



Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

Re-Examination Synoptic

July 2019

Max. Marks: 60

Class: B.E.

Course Code: CPC702

Name of the Course: Cryptography and System Security

Duration: 3 hr

Semester: **0VII**

Branch: Computer

Instructions:

- (1) All Questions are Compulsory
- (2) Draw neat diagrams
- (3) Assume suitable data if necessary

Q. No.		Max. Mks
Q1.a	<p>The rules to convert Plain-text to Cipher-text in Play fair Cipher Technique:</p> <ul style="list-style-type: none"> Plaintext is encrypted two letters at a time. If a pair is a repeated letter, insert filler like 'X'. If both letters fall in the same row, replace each with the letter to its right (circularly). If both letters fall in the same column, replace each with the the letter below it (circularly). Otherwise, each letter is replaced by the letter in the same row but in the column of the other letter of the pair. <p>Marks Distribution:</p> <p>The rules to convert Plain-text to Cipher-text in Play fair Cipher Technique----- 03mks</p> <p>Problem solved correctly----- 03mks</p>	06
Q1.b	<p>Three key objectives that are at the heart of computer security are:</p> <ol style="list-style-type: none"> Confidentiality Availability Integrity <p>Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.</p> <p>Integrity: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A</p> <div data-bbox="1159 1959 1638 2390" data-label="Diagram"> </div> <p>Figure 1.1 The Security Requirements Triad</p>	05



Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

	<p>loss of integrity is the unauthorized modification or destruction of information.</p> <p>Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.</p> <p>Marks Distribution:</p> <p>Explained all three goals properly with diagram----- 06mks</p> <p>Explained all three goals properly without diagram----- 04mks</p>																							
Q2.a	<p>Marks Distribution:</p> <p>Explained RSA Key Generation Algorithm-----02mks</p> <p>Explained RSA Encryption Algorithm-----02mks</p> <p>Explained RSA Decryption Algorithm-----02mks</p> <div><div><p>Key Generation Alice</p><table><tr><td>Select p, q</td><td>p and q both prime, $p \neq q$</td></tr><tr><td>Calculate $n = p \times q$</td><td></td></tr><tr><td>Calculate $\phi(n) = (p - 1)(q - 1)$</td><td></td></tr><tr><td>Select integer e</td><td>$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$</td></tr><tr><td>Calculate d</td><td>$d \equiv e^{-1} \pmod{\phi(n)}$</td></tr><tr><td>Public key</td><td>$PU = \{e, n\}$</td></tr><tr><td>Private key</td><td>$PR = \{d, n\}$</td></tr></table></div><div><p>Encryption by Bob with Alice's Public Key</p><table><tr><td>Plaintext:</td><td>$M < n$</td></tr><tr><td>Ciphertext:</td><td>$C = M^e \pmod n$</td></tr></table></div><div><p>Decryption by Alice with Alice's Public Key</p><table><tr><td>Ciphertext:</td><td>C</td></tr><tr><td>Plaintext:</td><td>$M = C^d \pmod n$</td></tr></table></div></div>	Select p, q	p and q both prime, $p \neq q$	Calculate $n = p \times q$		Calculate $\phi(n) = (p - 1)(q - 1)$		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	$PR = \{d, n\}$	Plaintext:	$M < n$	Ciphertext:	$C = M^e \pmod n$	Ciphertext:	C	Plaintext:	$M = C^d \pmod n$	06
Select p, q	p and q both prime, $p \neq q$																							
Calculate $n = p \times q$																								
Calculate $\phi(n) = (p - 1)(q - 1)$																								
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	$PR = \{d, n\}$																							
Plaintext:	$M < n$																							
Ciphertext:	$C = M^e \pmod n$																							
Ciphertext:	C																							
Plaintext:	$M = C^d \pmod n$																							

Figure 9.5 The RSA Algorithm



Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

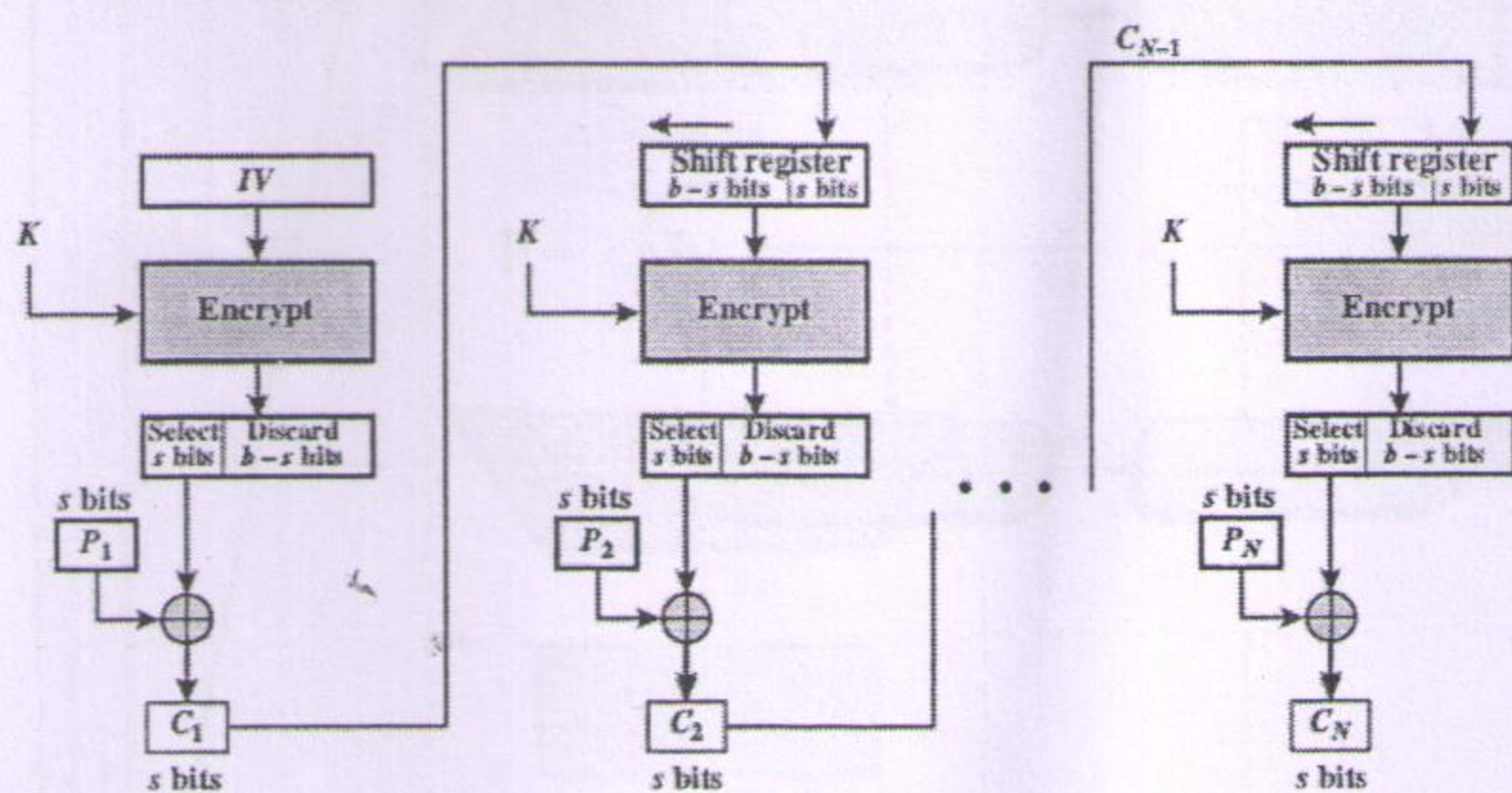
OR

Marks Distribution:

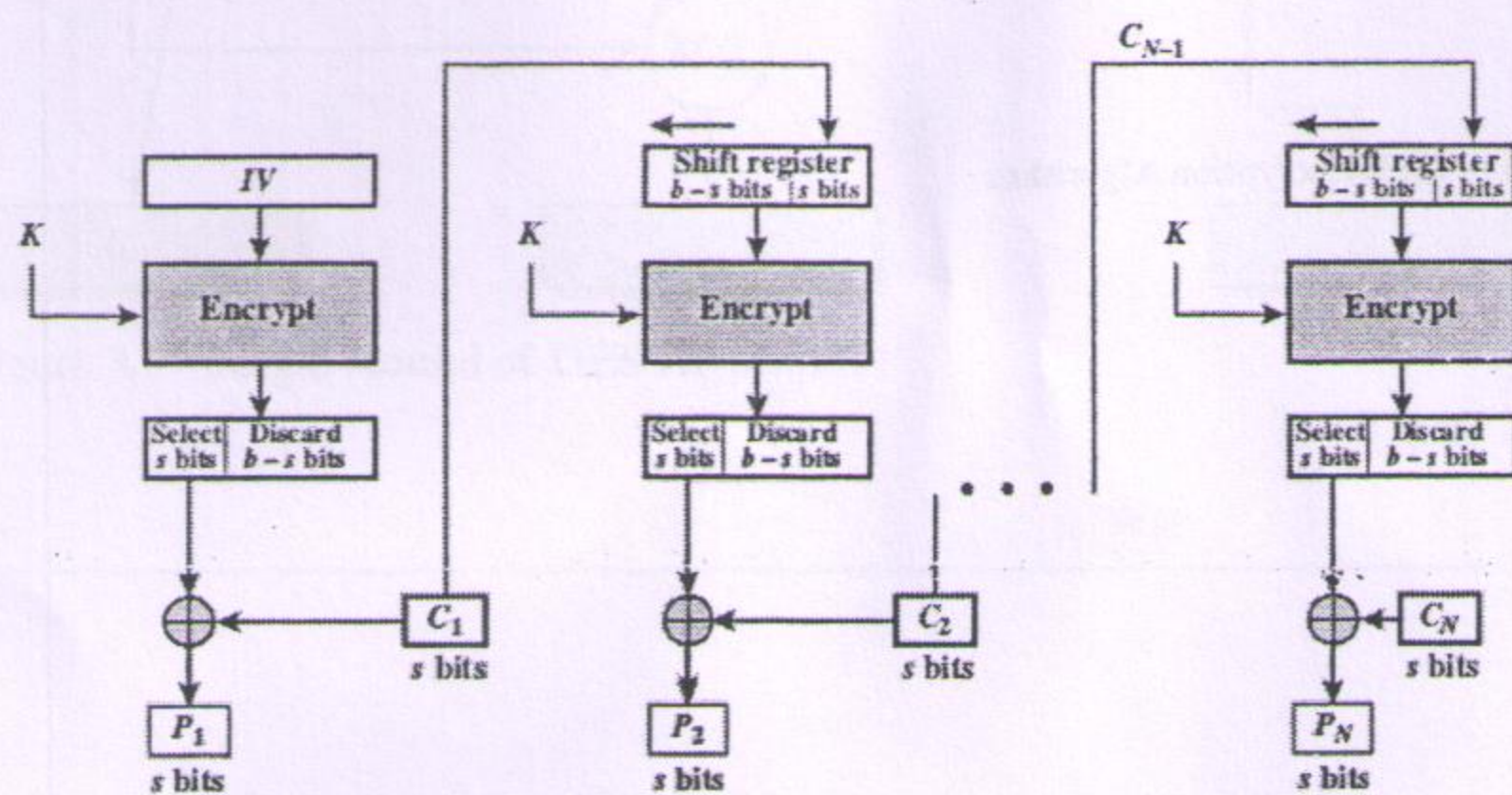
Explained properly the Cipher Feedback Mode Encryption with the help of diagrams----
03mks

Explained properly the Cipher Feedback Mode Decryption with the help of diagrams----
03mks

Cipher Feedback Mode



(a) Encryption



(b) Decryption

Marks Distribution:

Explained properly DES Encryption algorithm with diagram ----- 06 mks
Explained properly Single Round of DES Encryption algorithm with diagram --- 06 mks
Explained properly DES Encryption algorithm w/o diagram ----- 04 mks
Explained properly Single Round of DES Encryption algorithm w/o diagram --04 mks

12



Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

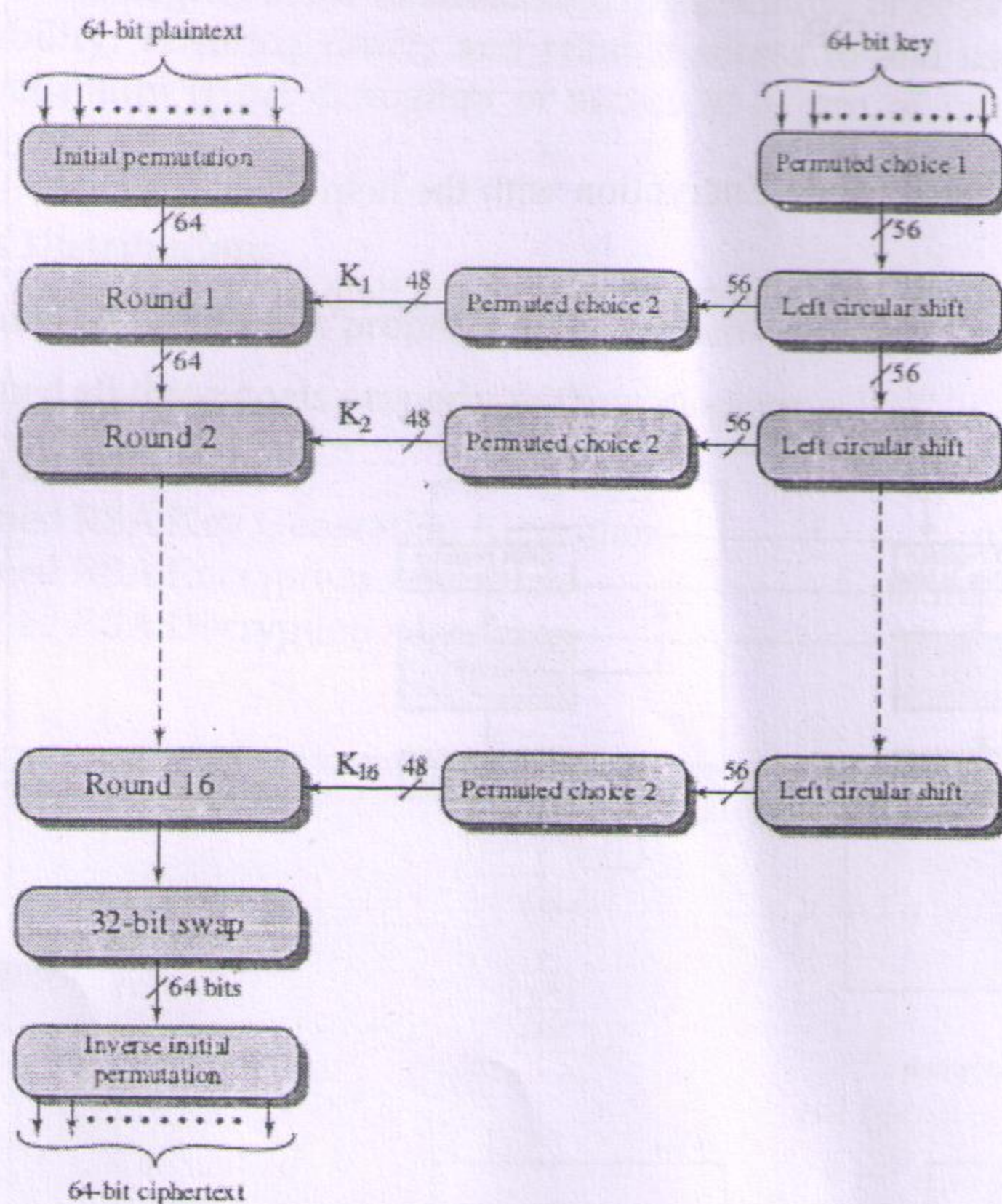
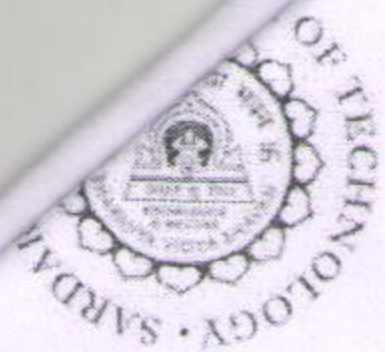


Figure 3.5 General Depiction of DES Encryption Algorithm



Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

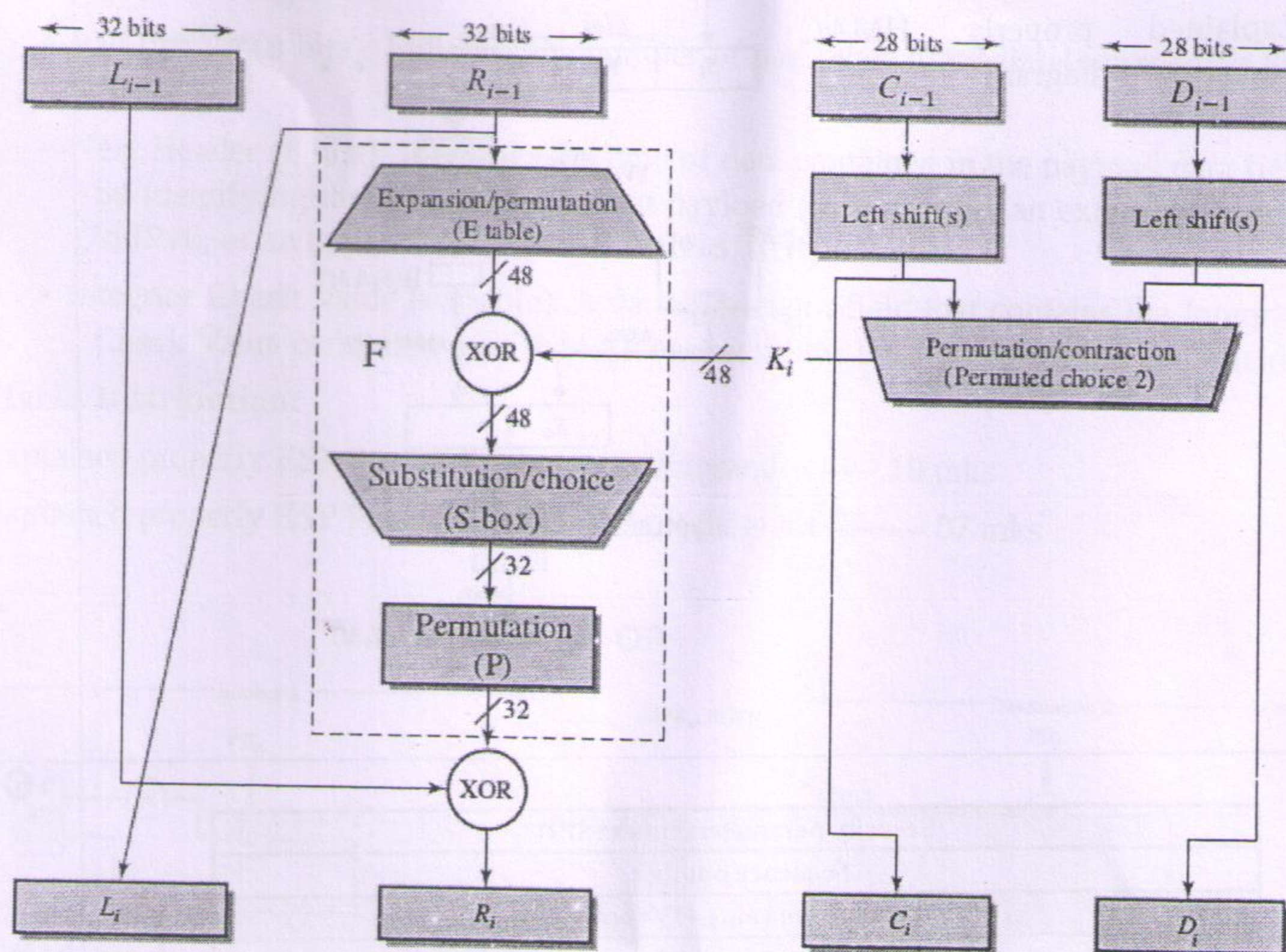
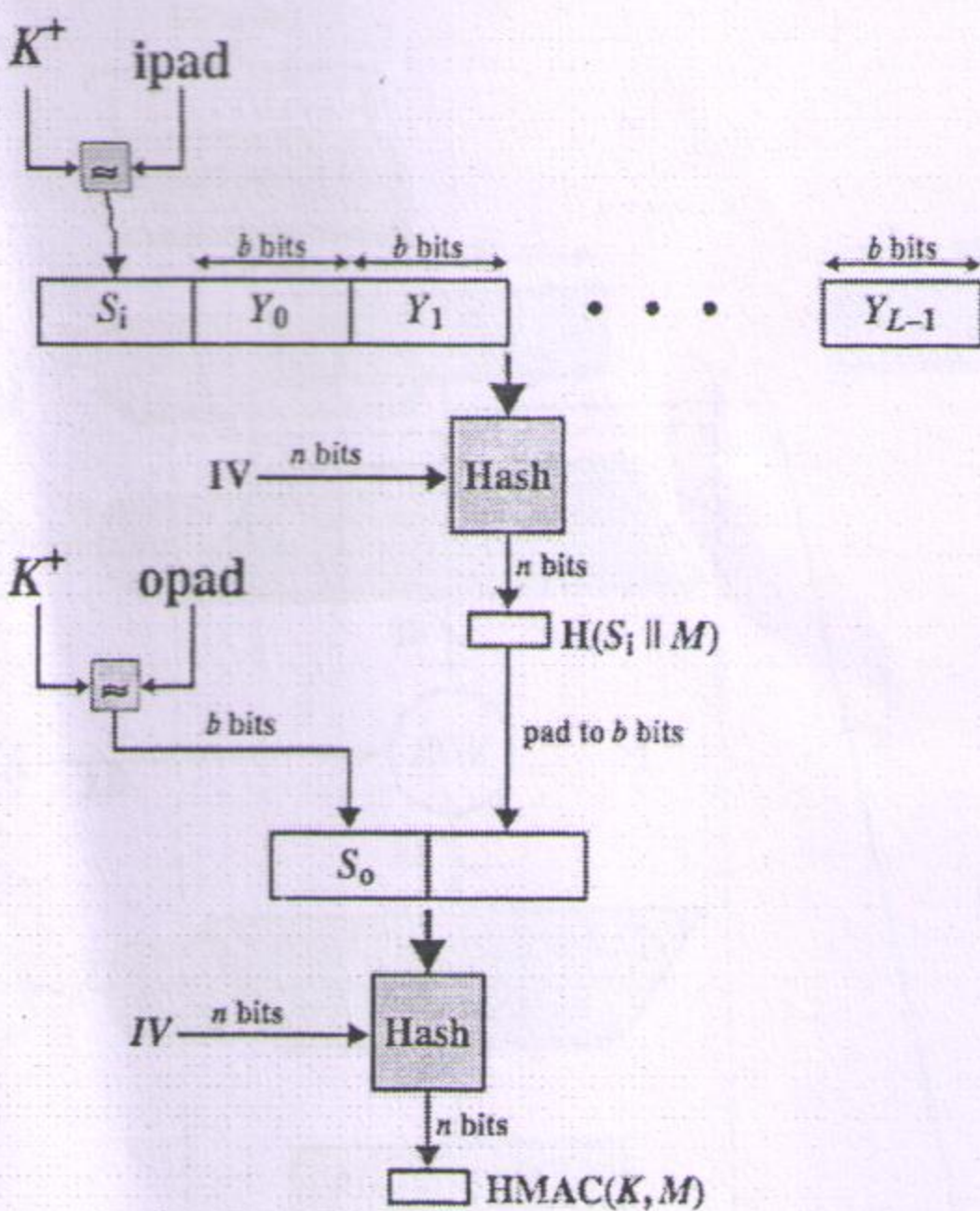
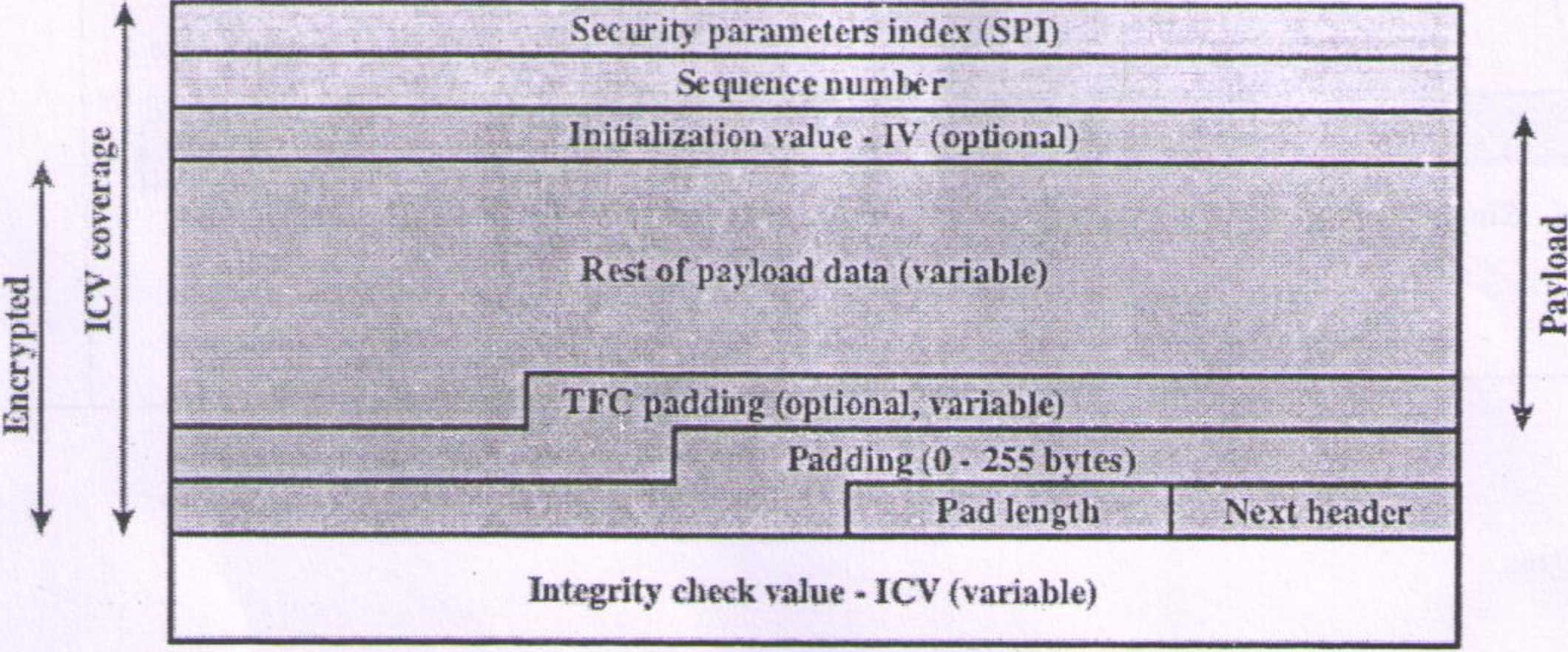


Figure 3.6 Single Round of DES Algorithm



Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

<p>Q3</p>	<p>Marks Distribution:</p> <ul style="list-style-type: none"> • Explained properly HMAC Structure with diagram ----- 10 mks • Explained properly HMAC Structure w/o diagram ----- 7 mks 	<p>10</p>
<p>Q4</p>	 <p>(b) Substructure of payload data</p> <p>Figure 19.5 ESP Packet Format</p> <ul style="list-style-type: none"> • Security Parameters Index (32 bits): A 32-bit value selected by the receiving end of an SA to uniquely identify the SA. • Sequence Number (32 bits): A monotonically increasing counter value; this provides an anti-replay function, as discussed for AH. 	<p>10</p>

Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

- 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): The Padding field is used to expand the plaintext to the required length.
- 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).
- Integrity Check Value (variable): A variable-length field that contains the Integrity Check Value computed over the ESP packet minus the Authentication Data field.

Marks Distribution:

Explained properly ESP Packet Format with diagram ----- 10 mks

Explained properly ESP Packet Format without diagram ----- 07 mks

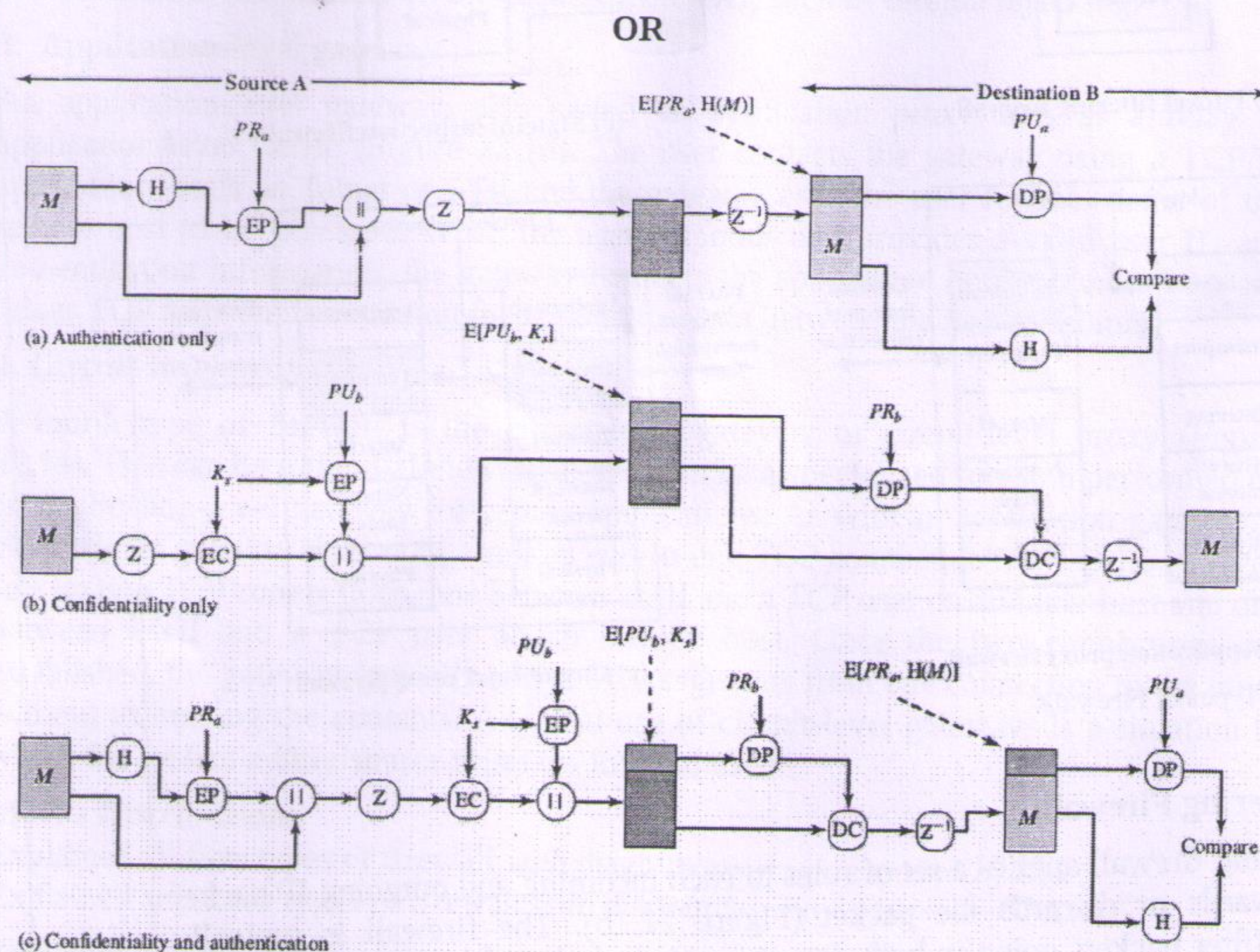


Figure 18.1 PGP Cryptographic Functions



Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

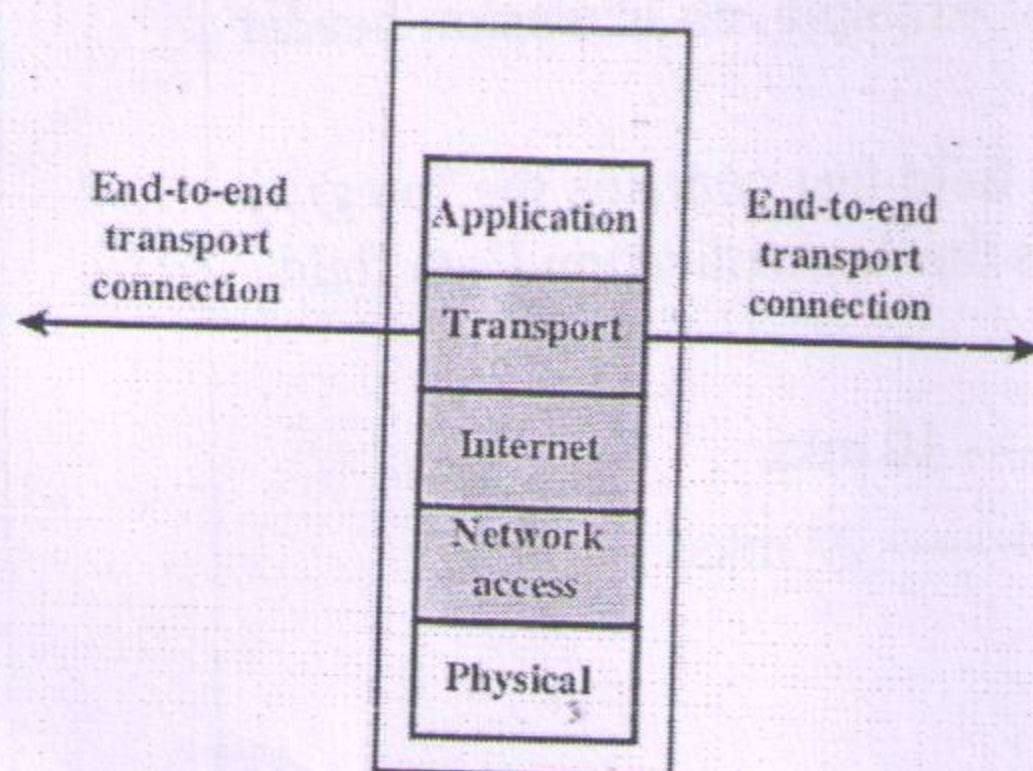
Marks Distribution:

Explained the PGP Cryptographic Functions for authentication with diagram-----03mks
Explained the PGP Cryptographic Functions for confidentiality with diagram-----03mks
Explained the PGP Cryptographic Functions for confidentiality and authentication both with diagram-----04mks

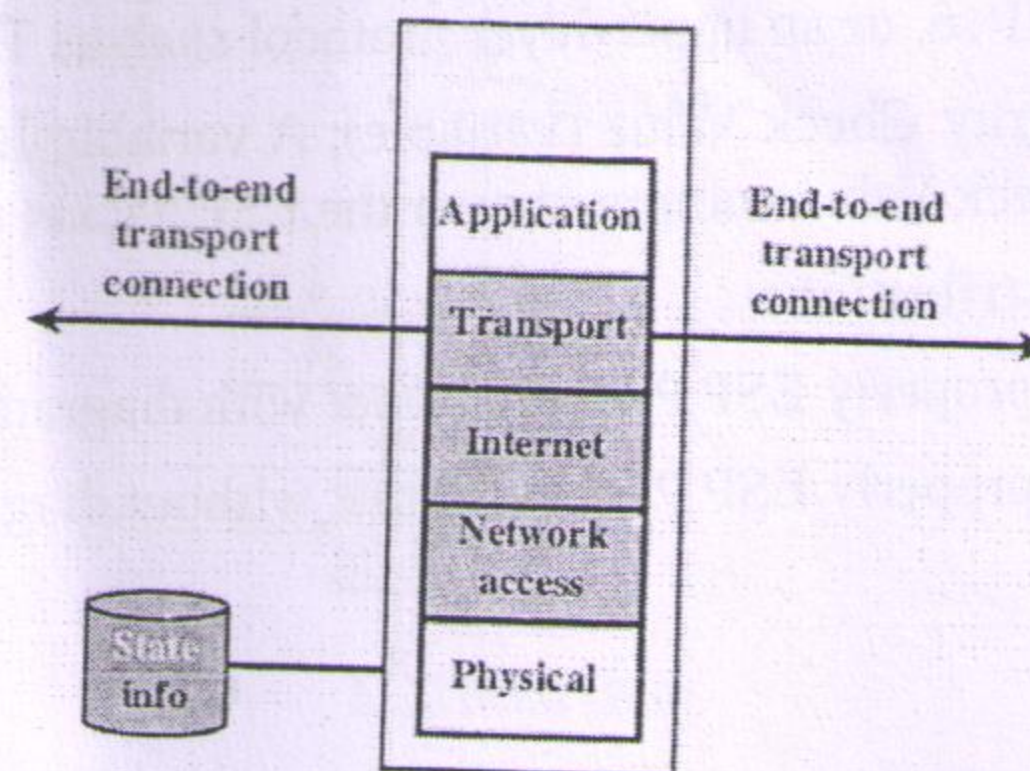
Q5

Explain different types of Firewall with diagram.

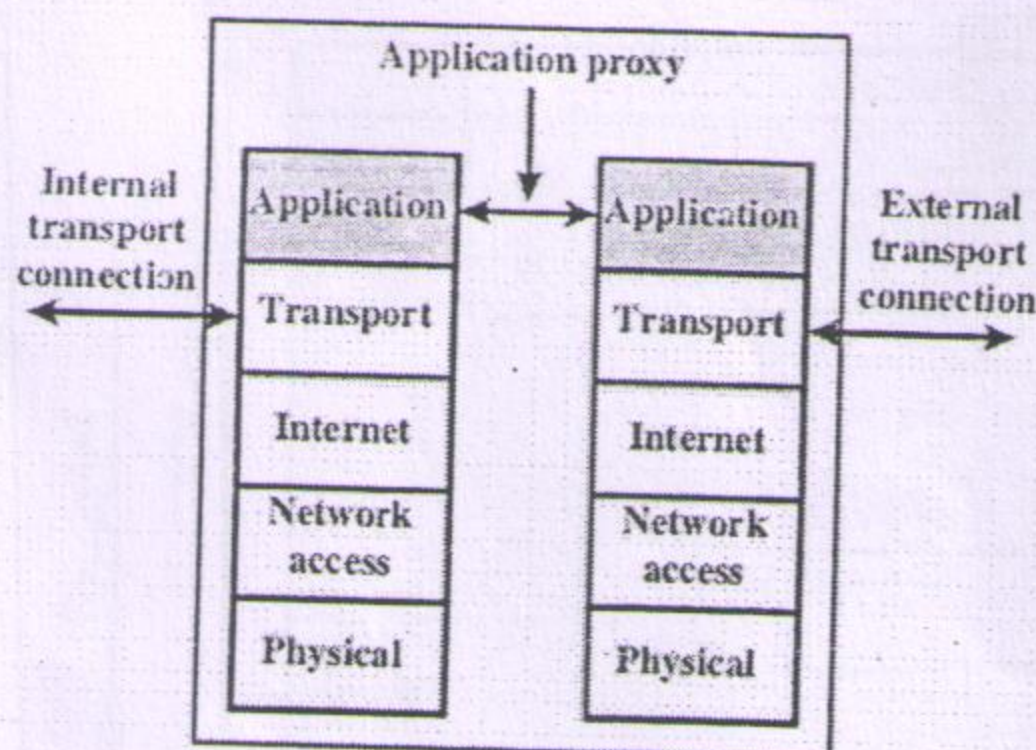
10



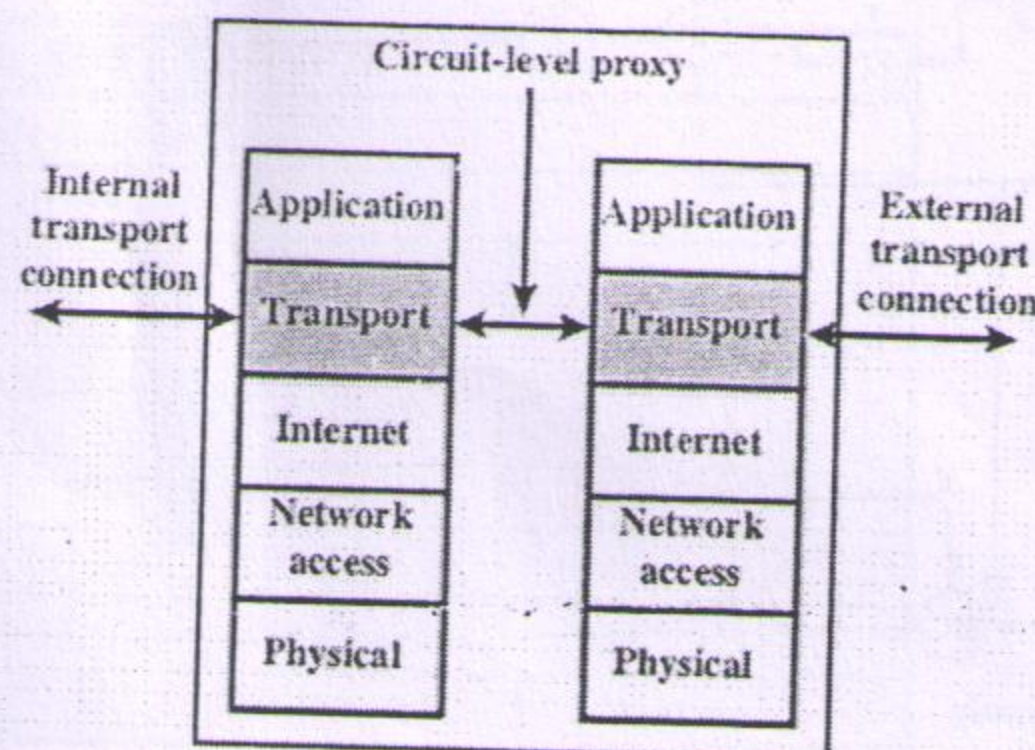
(b) Packet filtering firewall



(c) Stateful inspection firewall



(d) Application proxy firewall



(e) Circuit-level proxy firewall

Figure 22.1 Types of Firewalls

1. Packet Filtering Firewall:

A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet (Figure 22.1b). The firewall is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet:

- Source IP address: The IP address of the system that originated the IP packet (e.g.,



Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

192.178.1.1)

- Destination IP address: The IP address of the system the IP packet is trying to reach (e.g., 192.168.1.2)
- Source and destination transport-level address: The transport-level (e.g., TCP or UDP) port number, which defines applications such as SNMP or TELNET
- IP protocol field: Defines the transport protocol
- Interface: For a firewall with three or more ports, which interface of the firewall the packet came from or which interface of the firewall the packet is destined for.

2. Stateful inspection packet firewall:

A stateful inspection packet firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections, as shown in Table 22.2. There is an entry for each currently established connection. The packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory. A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall, but also records information about TCP connections (Figure 22.1c). Some stateful firewalls also keep track of TCP sequence numbers to prevent attacks that depend on the sequence number, such as session hijacking.

3. Application-level gateway :

An application-level gateway, also called an application proxy, acts as a relay of application-level traffic (Figure 22.1d). The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.

4. Circuit-level proxy:

A fourth type of firewall is the circuit-level gateway or circuit-level proxy (Figure 22.1e). This can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications. As with an application gateway, a circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users.

Marks Distribution:

- Explained all four types of firewall with diagrams----- 10mks
Explained any three types of firewall with diagrams----- 07 mks
Explained any two types of firewall with diagrams----- 05 mks