PVP 20

Code: 20AM3601, 20DS3601

III B.Tech - II Semester – Regular Examinations - APRIL 2025

CRYPTOGRAPHY AND NETWORK SECURITY

(Common for AIML & DS)

Duration: 3 hours Max. Marks: 70

Note: 1. This paper contains questions from 5 units of Syllabus. Each unit carries 14 marks and have an internal choice of Questions.
2. All parts of Question must be answered in one place.

BL – Blooms Level CO – Course Outcome

			BL	CO	Max. Marks
		UNIT-I			
1	Write short notes on				
	a)	Security attacks with appropriate diagrams.	L2	CO1	7 M
	b)	Security services .	L2	CO1	7 M
		OR			
2	a)	Write the requirements of Cryptography.	L2	CO1	7 M
	b)	Discuss model for network security.	L2	CO1	7 M
		UNIT-II			
3	a)	Illustrate any three substitution ciphers with examples.	L3	CO2	7 M
	b)	Mention the strengths and weakness of DES algorithm.	L2	CO1	7 M
		OR			
4	Analyze the general structure of DES algorithm.		L4	CO4	14 M

		UNIT-III			
5	a)	Illustrate RSA algorithm for encryption and decryption process with an example.	L3	CO2	7 M
	b)	Explain about Elliptic Curve Cryptography (ECC).	L2	CO1	7 M
		OR			
6		Analyze the ElGamal cryptographic system with an example.	L4	CO4	14 M
		UNIT-IV			
7	a)	Explain different approaches of NIST Digital Signature Algorithm with relevant diagrams.	L2	CO1	7 M
	b)	Summarize the properties of Hash Function.	L2	CO1	7 M
		OR			
8	a)	Identify the security services provided by digital signature.	L2	CO1	7 M
	b)	Analyze the process involved in message digest generation and processing of single block in SHA-512.	L4	CO4	7 M
		UNIT-V			
9	a)	Explain briefly about PGP.	L2	CO1	7 M
	b)	What is S/MIME? Explain its operational description in email security.	L2	CO1	7 M
		OR			

10	a)	Analyze the Internet Mail Architecture and its components.	L4	CO4	7 M
	b)	Explain about IP security overview.	L2	CO1	7 M

PVP20

Code No:20AM3601,20DS3601

III B. Tech – II Semester-Regular Examinations-APRIL2025
CRYPTOGRAPHY & NETWORK SECURITY
(Common to AIML, DS)

Duration: 3 Hours **Max. Marks: 70**

Note:

1. This question paper contains questions from 5 units of Syllabus. Each Unit carries 14 Marks and have an internal choice of Questions.
2. All parts of Question paper must be answered in one place.

5 x 14 = 70 Marks

Qno	Question	Marks Awarded	Total Marks
	UNIT - I		
1(a)	**Write a short note on Security Attacks with appropriate diagrams**	**L2**	**CO1**
	Passive attacks with diagrams	2M	7 M
	Active attacks with diagrams	5M	
1(b)	**Write a short note on Security Services**	**L2**	**CO1**
	Any Five Security Services	7M	7 M
	OR		
2(a)	**Write the requirements of Cryptography**	**L2**	**CO1**
	Any five requirements of Cryptography	7M	
2b)	**Discuss model for Network Security**	**L2**	**CO1**
	Model For Network Security Diagram	2M	7 M
	Discussion on components of Model	5M	
	UNIT -II		
3(a)	**Illustrate any three Substitution Ciphers with Examples**	**L3**	**CO2**
3(a)	Any three Substitution Cipher techniques with examples (a) Caesar Cipher (b) Monoalphabetic Cipher (c) Polyalphabetic Cipher(d) Playfair Cipher (e) Onetime Pad	7M	7 M
3(b)	**Mention the strength and weakness of DES Algorithm**	**L2**	**CO1**
	Any three Strengths	5M	7 M
	Any two Weaknesses	2M	
	OR		
4	**Analyze the general structure of DES Algorithm**	**L4**	**CO4**
	Introduction to DES	2M	14 M
	Overview of DES with a neat sketch	5 M	
	General Description of DES Algorithm with Steps	7 M	
	UNIT - III		
5(a)	**Illustrate RSA Algorithm for Encryption and Decryption Process with an Example**	**L3**	**CO2**

	Introduction & Overview of RSA	3M	7 M
	Encryption Process in RSA	1M	
	Decryption Process in RSA	1M	
	RSA Example	2 M	
5(b)	**Explain about Elliptic Curve Cryptography**	**L2**	**CO1**
	Introduction & Oveview of ECC	3 M	7 M
	Generation of Public Keys	2M	
	Calculation of Secret Keys	2M	
	OR		
6	**Analyze Elgamal Cryptosystem with an Example**	**L4**	**CO4**
	Introduction & Overview, Global Public Elements	4 M	14 M
	Key Generation Process	4 M	
	Encryption and Decryption Process	3 M	
	Example	3 M	
	UNIT - IV		
7(a)	**Explain different approaches of NIST Digital Signature Algorithm with relevant diagrams**	**L2**	**CO1**
	Overview of Digital Signature Algorithm	1M	7 M
	DSA Approach with diagram	3 M	
	RSA Approach with diagram	3M	
7(b)	**Summarize the properties of Hash Functions**	**L2**	**CO1**
	Introduction to Hash functions	2M	7 M
	Any three properties with explanation	5 M	
	OR		
8(a)	**Identify the Security Services provided by Digital Signatures**	**L2**	**CO1**
	Introduction to Digital Signatures	2M	7 M
	Any three services with explanation	5 M	
8(b)	**Analyze the Process involved in message digest generation and processing of single block of SHA-512**	**L4**	**CO4**
	Introduction to SHA-512 Algorithm	2M	7M
	Analyzation of Five Steps in SHA-512	5M	
	UNIT - V		
9(a)	Explain briefly about PGP	**L2**	**CO1**
	PGP Introduction	2 M	7 M
	Key Certification and Key Distribution	5M	
9(b)	**What S/MIME? Explain its operational Description in email Security**	**L2**	**CO1**
	S/MIME- Introduction & Overview	2M	7 M
	Operational Description – Services	5M	
	OR		
10(a)	**Analyze the Internet Mail Architecture and its components**	**L2**	**CO1**
	Internet E Mail Architecture- Introduction	2M	7 M
	Analysis of functioning of various components	5M	
10(b)	**Explain about IP Security Overview**	**L2**	**CO1**
	IP Security Introduction	2M	7 M
	Applications, Benefits, IPSec Documents, Services	5M	

PVP20

Code No:20AM3601,20DS3601

III B. Tech – II Semester-Regular Examinations-APRIL 2025
CRYPTOGRAPHY & NETWORK SECURITY
(Common to AIML, DS)

Duration: 3 Hours **Max. Marks: 70**

Note:

1. This question paper contains questions from 5 units of Syllabus. Each Unit carries 14 Marks and have an internal choice of Questions.
2. All parts of Question paper must be answered in one place.

5 x 14 = 70 Marks

UNIT-I

1. Write a Short notes on
   (a) Security Attacks with appropriate diagrams **7M**

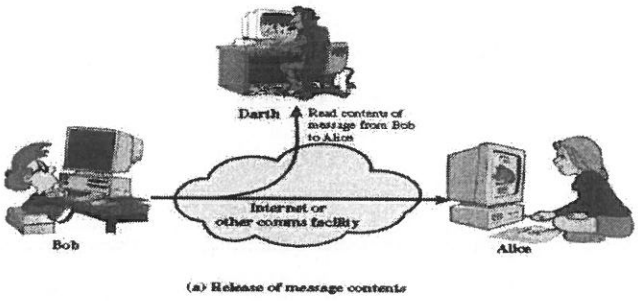
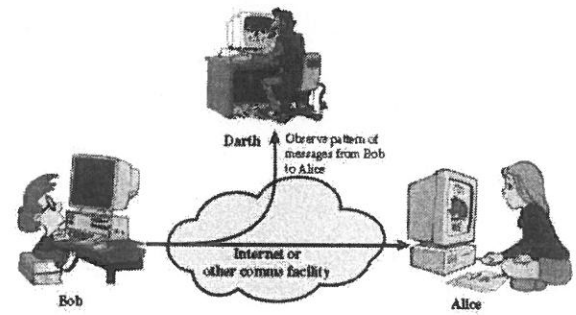
   Note: Passive Attacks- 2 M, Active Attacks – 5 M

(a) Security Attacks

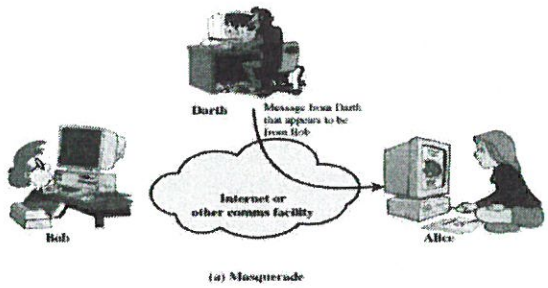
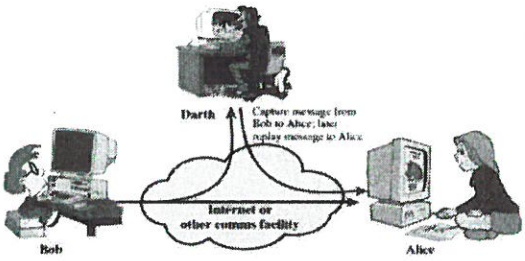
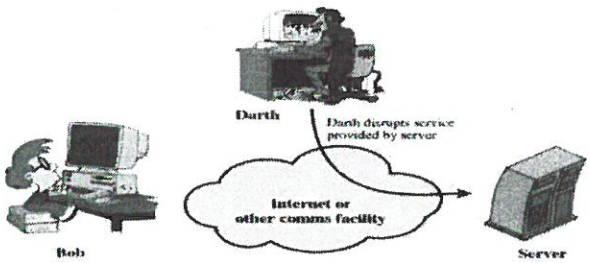
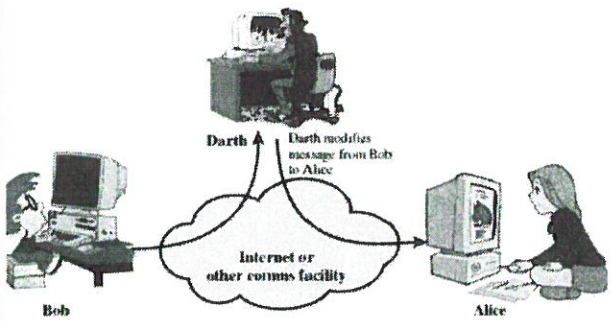
A **security attack** is any malicious attempt to compromise the confidentiality, integrity, or availability of a system or its data. Attacks can be passive (eavesdropping) or active (modifying data).

Types of Security Attacks

1. **Passive Attacks** – Attacker monitors/reads data without altering it.

RELEASE OF MESSAGE CONTENT 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. We would like to prevent an opponent from learning the contents of these transmissions	 (a) Release of message contents
TRAFFIC ANALYSIS: A second type of passive attack, traffic analysis, is subtler Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. Observing patterns in communication.	 (b) Traffic analysis

2. **Active Attacks** – Attacker modifies or disrupts data.

Masquerade (Spoofing) – Pretending to be an authorized user. A masquerade takes place when one entity pretends to be a different entity (Figure:). A masquerade attack usually includes one of the other forms of active attack	 (a) Masquerade
Replay Attack – Capturing and retransmitting data to deceive the system. **:** Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.	 (b) Replay
Denial of Service (DoS) – Overloading a system to disrupt services. The denial of service prevents or inhibits the normal use or management of communications facilities (Figure d). This attack may have a specific target; For example, an entity may suppress all messages directed to a particular destination (e.g., thesecurity audit service).	 (d) Denial of service
Modification of Messages – Altering data in transit. Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect	 (c) Modification of messages

1(b) Security Services **7M**

Note: Award full marks if the answer correctly describes any five security services

A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

i) DATA CONFIDENTIALITY: Ensures that the information in a computer system and transmitted information is accessible only for reading by authorized parties. Confidentiality is the protection of transmitted data from passive attacks. For example, when a TCP connection is set up between two systems, this broad protection prevents the release of any user data transmitted over the TCP connection.

ii) AUTHENTICATION: The authentication service is concerned with assuring that a communication. Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false

iii) DATA INTEGRITY: Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages. It means the assurance that data received are exactly as sent by an authorized entity.

iv) NON-REPUDIATION: Requires that neither the sender nor the receiver of a message be able to deny the transmission. When a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

v) ACCESS CONTROL: Requires that access to information resources may be controlled by the target system. Access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated

vi)AVAILABILITY: Requires that computer system assets be available to authorized parties when needed.

2(a) **Write the requirements of Cryptography** **7 M**

Note: Award full marks if the answer correctly describes any five Cryptography requirements

Cryptography is the science of securing data through encoding (encryption) to protect confidentiality, integrity, and authenticity. For a cryptographic system to be effective, it should meet the following core requirements:

1. Confidentiality

- Ensures that information is only accessible to those authorized to have access.
- Prevents unauthorized access or disclosure of data.
- Achieved through strong encryption algorithms (e.g., AES, RSA).

2. Integrity

- Ensures that data has not been altered or tampered with during transmission or storage.
- Detects unauthorized modifications.
- Achieved using **hash functions** (e.g., SHA-256), **digital signatures**, and **checksums**.

3. Authentication

- Verifies the identity of the sender or receiver of the information.
- Confirms that the communication is between legitimate parties.
- Techniques: **Digital certificates**, **public-key infrastructure (PKI)**, **user credentials**.

4. Non-repudiation

- Prevents denial of actions or communications by the sender.
- Ensures that once data is sent, the sender cannot later deny sending it.
- Achieved using **digital signatures** and secure audit logs.

5. Key Management

- Involves the creation, distribution, storage, rotation, and destruction of cryptographic keys.
- Strong key management ensures the overall strength of the cryptographic system.
- Uses protocols like **Diffie-Hellman** for key exchange and **PKI** for key distribution.

6. Scalability and Performance

- Cryptographic systems must support growing numbers of users, devices, or systems without degrading performance.
- Lightweight cryptography may be used for IoT and mobile devices.

7. Compliance with Standards

- Cryptographic techniques must adhere to industry standards (e.g., NIST, ISO/IEC 27001) to ensure interoperability and trust.

2(b) Discuss model for Network Security **7M**

Note: Description – 2M, Identification of Components- 2M, Diagram- 3M

Cryptography and Network Security – Unit I

A model for Network security

A model for much of what we will be discussing is captured, in very general terms, in Figure 1.3. A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

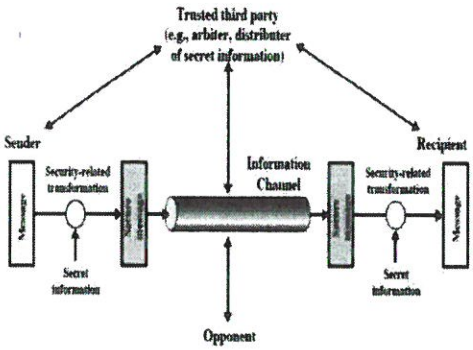


Figure 1.3. Model for Network Security

UNIT -II

3(a) Illustrate any three Substitution Ciphers with Examples **7M**

Note: Award full marks if the answer explains any three substitution ciphers with relevant examples.

A substitution cipher is a method of encryption where each letter or symbol in the plaintext is replaced with another according to a fixed system or key.

Types of Substitution Ciphers

1. Caesar Cipher: Shifts each letter by a fixed number of places in the alphabet.

- Example (shift by 3):
- Plaintext: HELLO
  Ciphertext: KHOOR

2. **Monoalphabetic Cipher**: Uses a fixed substitution alphabet, where each letter in the plaintext is always replaced by the same letter in the ciphertext. More secure than Caesar, but still vulnerable to frequency analysis.

- Example:

Plaintext: A B C D E F G H I ...
Ciphertext: Q W E R T Y U I O ...

3. **Polyalphabetic Cipher:** Uses multiple substitution alphabets to make the encryption more complex.

- Example: Vigenère Cipher
  - Uses a keyword to shift letters differently across the message.
  - More resistant to frequency analysis than monoalphabetic.

4. **Playfair Cipher**: Encrypts pairs of letters (digraphs) instead of single letters.Uses a 5x5 grid of letters (usually with I = J).

5.**One-Time Pad** : The one-time pad is one of the simplest yet most secure encryption methods available, as long as it's used correctly. Here's a quick overview:

How the One-Time Pad Works:

1. **Key Generation**: A random key is generated that is as long as the message.
2. **Encryption**: Each character of the plaintext is combined with the corresponding character of the key using modular arithmetic (typically modulo 26 for letters).

Example:

- Plaintext: HELLO
- Key: XMCKL *(random and same length)*
- Encryption (letter shift):
- H (7) + X (23) = 30 → 4 → E
  E (4) + M (12) = 16 → Q
  L (11) + C (2) = 13 → N
  L (11) + K (10) = 21 → V
  O (14) + L (11) = 25 → Z

3(b). Mention the strength and weakness of DES Algorithm

Note: Award 5 marks for any three valid strengths and 2 marks for one or two valid weaknesses.

It was adopted in 1977 by the National Bureau of Standards (NBS), now National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB46). This was the best algorithm proposed and was adopted in 1977 as Data Encryption Standard.

Strengths and weaknesses of DES

(a)The Use of 56-bit keys
(b) The Nature of DES Algorithm

(c) Timing Attacks

(a) The Use of 56-bit Keys

Strengths:

1. **Keyspace for Its Time:**

With 2562^{56}256 possible keys (~7.2×10167.2 \times 10^{16}7.2×1016), brute-force attacks were impractical with the computing power available in the 1970s.DES was considered secure for the duration of its initial expected lifespan.

2. **Balanced Design:**

The 56-bit key length was a trade-off between performance and security, making it practical for the hardware of its era.

Weaknesses:

Modern Brute-Force Feasibility:

Advances in computing made brute-force attacks feasible. Modern systems, especially distributed networks or specialized hardware (e.g., FPGA or ASIC), can test 2562^{56}256 keys in hours or minutes.

In 1998, the **EFF DES Cracker** successfully brute-forced a DES key in 56 hours, and similar tasks are even faster today.

Inadequacy for Long-Term Security:

A 56-bit key is insufficient against modern attackers, who expect at least 128-bit key lengths for secure encryption.

(b) The Nature of the DES Algorithm

Strengths:

1. **Block Cipher Security Principles:**

DES is a Feistel-based block cipher, leveraging substitution (S-boxes) and permutation for confusion and diffusion, which are critical to secure encryption.

2. **16 Rounds of Processing:**

Each round contributes to cryptographic strength by further diffusing the input and obscuring relationships between the plaintext, ciphertext, and key.

3. **Avalanche Effect:**

A small change in plaintext or key results in significant changes in ciphertext, making DES resistant to simple analysis.

Weaknesses:

1. **Small Block Size:**

DES operates on 64-bit blocks, which can lead to patterns in ciphertext when encrypting large amounts of data (known as the **block collision problem**).

Modern ciphers like AES use 128-bit blocks to address this issue.

2. **Fixed S-Boxes:**

Although robust during its creation, the fixed S-boxes are susceptible to modern cryptanalysis methods as they do not adapt to evolving threats.

3. **Limited Key Schedule Complexity:**

Weak and semi-weak keys can lead to vulnerabilities under certain conditions, reducing overall security.

4. **(b) Analyze the general structure of DES Algorithm** **14 M**

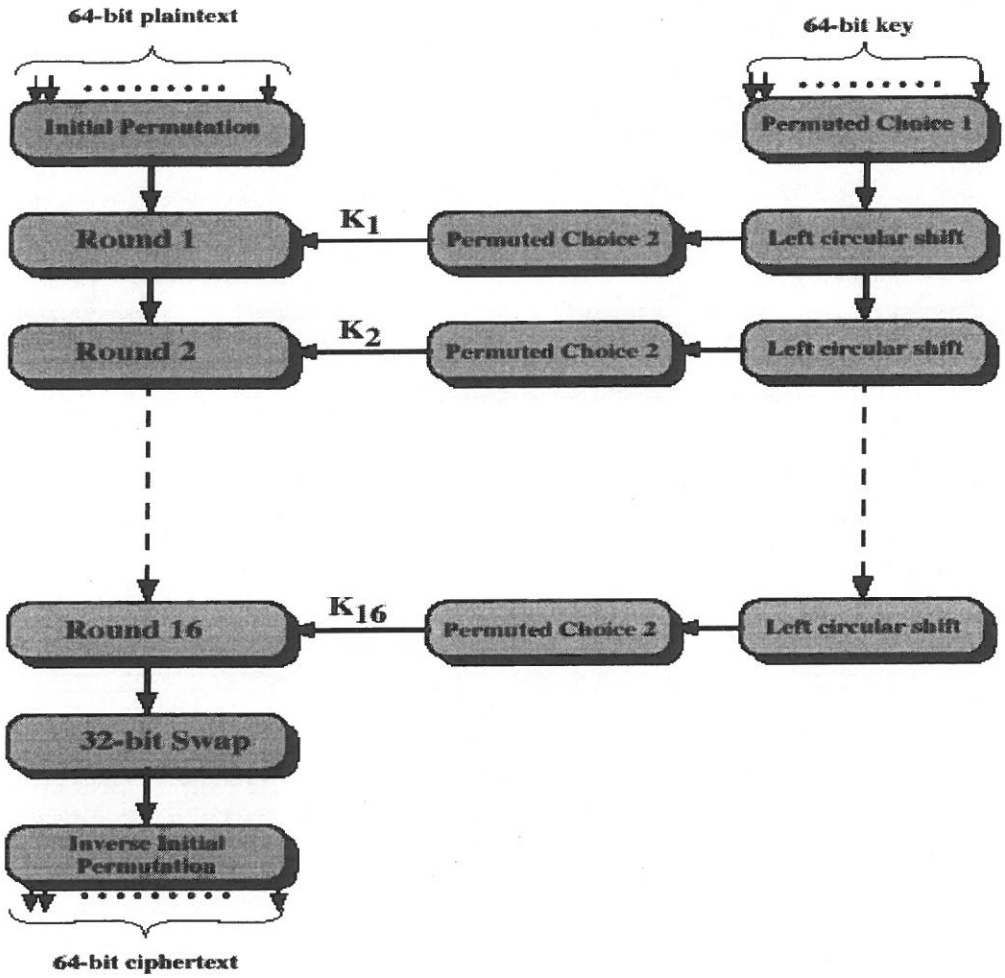
Note: Introduction to DES-2M,
Overview of DES with a neat Sketch- 5M
General Description of DES with steps – 7M

I. The Data Encryption Standard

It was adopted in 1977 by the National Bureau of Standards (NBS), now National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB46). This was the best algorithm proposed and was adopted in 1977 as Data Encryption Standard.

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

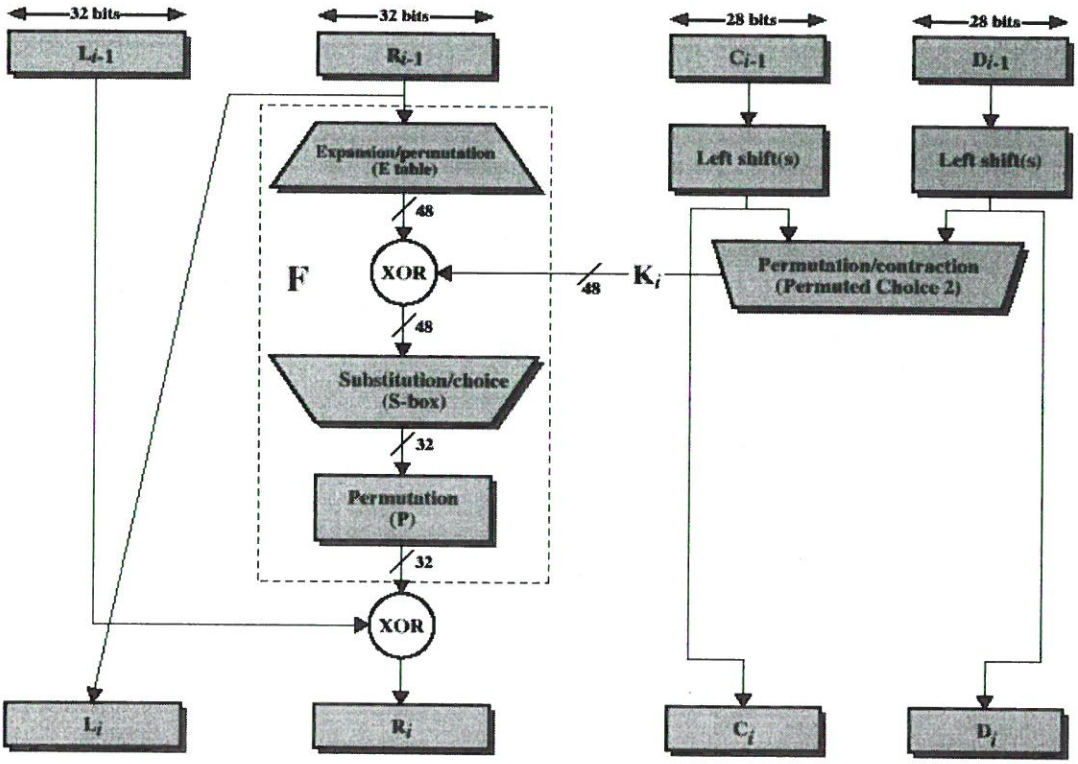
DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).



General Depiction of DES Encryption Algorithm

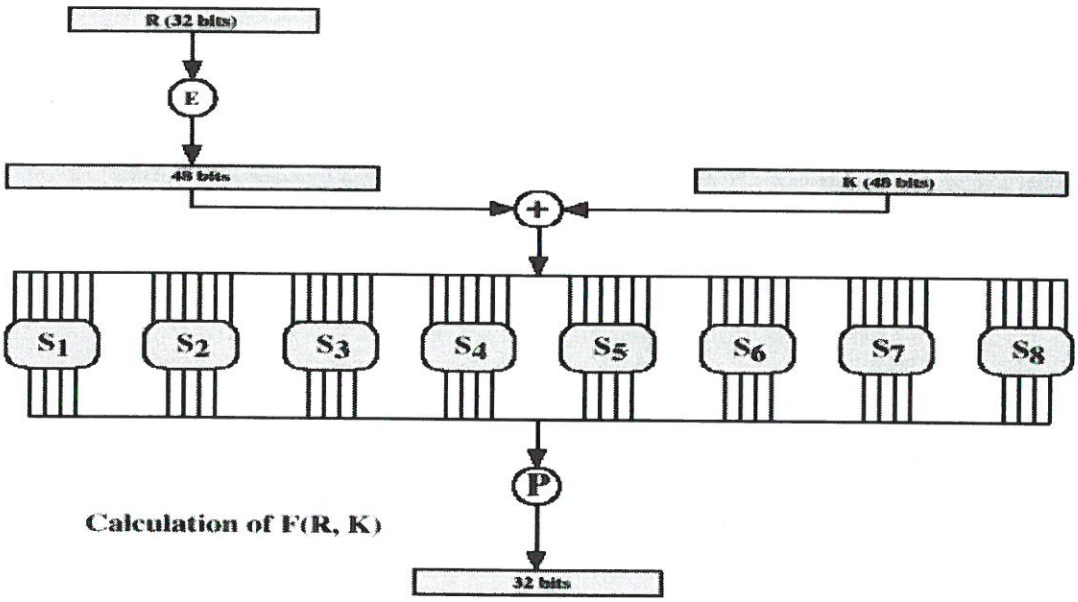
The 64 bit input enters into initial permutation and the permutated output is fed into sixteen rounds with kay values and then 32-bit swap swaps left and 32-bit halves obtained after Round 16, we get preoutput. Finally, preoutput passes through a permutation IP-1, that is inverse to initial permutation IP, to produce the 64-bit ciphertext. The right-hand portion of Fig. 3.7 shows the way in which 56-bit is used. For each of 16 rounds a subkey Ki is produced by the combination of a left circular shift and a permutation. The permutation function is the same for each round.

DETAILS OF SINGLE ROUND(Optional Diagram for Student)



Single Round of DES Algorithm

The r



Calculation of F(R, K)

Input key has 64 bits. But each 8th bit is not used: bits 8,16,24,32,40,48,56,64 are not further used. The 56-bit key is used. The resulting 56-bit key is then treated as 2 28-bit quantities, labeled C0 and D0. At each round, C i-1 and Di-1 are separately subjected to a circular left shift, or rotation, of 1 or 2 bits as governed by the following:

Schedule of Left Shifts															
Round number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

UNIT -III

5(a) Illustrate RSA Algorithm for Encryption and Decryption Process with an Example 7M

Note: Algorithm with Key Generation, Encryption and Decryption Process- 5M, Any example-2M

RSA is the most common public-key algorithm, named after its inventors **Rivest, Shamir, and Adelman (RSA).**

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:	$M = C^d \bmod n$

Figure 9.5 The 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 mod f(n)=1, i.e. d*7 mod 160=1. 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 $M = 88$.

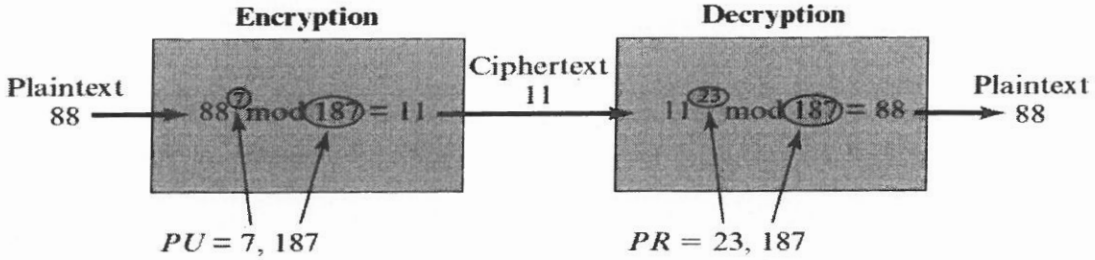


Figure 9.6 Example of RSA Algorithm

5(b) **Explain about Elliptic Curve Cryptography** **7M**

Note: Introduction to ECC- 3 M, Generation of Public Keys- 2M, Generation of Secret keys- 2M

Elliptic Curve Cryptography (ECC)

Definition: Elliptic Curve Cryptography (ECC) is a type of **public-key cryptography** based on the algebraic structure of **elliptic curves over finite fields**. It provides strong security with relatively **smaller key sizes** compared to traditional algorithms like RSA.

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
$K = n_B \times P_A$

Figure 10.7 ECC Diffie–Hellman Key Exchange

(6) **Analyze Elgamal Cryptosystem with an Example** **14 M**

Note: Introduction & Overview, Selection of Global Public Elements- 4M
Key Generation Process-4 M
Encryption & Decryption Process-3 M
Any relevant example – 3 M

In 1984, T. Elgamal announced a public-key scheme based on discrete logarithms, closely related to the Diffie–Hellman technique [ELGA84, ELGA85]. The Elgamal2 cryptosystem is used in some form in a number of standards including the digital signature standard (DSS), and the S/MIME email standard.

Global Public Elements	
q	prime number
α	$\alpha < q$ and α a primitive root of q

Key Generation by Alice	
Select private X_A	$X_A < q - 1$
Calculate Y_A	$Y_A = \alpha^{X_A} \bmod q$
Public key	$\{q, \alpha, Y_A\}$
Private key	X_A

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < q$
Select random integer k	$k < q$
Calculate K	$K = (Y_A)^k \bmod q$
Calculate C_1	$C_1 = \alpha^k \bmod q$
Calculate C_2	$C_2 = KM \bmod q$
Ciphertext:	(C_1, C_2)

Decryption by Alice with Alice's Private Key	
Ciphertext:	(C_1, C_2)
Calculate K	$K = (C_1)^{X_A} \bmod q$
Plaintext:	$M = (C_2 K^{-1}) \bmod q$

Figure 10.3 The Elgamal Cryptosystem

Example with Numbers:

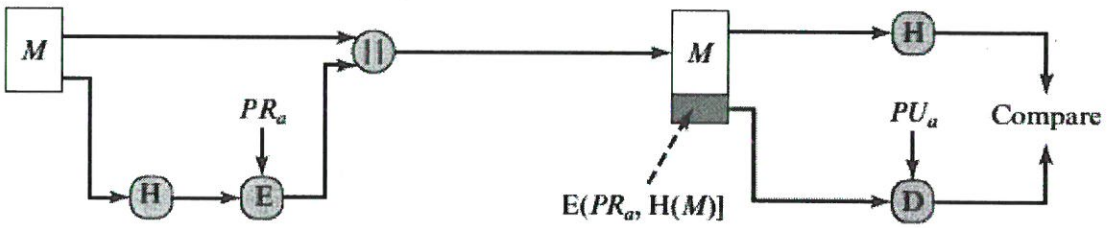
1. Alice chooses:
   - $p = 17$, $g = 3$, $x = 15$.
   - Public Key $h = 3^{15} \mod 17 = 6$.
2. Bob wants to encrypt $M = 10$:
   - $y = 13$, $C_1 = 3^{13} \mod 17 = 12$.
   - $C_2 = 10 \cdot 6^{13} \mod 17 = 10 \cdot 5 = 50 \mod 17 = 16$.
   - Bob sends $(C_1, C_2) = (12, 16)$.
3. Alice decrypts:
   - $s = C_1^x \mod 17 = 12^{15} \mod 17 = 5$.
   - $M = C_2 \cdot s^{-1} \mod 17 = 16 \cdot 7 \mod 17 = 112 \mod 17 = 10$.
   - Original message $M = 10$ is recovered!

UNIT -IV

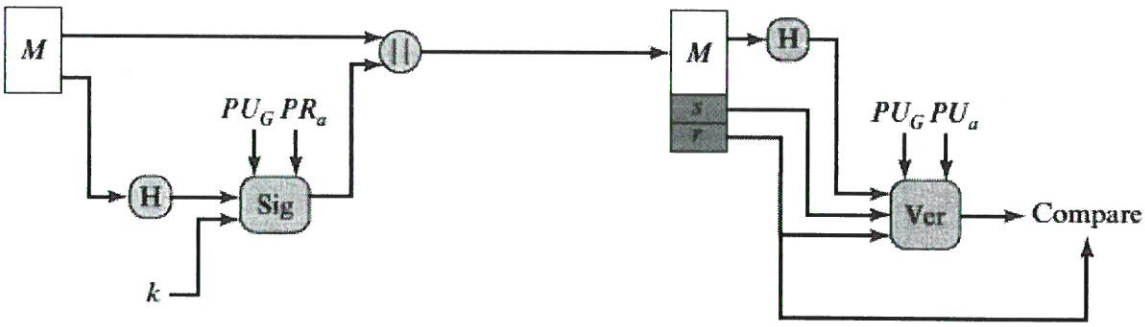
7(a) **Explain different approaches of NIST Digital Signature Algorithm with relevant diagrams** **7M**

Note: Overview of DSA- 01 M, DSA Approach- 3M, RSA Approach – 3M

The National Institute of Standards and Technology (NIST) has published Federal Information Processing Standard FIPS 186, known as the Digital Signature Algorithm (DSA). The DSA makes use of the Secure Hash Algorithm (SHA) described in Chapter 12. The DSA was originally proposed in 1991 and revised in 1993 in response to public feedback concerning the security of the scheme. There was a further minor revision in 1996. In 2000, an expanded version of the standard was issued as FIPS 186-2, subsequently updated to FIPS 186-3 in 2009, and FIPS 186-4 in 2013. This latest version also incorporates digital signature algorithms based on RSA and on elliptic curve cryptography. In this section, we discuss DSA.



(a) RSA approach



(b) DSA approach

Figure 13.2 Two Approaches to Digital Signatures

7(b) **Summarize the properties of Hash Functions** **7M**

Note: Introduction to Hash functions – 2M, Any three Properties with explanation – 5 M

Hash functions are essential in cryptography and data integrity verification. They convert input data into a fixed-size string of characters, often referred to as a "hash value" or "digest." Here are the main properties of hash functions:

1. **Deterministic**: The same input always produces the same hash output, ensuring consistency.
2. **Fixed-Length Output**: Regardless of input size, the hash function generates an output of a fixed size (e.g., 256 bits for SHA-256).
3. **Efficiency**: Hash functions should compute quickly for any input.
4. **Pre-image Resistance**: Given a hash value, it should be computationally infeasible to reverse-engineer the original input.
5. **Collision Resistance**: Two different inputs should not produce the same hash output. Preventing collisions is critical for security.

6. **Avalanche Effect**: A small change in the input should result in a vastly different hash output, enhancing unpredictability.
7. **Second Pre-image Resistance**: It should be challenging to find a different input that produces the same hash as a given input.

8(a) **Identify the Security Services provided by Digital Signatures 7M**

Note: Introduction to Digital Signatures – 2M, Any three services with explanation – 5M

A **Digital signature** is a cryptographic technique that ensures the authenticity, integrity, and non-repudiation of a message or document. It uses asymmetric encryption, where the sender signs the data with their **private key**, and the recipient verifies it using the sender's **public key**. Digital signatures prevent tampering and impersonation, making them crucial for secure transactions, software distribution, and legal agreements. Common algorithms include **RSA, DSA, and ECDSA**. Digital signatures provide several vital security services that ensure the authenticity, integrity, and non-repudiation of electronic communications and data. Here's an outline of these services:

1. **Authentication**: Verifies the identity of the sender. A digital signature ensures that the message originates from the claimed sender.
2. **Data Integrity**: Ensures that the data or message has not been altered during transmission. If the data is modified, the signature verification fails.
3. **Non-repudiation**: Prevents the sender from denying their involvement. Once a document or message is signed, the sender cannot claim they did not send it.
4. **Confidentiality (When Combined with Encryption)**: Although not inherent to digital signatures alone, they can be used alongside encryption to provide confidentiality.

8(b) **Analyze the Process involved in message digest generation and processing of single block of SHA-512 7M**

Note: Introduction to SHA- 512- 2M, Analyzation of Five Steps in SHA-512 – 5M

SHA (Secure Hash Algorithm) was developed by the National Institute of Standards and Technology (NIST) and published as a federal information processing standard (FIPS 180) in 1993. **SHA-512** is a cryptographic hash function from the **SHA-2 family**, producing a **512-bit (64-byte) hash value**. It processes input data in **1024-bit blocks** using a series of logical operations (AND, OR, XOR, shifts) and ensures **collision resistance** and **preimage resistance**. Commonly used in **digital signatures, password hashing, and blockchain**, it provides stronger security than older algorithms like **MD5 or SHA-1**.

SHA-512 Logic

The algorithm takes as input a message with a maximum length of less than 2^{128} bits and produces as output a 512- bit message digest. The input is processed in 1024-bit blocks. Figure 11.9 depicts the overall processing of a message to produce a digest.

Step 1 Append padding bits. The message is padded so that its length is congruent to 896 modulo 1024 [length K 896(mod 1024)]. Padding is always added, even if the message is already of the desired length. Thus, the number of padding bits is in the range of 1 to 1024. The padding consists of a single 1 bit followed by the necessary number of 0 bits.

Step 2 Append length. A block of 128 bits is appended to the message. This block is treated as an unsigned 128-bit integer (most significant byte first) and contains the length of the original message in bits (before the padding). The outcome of the first two steps yields a message that is an integer

multiple of 1024 bits in length. In Figure 11.9, the expanded message is represented as the sequence of 1024-bit blocks *M*1, *M*2, c, *MN*, so that the total length of the expanded message is *N* * 1024 bits.
Step 3 Initialize hash buffer. A 512-bit buffer is used to hold intermediate and final results of the hash function. The buffer can be represented as eight 64-bit registers (a, b, c, d, e, f, g, h). These registers are initialized to the following 64-bit integers (hexadecimal values):

a = 6A09E667F3BCC908
b = BB67AE8584CAA73B
c = 3C6EF372FE94F82B
d = A54FF53A5F1D36F1
e = 510E527FADE682D1
f = 9B05688C2B3E6C1F
g = 1F83D9ABFB41BD6B
h = 5BE0CD19137E2179

These values are stored in **big-endian** format, which is the most significant byte of a word in the low-address (leftmost) byte position. These words were obtained by taking the first sixty-four bits of the fractional parts of the square roots of the first eight prime numbers.

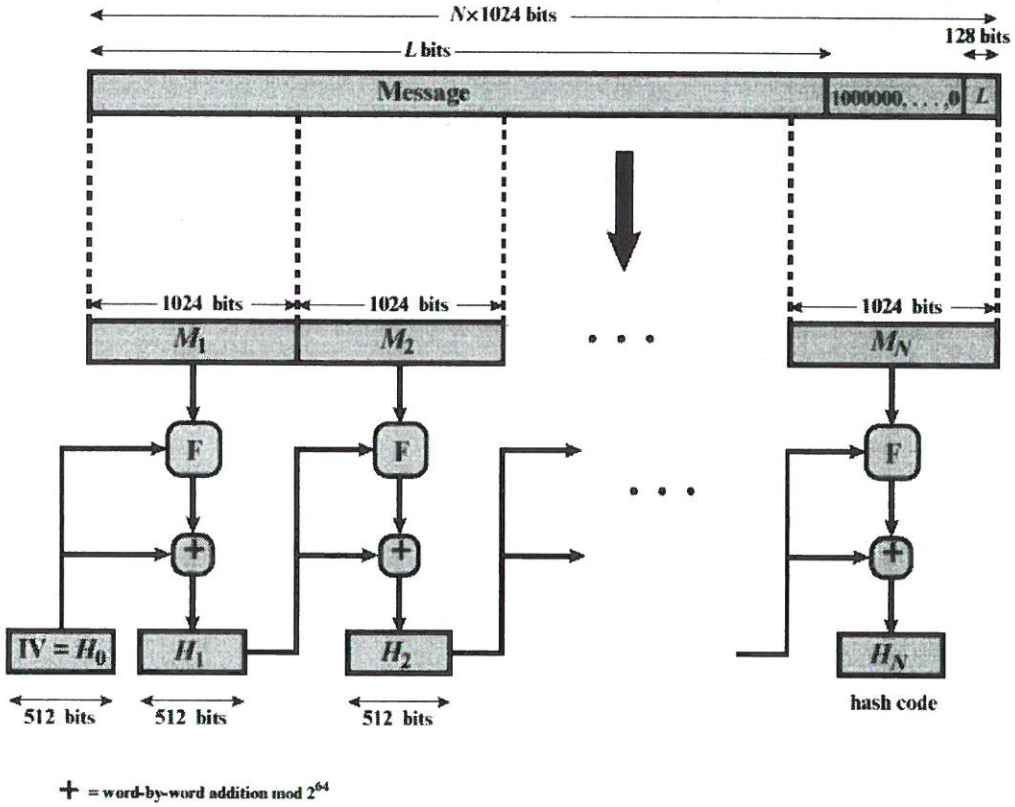


Figure 11.9 Message Digest Generation Using SHA-512

Step 4 Process message in 1024-bit (128-byte) blocks. The heart of the algorithm is a module that consists of 80 rounds; this module is labeled F in Figure 11.9. The logic is illustrated in Figure 11.10.**(Diagram Optional to Student)**

Each round takes as input the 512-bit buffer value, abcdefgh, and updates the contents of the buffer. At input to the first round, the buffer has the value of the intermediate hash value, *Hi*-1. Each round *t* makes use of a 64-bit value *Wt*, derived from the current 1024-bit block being processed (*Mi*). These values are derived using a message schedule described subsequently. Each round also makes use of an additive constant *Kt*, where 0 ... *t* ... 79 indicates one of the 80 rounds. These words represent the first 64 bits of the fractional parts of the cube roots of the first 80 prime numbers.

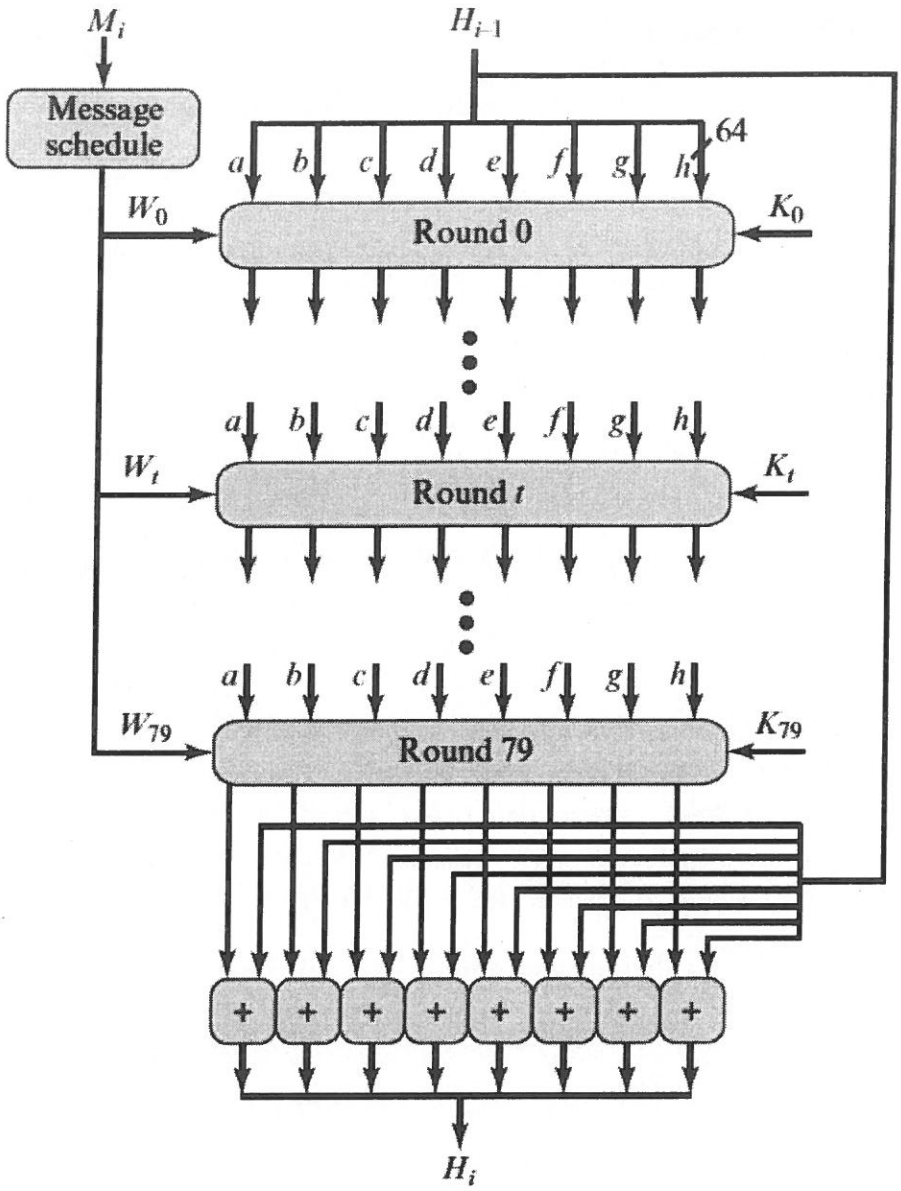


Figure 11.10 SHA-512 Processing of a Single 1024-Bit Block

The output of the eightieth round is added to the input to the first round (H_{i-1}) to produce *Hi*. The addition is done independently for each of the eight words in the buffer with each of the corresponding words in *Hi*-1, using addition modulo 2^{64}.

Step 5 Output. After all *N* 1024-bit blocks have been processed, the output from the *N*th stage is the 512-bit message digest.

We can summarize the behavior of SHA-512 as follows:

*H*0 = IV

Hi = SUM64(*Hi*-1, abcdefgh*i*)

MD = *HN*

where

IV = initial value of the abcdefgh buffer, defined in step 3

abcdefgh*i* = the output of the last round of processing of the *i*th message block

N = the number of blocks in the message (including padding and length fields)

SUM64 = addition modulo 264 performed separately on each word of the pair of inputs

MD = final message digest value

UNIT V

9(a) **Explain briefly about PGP** **7M**

Note: PGP Introduction- 2M, Key certification and Key Distribution – 5M

An alternative email security protocol is Pretty Good Privacy (PGP), which has essentially the same functionality as S/MIME. PGP was created by Phil Zimmerman and implemented as a product first released in 1991. It was made available free of charge and became quite popular for personal use. There are two significant differences between S/MIME and OpenPGP:

- **Key Certification:** S/MIME uses X.509 certificates that are issued by Certificate Authorities (or local agencies that have been delegated authority by a CA to issue certificates). In OpenPGP, users generate their own OpenPGP public and private keys and then solicit signatures for their public keys from individuals or organizations to which they are known.

- **Key Distribution:** OpenPGP does not include the sender's public key with each message, so it is necessary for recipients of OpenPGP messages to separately obtain the sender's public key in order to verify the message. Many organizations post OpenPGP keys on TLS-protected websites: People who wish to verify digital signatures or send these organizations encrypted mail need to manually download these keys and add them to their OpenPGP clients. Keys may also be registered with the OpenPGP public key servers, which are servers that maintain a database of PGP public keys organized by email address. Anyone may post a public key to the OpenPGP key servers, and that public key may contain any email address. There is no vetting of OpenPGP keys, so users must use the Web-of-Trust to decide whether to trust a given public key.

9(b). What S/MIME? Explain its operational Description in email Security 7M

Note: Introduction to S/MIME-2M, Operational Description-Services-5M

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. S/MIME is a complex capability that is defined in a number of documents. The most important documents relevant to S/MIME include the following:

Operational Description:S/MIME provides for four message-related services: authentication, confidentiality, compression, and email compatibility (Table 19.4)

Table 19.4 **Summary of S/MIME Services**

Function	Typical Algorithm	Typical Action
Digital signature	RSA/SHA-256	A hash code of a message is created using SHA-256. This message digest is encrypted using SHA-256 with the sender's private key and included with the message.
Message encryption	AES-128 with CBC	A message is encrypted using AES-128 with CBC with a one-time session key generated by the sender. The session key is encrypted using RSA with the recipient's public key and included with the message.
Compression	unspecified	A message may be compressed for storage or transmission.
Email compatibility	Radix-64 conversion	To provide transparency for email applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.

10(a). **Analyze the Internet Mail Architecture and its components** **7M**

Note: Internet E Mail Architecture- 2M, Analysis of functional components- 5M

Internet mail architecture, which is currently defined in RFC 5598 (*Internet Mail Architecture*, July 2009). This section provides an overview of the basic concepts.

(a) E Mail Components:

Internet mail architecture consists of a **user world** in the form of Message User Agents (MUA), and the **transfer world**, in the form of the **Message Handling Service (MHS)**, which is composed of Message Transfer Agents (MTA). The MHS accepts a message from one user and delivers it to one or more other users, creating a virtual MUA-to-MUA exchange environment. This architecture involves **three types of interoperability**. One is **directly between users**: messages must be formatted by the MUA on behalf of the message author so that the message can be displayed to the message recipient by the destination MUA. There are also **interoperability requirements between the MUA and the MHS**— first when a message is posted from an MUA to the MHS and later when it is delivered from the MHS to the destination MUA. Interoperability is required among the MTA components along the transfer path through the MHS.

- **Message User Agent (MUA):** Operates on behalf of user actors and user applications. It is their representative within the email service. Typically, this function is housed in the user's computer and is referred to as a client email program or a local network email server. The author MUA formats a message and performs initial submission into the MHS via a MSA. The recipient MUA processes received mail for storage and/or display to the recipient user.
- **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. This function may be located together with the MUA or as a separate functional model. In the latter case, the Simple Mail Transfer Protocol (SMTP) is used between the MUA and the MSA.
- **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. Relaying is performed by a sequence of MTAs until the message reaches a destination MDA. An MTA also adds trace information to the message header. SMTP is used between MTAs and between an MTA and an MSA or MDA.
- **Mail Delivery Agent (MDA):** Responsible for transferring the message from the 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).

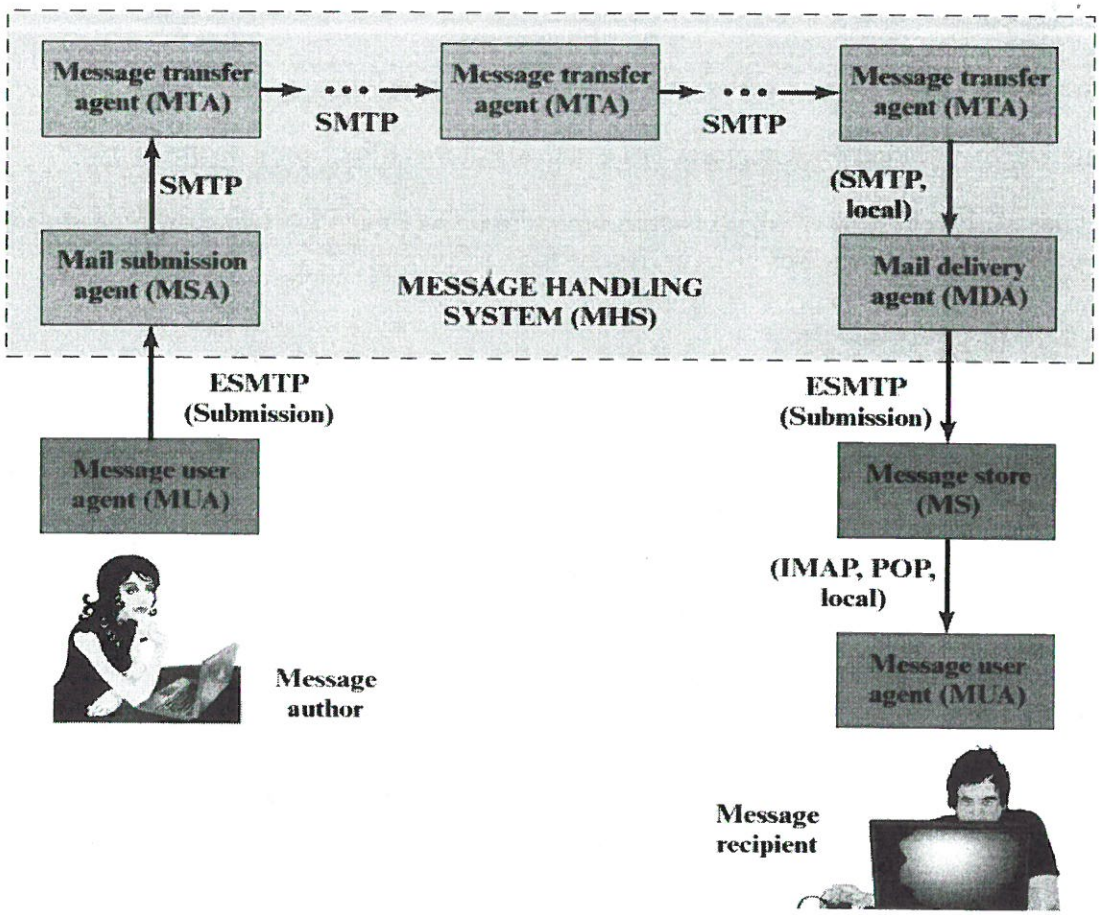


Figure 19.1 Function Modules and Standardized Protocols Used between them in the Internet Mail Architecture

10(b) **Explain about IP Security Overview 7M**

Note: Introduction to IP Sec- 2 M, Applications, Benefits, Documents, Services-5M

In 1994, the Internet Architecture Board (IAB) issued a report titled "Security in the Internet Architecture" (RFC 1636). The report identified key areas for security mechanisms. Among these were the need to secure the network infrastructure from unauthorized monitoring and control of network traffic and the need to secure end user- to-end-user traffic using authentication and encryption mechanisms.

(a) Applications of IPsec

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.
- ■ Establishing extranet and intranet connectivity with partners:
- ■ Enhancing electronic commerce security:

(b) Benefits of IPsec

- IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.
- IPsec is below the transport layer (TCP, UDP) and so is transparent to applications.
- IPsec can be transparent to end users.
- IPsec can provide security for individual users if needed.

(c) Routing Applications

In addition to supporting end users and protecting premises systems and networks, IPsec can play a vital role in the routing architecture required for internetworking. [HUIT98] lists the following examples of the use of IPsec. IPsec can assure that

- A router advertisement (a new router advertises its presence) comes from an authorized router.
- A neighbor advertisement (a router seeks to establish or maintain a neighbor relationship with a router in another routing domain) comes from an authorized router.
- A redirect message comes from the router to which the initial IP packet was sent.
- A routing update is not forged. Without such security measures, an opponent can disrupt communications or divert some traffic. Routing protocols such as Open Shortest Path First (OSPF) should be run on top of security associations between routers that are defined by IPsec.

(d) IPsec Documents

IPsec encompasses three functional areas: **authentication, confidentiality, and key management**. The documents can be categorized into the following groups.

- Architecture:
- Authentication Header (AH):
- Encapsulating Security Payload (ESP):
- Internet Key Exchange (IKE):
- Cryptographic algorithms:

(e) IPsec Services

IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services.

Two protocols are used to provide security: **an authentication protocol designated by the header of the protocol, Authentication Header (AH);** and a combined encryption/authentication protocol designated by the format of the packet for that protocol, **Encapsulating Security Payload (ESP).** RFC 4301 lists the following services:

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets (a form of partial sequence integrity)
- Confidentiality (encryption)
- Limited traffic flow confidentiality