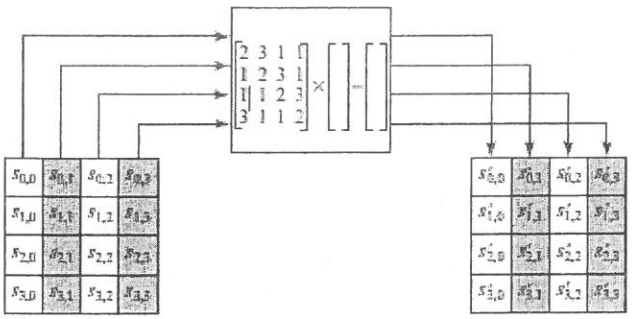
Note: Students choose their own Example.

4.(b).Describe AES MixColumns transformation.----------2M

Ans:

Mix Columns

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



(b) Mix column transformation

5.(a). Make use of AES structure, explain number of rounds and key size. ----------8M

Ans:

ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

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

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

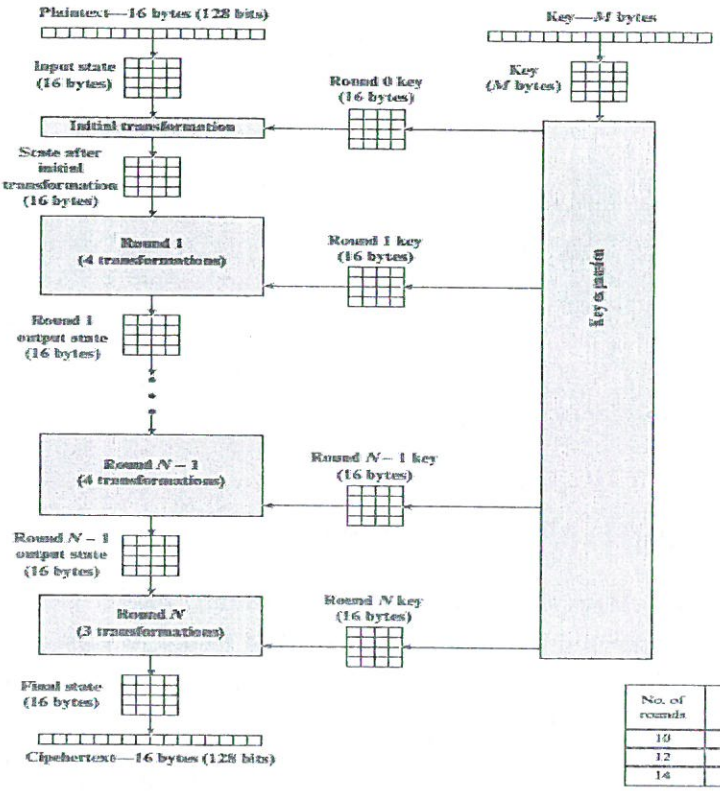
The features of AES are as follows:

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

Operation of AES

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix: Unlike DES, the number of rounds in AES is variable and depends on the length of the key.

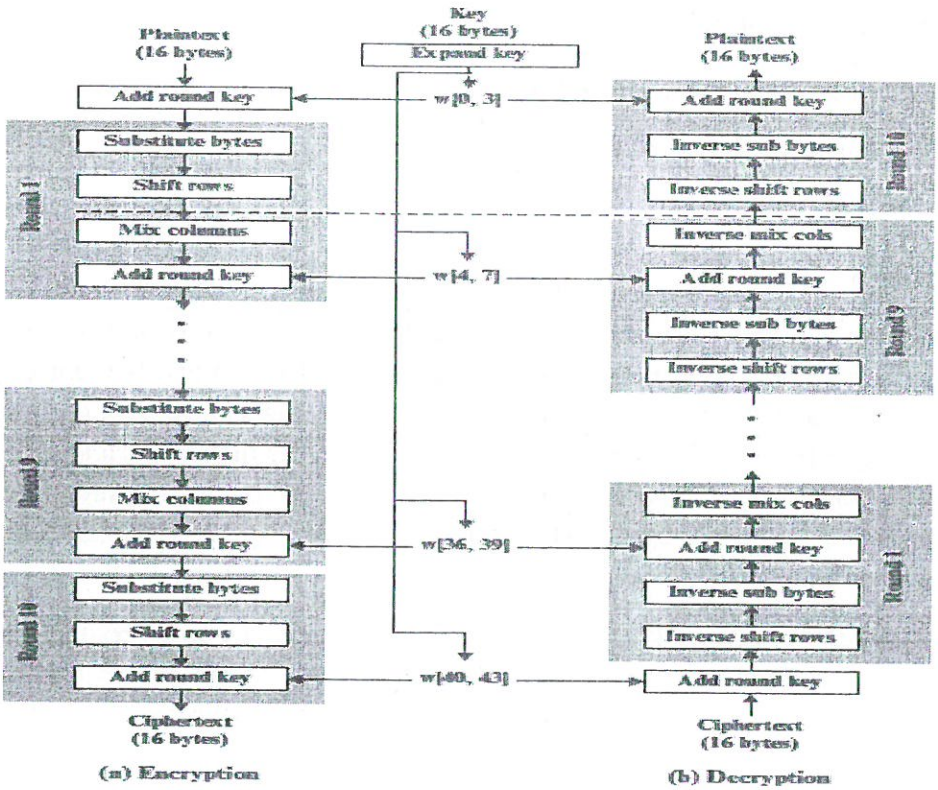
AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. The schematic of AES structure is given in the following illustration:



No. of rounds	Key Length (bytes)
10	16
12	24
14	32

Encryption Process

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



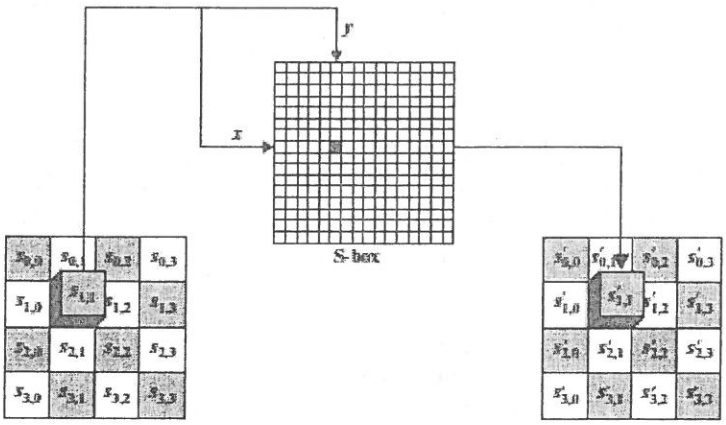
Byte Substitution (Sub Bytes)

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

This stage (known as Sub Bytes) is simply a table lookup using a 16 × 16 matrix of byte values called an s-box.

This matrix consists of all the possible combinations of (16× 16 = 256).

However, the s-box is not just a random permutation of these values and there is a well defined method for creating the s-box tables.

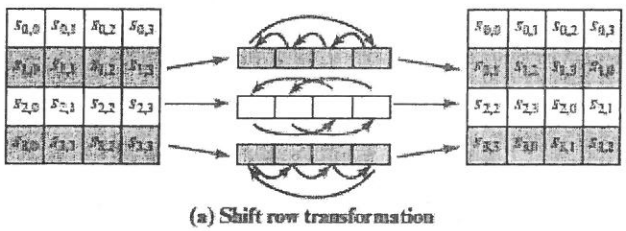


(a) Substitute byte transformation

Shift rows

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

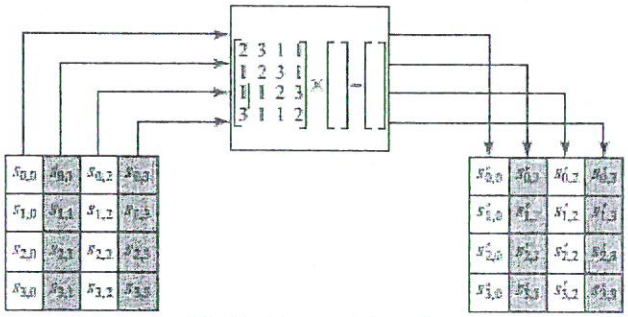
- First row is not shifted
- Second row is shifted one (byte) position to the left
- Third row is shifted two positions to the left
- Fourth row is shifted three positions to the left
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other



(a) Shift row transformation

Mix Columns

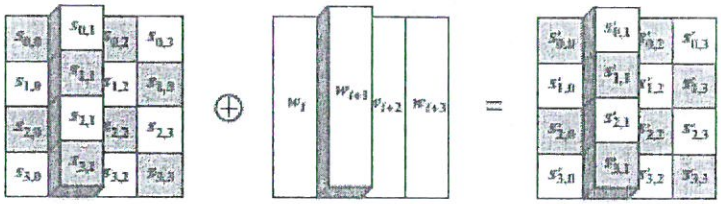
Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that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



(b) Mix column transformation

Add round key

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



(b) Add round key transformation

Decryption Process

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

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

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

5.(b). Describe block cipher design principles.----------2M

Ans:

Number of Rounds

The cryptographic strength of a Feistel cipher derives from three aspects of the design: the number of rounds, the function F, and the key schedule algorithm. Let us look first at the choice of the number of rounds.

Design of Function F

The heart of a Feistel block cipher is the function F, which provides the element of confusion in a Feistel cipher. Thus, it must be difficult to "unscramble" the substitution performed by F. One obvious criterion is that F be nonlinear, as we discussed previously. The more nonlinear F, the more difficult any type of cryptanalysis will be.

Key Schedule Algorithm

Feistel block cipher, the key is used to generate one subkey for each round. In general, we would like to select subkeys to maximize the difficulty of deducing individual subkeys and the difficulty of working back to the main key.

UNIT-III

6.(a). Analyze the RSA algorithm with detailed steps.----------8M

Ans:

RSA ALGORITHM:

The Rivest-Shamir- Adleman (RSA) scheme has since that time reigned supreme as the most widely accepted and implemented general-purpose approach to public-key encryption.

The RSA scheme is a block cipher in which the plaintext and cipher text are integers between 0 and n - 1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 2^{1024}. We examine RSA in this section in some detail, beginning with an explanation of the algorithm. Then we examine some of the computational and crypt analytical implications of RSA

Description of the Algorithm

RSA makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to log2 (n) + 1; in practice, the block size is i bits, where $2^i < n \leq 2^{i+1}$. Encryption and decryption are of the following form, for some plaintext block M and cipher text block C.

$$C = M^e \bmod n$$
$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of PU = {e, n} and a private key of PR = {d, n}.

For this algorithm to be satisfactory for public-key encryption, the following requirements must be met.

1. It is possible to find values of e, d, n such that $Med \bmod n = M$ for all $M < n$.

2. It is relatively easy to calculate M^e mod n and C^d mod n for all values of $M < n$.

3. It is infeasible to determine d given e and n.

Key Generation by Alice	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calcuate $\phi(n) = (p - 1)(q - 1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption by Alice with Alice's Public Key	
Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Example of RSA algorithm:

1. Select two prime numbers, $p = 17$ and $q = 11$.

2. Calculate $n = pq = 17 * 11 = 187$.

3. Calculate f(n) = (p - 1)(q - 1) = 16 * 10 = 160.

4. Select e such that e is relatively prime to f(n) = 160 and less than f(n); we choose $e = 7$.

5. Determine d such that de K 1 (mod 160) and d 6 160. The correct value is $d = 23$, because 23 * 7 = 161 = (1 * 160) + 1; d can be calculated using the extended Euclid's algorithm (Chapter 2).

The resulting keys are public key $PU = \{7, 187\}$ and private key $PR = \{23, 187\}$. The example shows the use of these keys for a plaintext input of $M = 88$. For encryption, we need to calculate $C = 887$ mod 187. Exploiting the properties of

modular arithmetic, we can do this as follows.

887 mod 187 = [(884 mod 187) * (882 mod 187)

* (881 mod 187)] mod 187

881 mod 187 = 88

882 mod 187 = 7744 mod 187 = 77

884 mod 187 = 59,969,536 mod 187 = 132

887 mod 187 = (88 * 77 * 132) mod 187 = 894,432 mod 187 = 11

For decryption, we calculate $M = 1123 \bmod 187$:

1123 mod 187 = [(111 mod 187) * (112 mod 187) * (114 mod 187)

* (118 mod 187) * (118 mod 187)] mod 187

111 mod 187 = 11

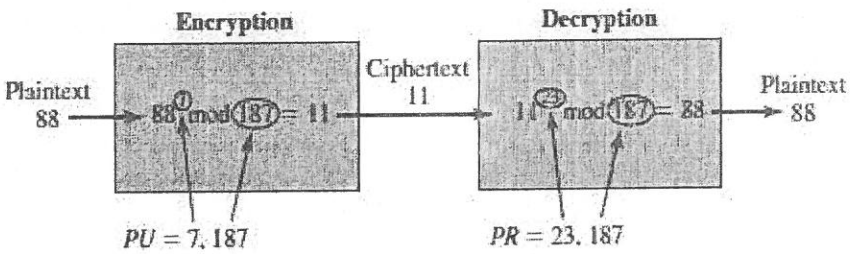
112 mod 187 = 121

114 mod 187 = 14,641 mod 187 = 55

118 mod 187 = 214,358,881 mod 187 = 33

1123 mod 187 = (11 * 121 * 55 * 33 * 33) mod 187

= 79,720,245 mod 187 = 88



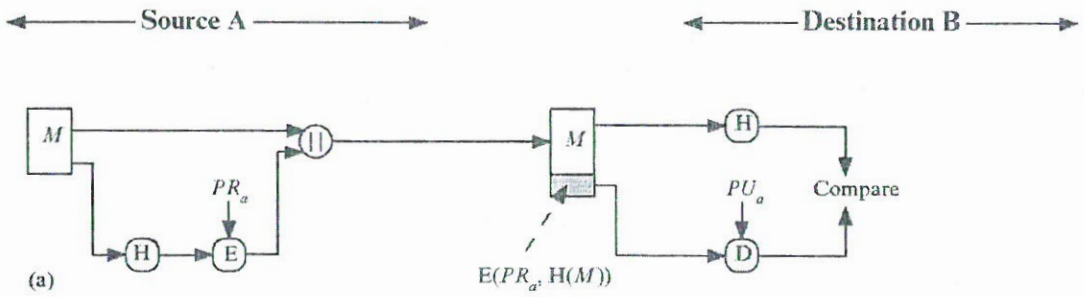
Note: Students Choose their own Example.

6.(b). Describe digital signature verification ----------2M

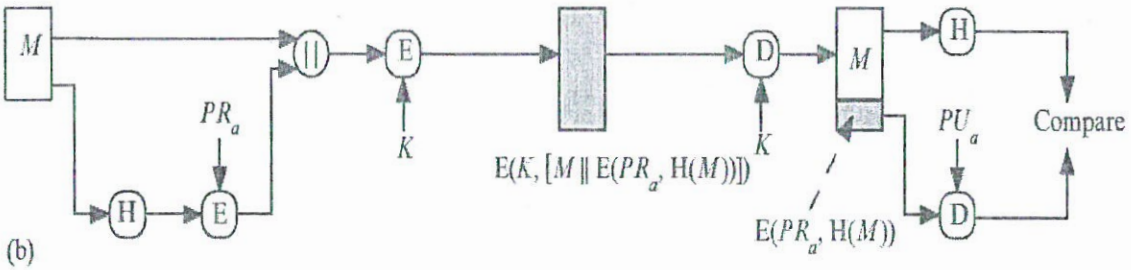
Ans:

Digital Signature:

- Another important application, which is similar to the message authentication application, is the digital signature.
- The hash value of a message is encrypted with a user's private key.
- Anyone who knows the user's public key can verify the integrity of the message that is associated with the digital signature.



- The hash code is encrypted, using public-key encryption with the sender's private key.
- This provides authentication.
- It also provides a digital signature, because only the sender could have produced the encrypted hash code.
- In fact, this is the essence of the digital signature technique.



If confidentiality as well as a digital signature is desired, then the message plus the private-key-encrypted hash code can be encrypted using a symmetric secret key. This is a common technique.

7.(a). Analyze the Elliptic Curve Cryptography and its working principle. ----------8M

Ans:

- The principal attraction of ECC, compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead.
- ECC is fundamentally more difficult to explain than either RSA or Diffie–Hellman.
- For elliptic curve cryptography, an operation over elliptic curves, called addition, is used. Multiplication is defined by repeated addition.
- An **elliptic curve** is defined by an equation in two variables with coefficients. For cryptography, the variables and coefficients are restricted to elements in a finite field.
- equations of the form $y2 = x3 + ax + b$
- The addition operation in ECC is the counterpart of modular multiplication in RSA, and multiple addition is the counterpart of modular exponentiation.

- To form a cryptographic system using elliptic curves, we need to find a "hard problem" corresponding to factoring the product of two primes or taking the discrete logarithm.
- Consider the equation $Q = kP$ where $Q, P \in EP(a, b)$ and $k < p$. It is relatively easy to calculate Q given k and P, but it is hard to determine k given Q and P.

Analog of Diffie–Hellman Key Exchange:

Key exchange using elliptic curves can be done in the following manner. First pick a large integer q, which is either a prime number p or an integer of the form 2^m, and elliptic curve parameters a and b. This defines the elliptic group of points $Eq(a, b)$. Next, pick a *base point* $G = (x1, y1)$ in $Ep(a, b)$ whose order is a very large value n. The **order** n of a point G on an elliptic curve is the smallest positive integer n such that $n G = 0$ and G are parameters of the cryptosystem known to all participants.

A key exchange between users A and B can be accomplished as follows.

Global Public Elements	
$E_q(a, b)$	elliptic curve with parameters a, b, and q, where q is a prime or an integer of the form 2^m
G	point on elliptic curve whose order is large value n

User A Key Generation	
Select private n_A	$n_A < n$
Calculate public P_A	$P_A = n_A \times G$

User B Key Generation	
Select private n_B	$n_B < n$
Calculate public P_B	$P_B = n_B \times G$

Calculation of Secret Key by User A
$K = n_A \times P_B$

Calculation of Secret Key by User B
$K = n_B \times P_A$

Elliptic Curve Encryption/Decryption:

It is the point *Pm(plain text)* that will be encrypted as a ciphertext and subsequently decrypted.an encryption/decryption system requires a point G and an elliptic group $Eq(a, b)$ as parameters. Each user A selects a private key n_A and generates a public key $P_A = n_A * G$.

To encrypt and send a message Pm to B, A chooses a random positive integer k and produces the ciphertext Cm consisting of the pair of points:

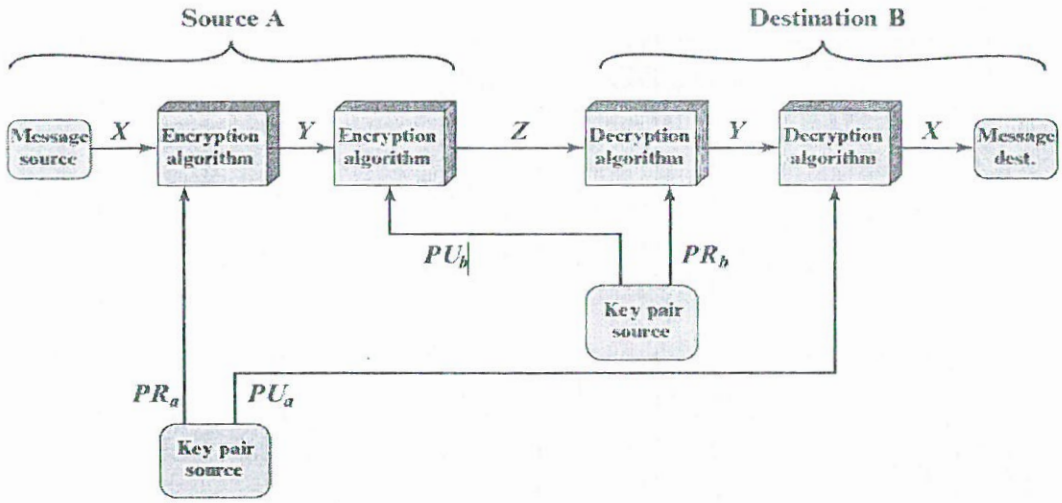
$Cm = \{kG, Pm + kP_B\}$

To decrypt the ciphertext, B multiplies the first point in the pair by B's private key and subtracts the result from the second point:

$Pm=C_2+(-KC_1)$

7.(b). Describe the applications of public key cryptography----------2M

Ans:



public-key cryptosystems into three categories

Encryption/decryption: The sender encrypts a message with the recipient's public key, and the recipient decrypts the message with the recipient's private key.

Digital signature: The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.

Key exchange: Two sides cooperate to exchange a session key, which is a secret key for symmetric encryption generated for use for a particular transaction (or session) and valid for a short period of time. Several different approaches are possible, involving the private key(s) of one or both parties.

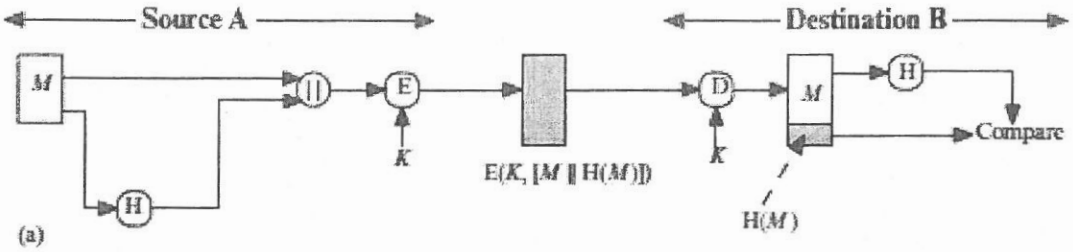
UNIT-IV

8.(a). Apply the role of hash functions in message authentication.----------5M

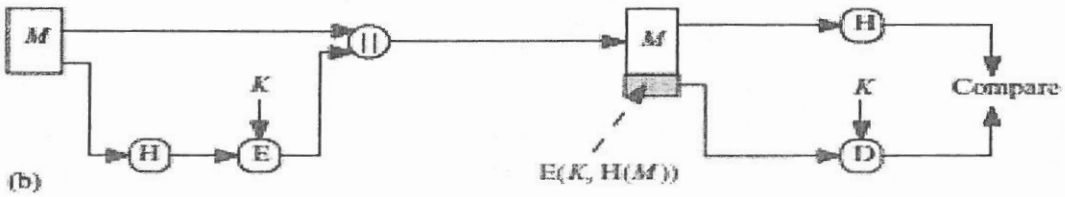
Ans:

Message Authentication:

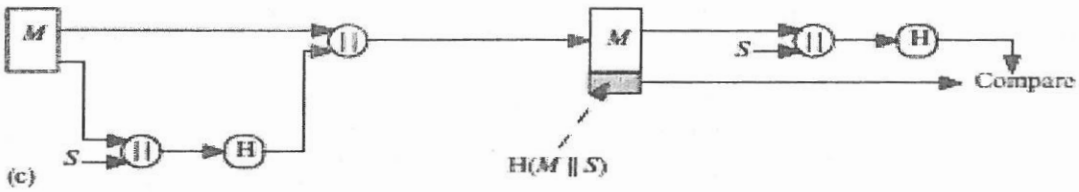
- Message authentication is a mechanism or service used to verify the integrity of a message.
- Message authentication assures that data received are exactly as sent.
- When a hash function is used to provide message authentication, the hash function value is often referred to as a **message digest**.



- The message plus concatenated hash code is encrypted using symmetric encryption. Because only A and B share the secret key, the message must have come from A and has not been altered.
- The hash code provides the structure or redundancy required to achieve authentication.
- Because encryption is applied to the entire message plus hash code, confidentiality is also provided.

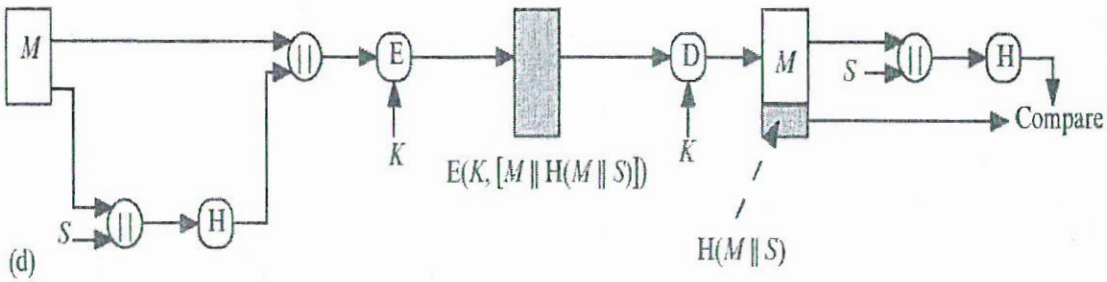


- This diagram shows the authentication.
- Only the hash code is encrypted, using symmetric encryption.
- This reduces the processing burden for those applications that do not require confidentiality.



- The technique assumes that the two communicating parties share a common secret value *S*.
- A computes the hash value over the concatenation of *M* and *S* and appends the resulting hash value to *M*.

- Because B possesses S, it can recompute the hash value to verify. Because the secret value itself is not sent, an opponent cannot modify an intercepted message and cannot generate a false message.



- Confidentiality can be added to the approach of method (c) by encrypting the entire message plus the hash code.

8.(b). Describe hash functions based on Cipher Block Chaining (CBC). ----------5M

Ans:

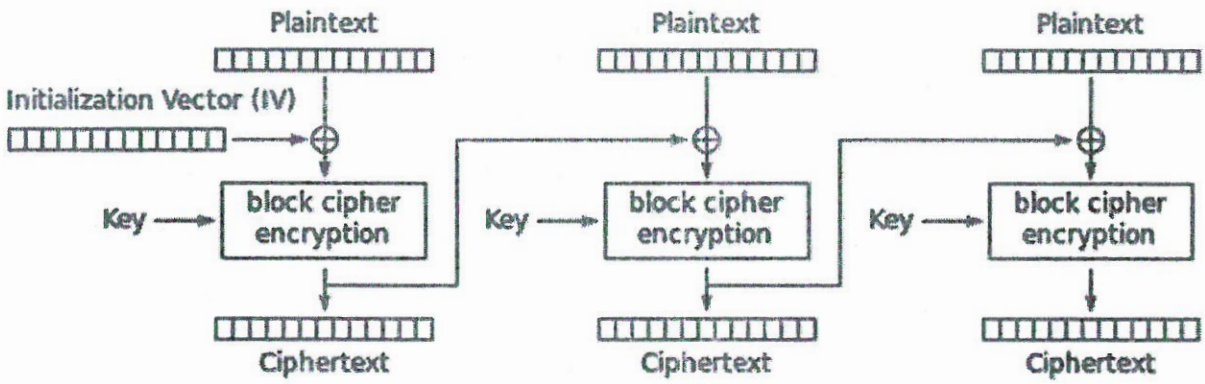
A number of proposals have been made for hash functions based on using a cipher block chaining technique, but without using the secret key. One of the first such proposals was that of Rabin . Divide a message M into fixed-size blocks $M1$, $M2$, ----- M_n and use a symmetric encryption system such as DES to compute the hash code G as

H_0 = initial value

$H_i = E(M_i, H_{i-1})$

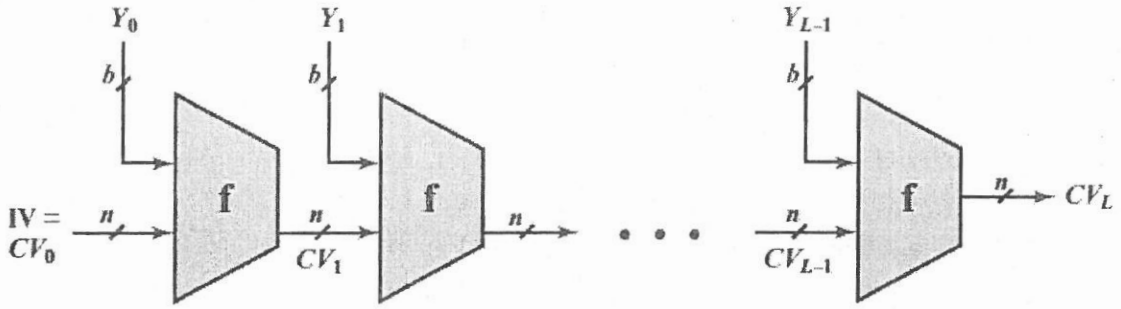
$G = H_n$

This is similar to the CBC technique, but in this case, there is no secret key. As with any hash code, this scheme is subject to the birthday attack, and if the encryption algorithm is DES and only a 64-bit hash code is produced, then the system is vulnerable.



This is similar to the CBC technique, but in this case, there is no secret key. The hash function takes an input message and partitions it into L fixed-sized blocks of b bits each. If necessary, the final block is padded to b bits. The final block also includes the value of the total length of the input to the hash function. The inclusion of the length makes the job of the

opponent more difficult. Either the opponent must find two messages of equal length that hash to the same value or two messages of differing lengths that, together with their length values, hash to the same value.



IV = Initial value
CV_i = Chaining variable
Y_i = ith input block
f = Compression algorithm
L = Number of input blocks
n = Length of hash code
b = Length of input block

9.(a). Apply the Elliptic Curve Digital Signature Algorithm.----------5M

Ans:

Elliptic Curve Digital Signature Algorithm

In 2009, version of FIPS 186 includes a new digital signature technique based on elliptic curve cryptography, known as the **Elliptic Curve Digital Signature Algorithm (ECDSA)**. ECDSA is enjoying increasing acceptance due to the efficiency advantage of elliptic curve cryptography, which yields security comparable to that of other schemes with a smaller key bit length.

Four elements are involved.

1. All those participating in the digital signature scheme use the same global domain parameters, which define an elliptic curve and a point of origin on the curve.
2. A signer must first generate a public, private key pair.
3. A hash value is generated for the message to be signed. The signature consists of two integers, r and s.
4. To verify the signature, the verifier uses as input the signer's public key, the domain parameters, and the integer s. The output is a value v that is compared to r. The signature is verified if $v = r$.

Key Generation

1. Select a random integer d, $d \in [1, n - 1]$
2. Compute $Q = dG$. This is a point in $Eq(a, b)$
3. Bob's public key is Q and private key is d.

Digital Signature Generation and Authentication

1. Select a random or pseudorandom integer k, $k \in [1, n - 1]$
2. Compute point $P = (x, y) = kG$ and $r = x \bmod n$. If $r = 0$ then goto step 1
3. Compute $t = k\text{-}1 \bmod n$
4. Compute $e = H(m)$, where H is one of the SHA-2 or SHA-3 hash functions.

5. Compute $s = k\text{-}1(e + dr) \bmod n$. If $s = O$ then goto step 1
6. The signature of message m is the pair (r, s).

Alice knows the public domain parameters and Bob's public key. Alice is presented with Bob's message and digital signature and verifies the signature using the following steps:

1. Verify that r and s are integers in the range 1 through n - 1
2. Using SHA, compute the 160-bit hash value $e = H(m)$
3. Compute $w = s\text{-}1 \bmod n$
4. Compute $u1 = ew$ and $u2 = rw$
5. Compute the point $X = (x1, y1) = u1G + u2Q$
6. If $X = O$, reject the signature else compute $v = x1 \bmod n$
7. Accept Bob's signature if and only if $v = r$

9.(b). List attacks on digital signatures----------5M

Ans:

lists the following types of attacks, in order of increasing severity. Here 'A' denotes the user whose signature method is being attacked, and 'C' denotes the attacker.

- **Key-only attack:** C only knows A's public key.
- **Known message attack:** C is given access to a set of messages and their signatures.
- **Generic chosen message attack:** C chooses a list of messages before attempting to breaks A's signature scheme, independent of A's public key. C then obtains from A valid signatures for the chosen messages. The attack is generic, because it does not depend on A's public key; the same attack is used against everyone.
- **Directed chosen message attack:** Similar to the generic attack, except that the list of messages to be signed is chosen after C knows A's public key but before any signatures are seen.
- **Adaptive chosen message attack:** C is allowed to use A as an "oracle." This means that C may request from A signatures of messages that depend on previously obtained message-signature pairs.

UNIT-V

10.(a). Explain IP Security policy and Security Association Database.----------3M

Ans:

IP SECURITY POLICY:

Fundamental to the operation of IPsec is the concept of a security policy applied to each IP packet that transits from a source to a destination. IPsec policy is determined primarily by the interaction of two databases, the **security association database (SAD)** and the **security policy database (SPD)**.

Security Association Database:

In each IPSec implementation, there is a nominal Security Association Database that defines the parameters associated with each SA. A security association is normally defined by the following parameters:

• **Sequence Number Counter:** A 32-bit value used to generate the Sequence Number field in AH or ESP headers .

• **Sequence Counter Overflow:** A flag indicating whether overflow of the Sequence Number Counter should generate an auditable event and prevent further transmission of packets on this SA (required for all implementations).

• **Anti-Replay Window:** Used to determine whether an inbound AH or ESP packet is a replay

• **AH Information:** Authentication algorithm, keys, key lifetimes, and related parameters being used with AH (required for AH implementations).

• **ESP Information:** Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP (required for ESP implementations).

• **Lifetime of This Security Association:** A time interval or byte count after which an SA must be replaced with a new SA (and new SPI) or terminated, plus an indication of which of these actions should occur (required for all implementations).

• **IPSec Protocol Mode:** Tunnel, transport, or wildcard (required for all implementations). These modes are discussed later in this section.

• **Path MTU:** Any observed path maximum transmission unit (maximum size of a packet that can be transmitted without fragmentation) and aging variables (required for all implementations).

Transport and Tunnel Modes :

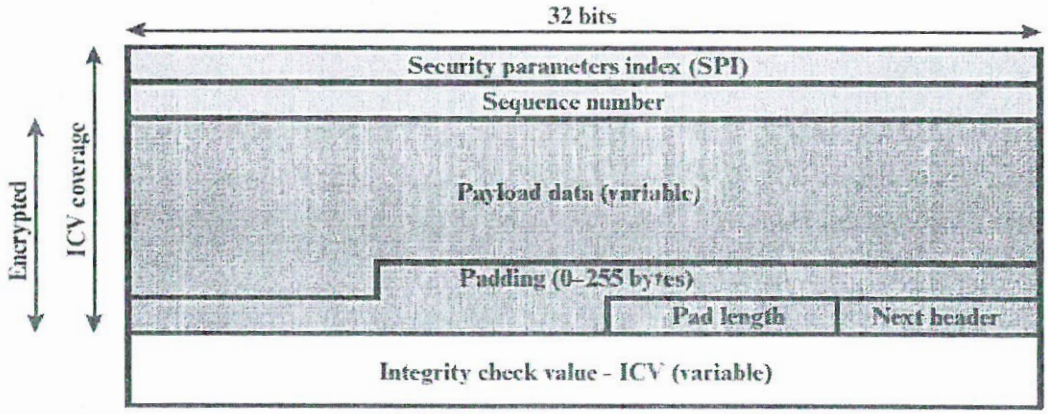
Both AH and ESP support two modes of use: transport and tunnel mode.

10.(b). Analyze the ESP packet format used in IPsec ----------7M

Ans:

ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality. The set of services provided depends on options selected at the time of Security Association (SA) establishment and on the location of the implementation in a network topology.

ESP Format :



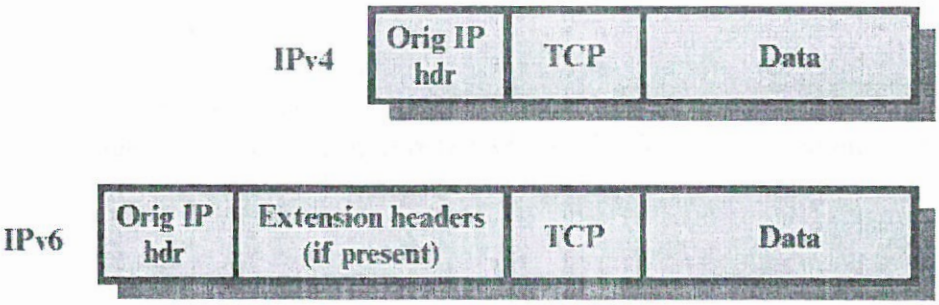
(a) Top-level format of an ESP Packet

The following figure shows the format of an ESP packet. It contains the following fields:

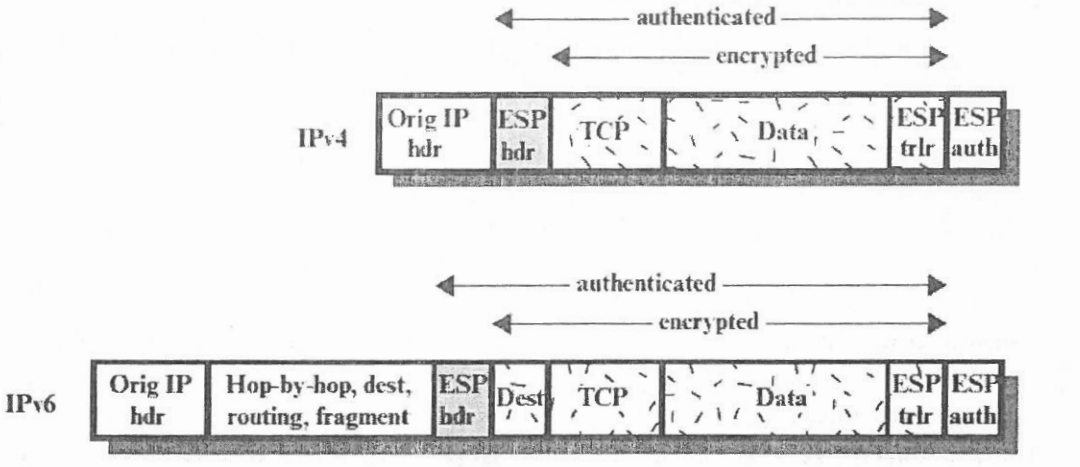
- **Security Parameters Index** (32 bits): Identifies a security association.
- **Sequence Number** (32 bits): A monotonically increasing counter value; this provides an anti-replay function, as discussed for AH.
- **Payload Data (variable):** This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
- **Padding (0-255 bytes):** This field is used to make the length of the plaintext to be a multiple of some desired number of bytes. It is also added to provide confidentiality.
- **Pad Length (8 bits):** Indicates the number of pad bytes immediately preceding this field.
- **Next Header (8 bits):** Identifies the type of data contained in the payload data field by identifying the first header in that payload (for example, an extension header in IPv6, or an upper-layer protocol such as TCP).
- **Authentication Data (variable):** A variable-length field (must be an integral number of 32-bit words) that contains the Integrity Check Value computed over the ESP packet minus the Authentication Data field.

Transport and Tunnel Modes:

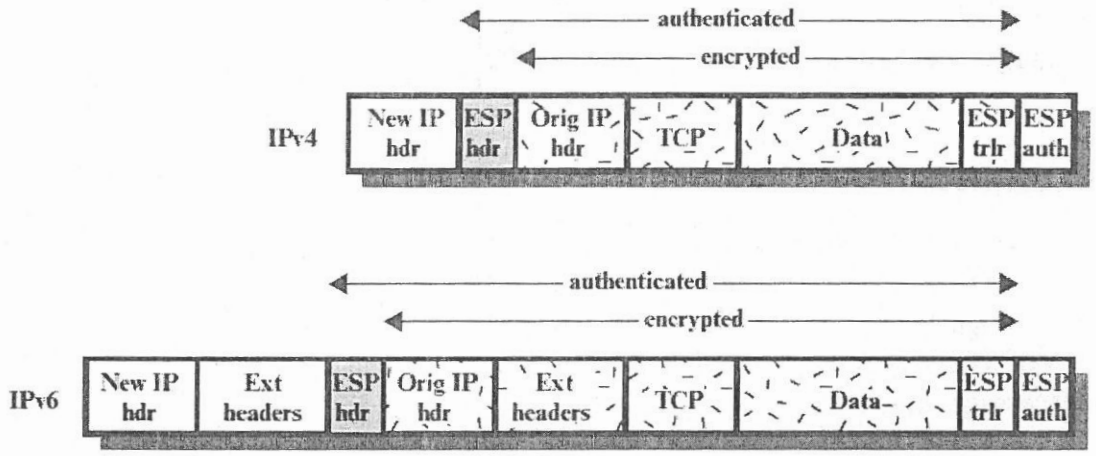
Adding encryption makes ESP a bit more complicated because the encapsulation *surrounds* the payload rather than *precedes* it as with AH: ESP includes header and trailer.



(a) Before Applying ESP



(b) Transport Mode



(c) Tunnel Mode

11.(a). Explain email threats and comprehensive email security. ----------3M

Ans:

email security threats can be classified as follows:

- **Authenticity-related threats:** Could result in unauthorized access to an enterprise's email system.
- **Integrity-related threats:** Could result in unauthorized modification of email content.
- **Confidentiality-related threats:** Could result in unauthorized disclosure of sensitive information.
- **Availability-related threats:** Could prevent end users from being able to send or receive email.

A variety of standardized protocols as a means for countering these threats. These include:

- **STARTTLS:** An SMTP security extension that provides authentication, integrity, non-repudiation (via digital signatures) and confidentiality (via encryption)for the entire SMTP message by running SMTP over TLS.
- **S/MIME:** Provides authentication, integrity, non-repudiation (via digital signatures) and confidentiality (via encryption) of the message body carried in SMTP messages.

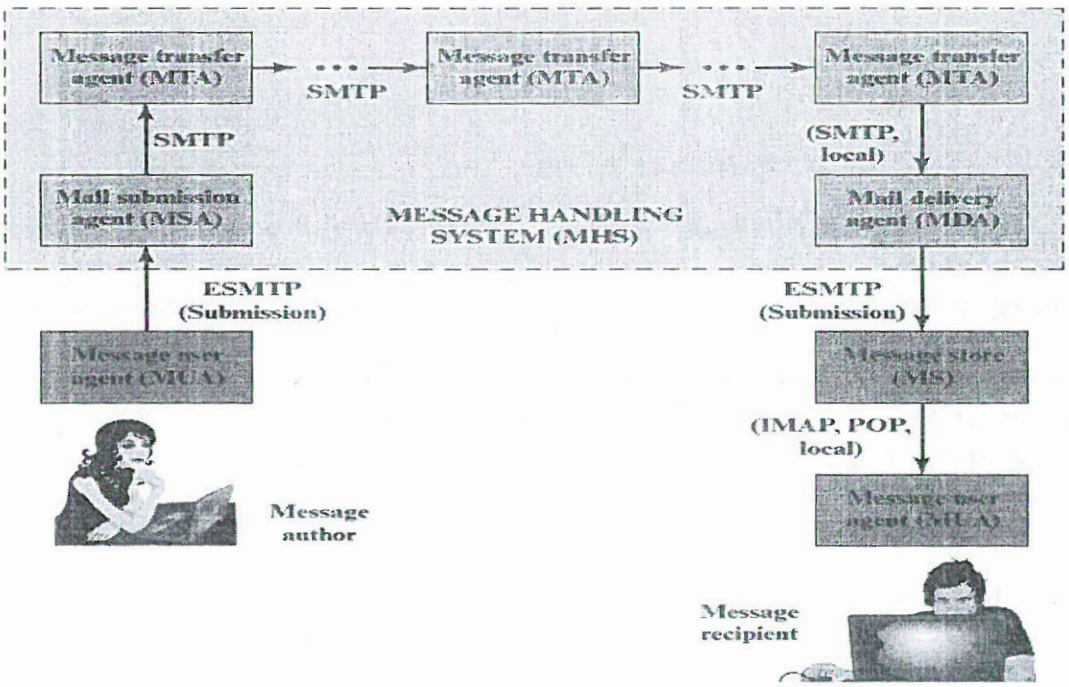
- **DNS Security Extensions (DNSSEC):** Provides authentication and integrity protection of DNS data, and is an underlying tool used by various email security protocols.
- **DNS-based Authentication of Named Entities (DANE):** Is designed to overcome problems in the certificate authority (CA) system by providing an alternative channel for authenticating public keys based on DNSSEC.
- **Sender Policy Framework (SPF):** Uses the Domain Name System (DNS) to allow domain owners to create records that associate the domain name with a specific IP address range of authorized message senders.
- **DomainKeys Identified Mail (DKIM):** Enables an MTA to sign selected headers and the body of a message. This validates the source domain of the mail and provides message body integrity.
- **Domain-based Message Authentication, Reporting, and Conformance(DMARC):** Lets senders know the proportionate effectiveness of their SPF and DKIM policies, and signals to receivers what action should be taken in various individual and bulk attack scenarios.

11.(b). Analyze the Internet mail architecture and email components.----------7M

Ans:

Email Components:

- Message User Agent (MUA)
- Mail Submission Agent (MSA)
- Message Transfer Agent (MTA)
- Mail Delivery Agent (MDA)
- Message Store (MS)



Message User Agent (MUA): Operates on behalf of user actors and user applications. It is their representative within the email service.

Mail Submission Agent (MSA): Accepts the message submitted by an MUA and enforces the policies of the hosting domain and the requirements of Internet standards.

Message Transfer Agent (MTA): Relays mail for one application-level hop. It is like a packet switch or IP router in that its job is to make routing assessments and to move the message closer to the recipients.

Mail Delivery Agent (MDA): Responsible for transferring the message fromthe MHS to the MS.

Message Store (MS): An MUA can employ a long-term MS. An MS can be located on a remote server or on the same machine as the MUA. Typically, an MUA retrieves messages from a remote server using POP (Post Office Protocol) or IMAP (Internet Message Access Protocol).

Email Protocols:

Two types of protocols are used for transferring email.

- The first type is used to move messages through the Internet from source to destination. The protocol used for this purpose is SMTP.
- The second type consists of protocols used to transfer messages between mail servers, of which IMAP and POP are the most commonly used.

57

20
9600
6000
1200