Sardar Patel Institute of Technology

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

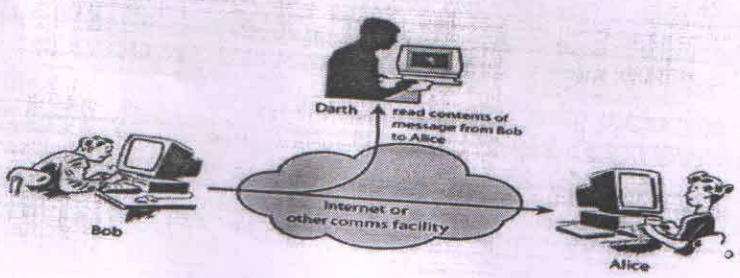
End Semester Examination

May 2019

Max. Marks: 60 | **Duration: 3 hr**
Class: T.E. | **Semester: IV**
Course Code: CE62 | **Branch: Computer**
Name of the Course: Cryptography and System Security

Instructions:

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

Q. No.		Max. Mks
Q1.a.	A **passive** attack attempts to learn or make use of information from the system but does not affect system resources. An **active** attack attempts to alter system resources or affect their operation. **Types of 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 illustrated in Fig.1. 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.  Fig.1. Release of Message contents • A second type of passive attack, traffic analysis, is illustrated in Fig.2. 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.	06

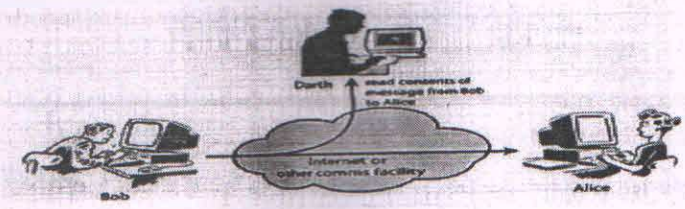
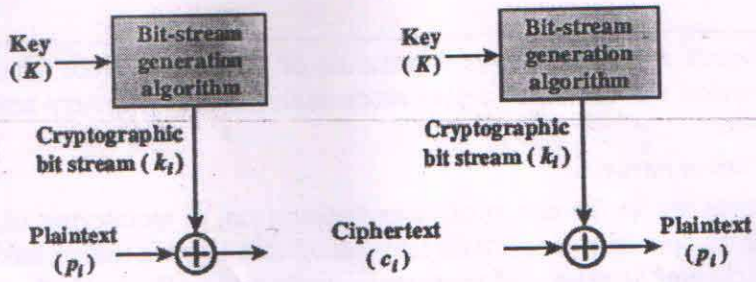


Fig 2: Traffic Analysis

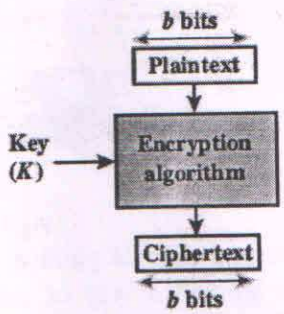
Marks Distribution:
Difference between Active and Passive Attacks---------- 02 mk
Types of Passive Attacks with diagram ------ 02mks (for each type)

Q1.b. 06



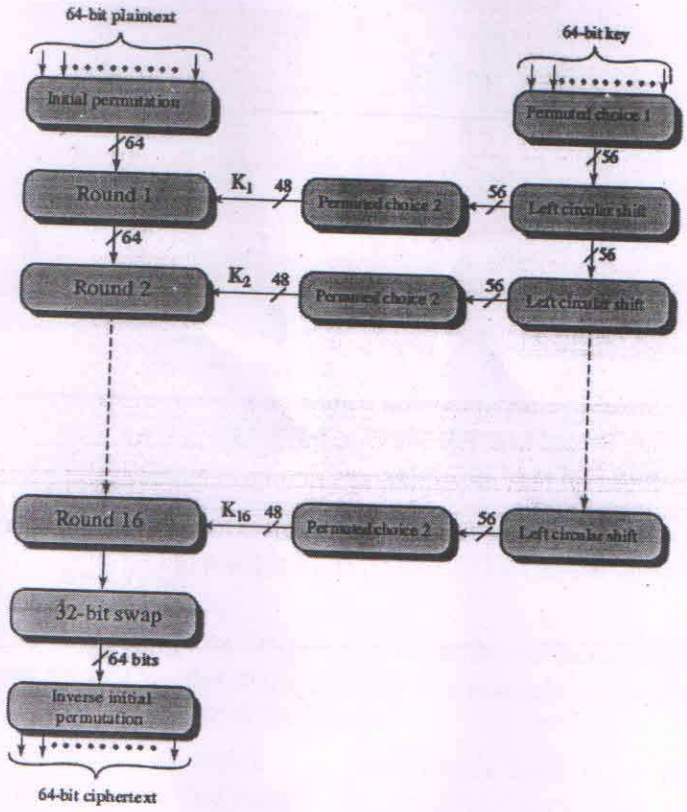
(a) Stream cipher using algorithmic bit-stream generator

A **stream cipher** is one that encrypts a digital data stream one bit or one byte at a time. Examples of classical stream ciphers are the autokeyed Vigenère cipher and the Vernam cipher. In the ideal case, a one-time pad version of the Vernam cipher would be used in which the keystream (ki) is as long as the plaintext bit stream (pi) . If the cryptographic keystream is random, then this cipher is unbreakable by any means other than acquiring the keystream. However, the keystream must be provided to both users in advance via some independent and secure channel.



(b) Block cipher

A **block cipher** is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length. Typically, a block size of 64 or 128 bits is used. As with a stream cipher, the two users share a symmetric encryption key. In general, they seem applicable to a broader range of applications than stream ciphers. The vast majority of network-based symmetric

	cryptographic applications make use of block ciphers. **Marks Distribution:** Explain Stream and Block Cipher with diagram-------- 3mks for each cipher Explain Stream and Block Cipher without diagram-------- 2mks for each cipher	
Q2. a	**Marks Distribution:** Explained RSA Key Generation Algorithm----------**03mks** Explained RSA Encryption Algorithm----------**1.5mks** Explained RSA Decryption Algorithm----------**1.5mks**	6
Q2. b	**DES Encryption algorithm**  Figure 3.5 General Depiction of DES Encryption Algorithm	6

Sardar Patel Institute of Technology

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

Single Round of DES Algorithm

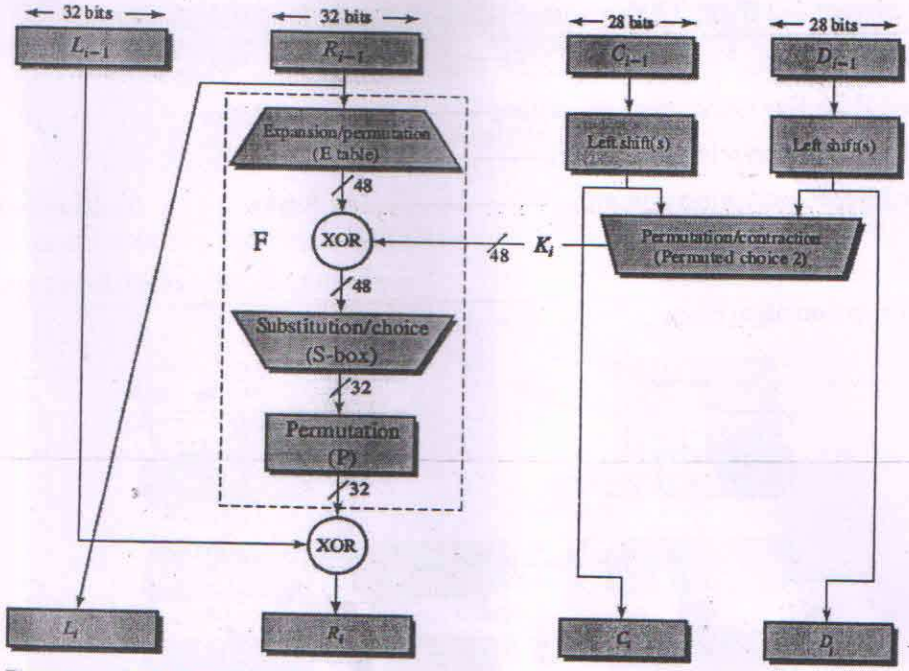


Figure 3.6 Single Round of DES Algorithm

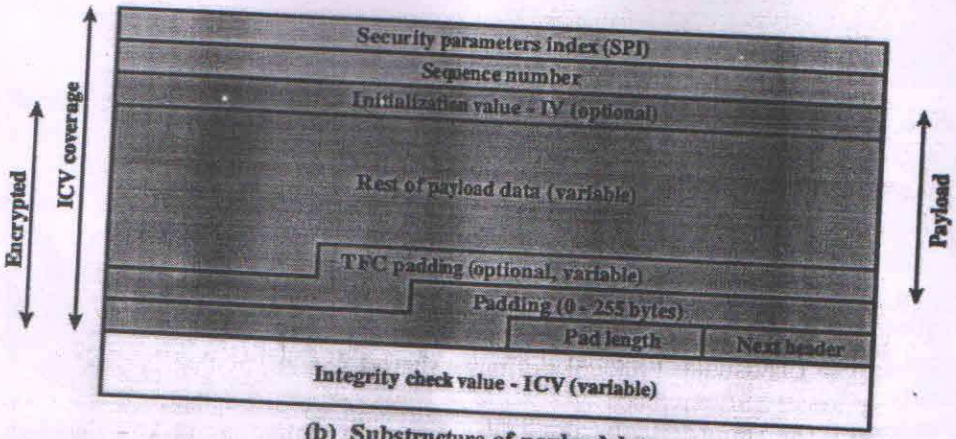
Marks Distribution:

Explained properly DES Encryption algorithm with diagram ---------- 03mks
Explained properly Single Round of DES Encryption algorithm with diagram --- 03mks
Explained properly DES Encryption algorithm w/o diagram ---------- 02mks
Explained properly Single Round of DES Encryption algorithm w/o diagram –02mks

Q3.

ESP Packet Format:

- Security Parameters Index (32 bits): A 32-bit value selected by the receiving end of an SA to uniquely identify the SA. In an SAD entry for an outbound SA, the SPI is used to construct the packet's AH or ESP header. In an SAD entry for an inbound SA, the SPI is used to map traffic to the appropriate SA.
- 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): The Padding field is used to expand the plaintext (consisting of the Payload Data, Padding, Pad Length, and Next Header fields) to the required length.



(b) Substructure of payload data

Figure 19.5 ESP Packet Format

- 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 (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.

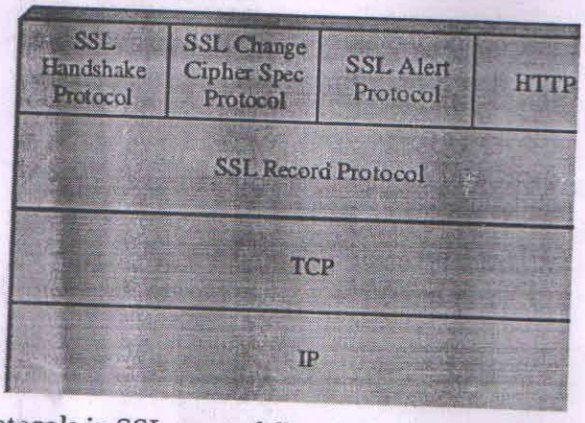
Marks Distribution:

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

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

10

OR



Protocols in SSL are as follows:
1. Record Protocol
2. Change Cipher Spec Protocol
3. Alert Protocol
4. Handshake Protocol

1. Record Protocol:

The SSL Record Protocol provides *two services* for SSL connections:

- **Confidentiality:** The Handshake Protocol defines a shared secret **key** that is used for conventional encryption of SSL payloads.
- **Message Integrity:** The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

Figure shown below indicates the overall operation of the SSL Record Protocol. The Record Protocol takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment. Received data are decrypted, verified, decompressed, and reassembled before being delivered to higher-level users.

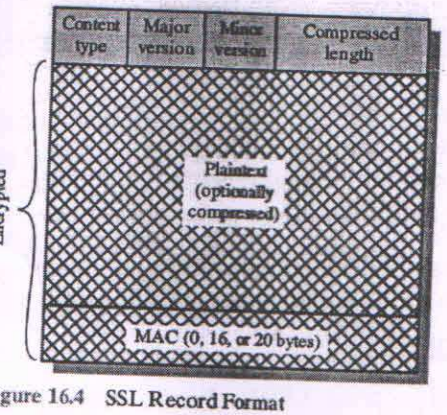


Figure 16.4 SSL Record Format

SSL Record Protocol format consist of the following fields as represented in the fig above:

- Content Type (8 bits): The higher-layer protocol used to process the enclosed fragment.
- Major Version (8 bits): Indicates major version of SSL in use. For SSLv3, the value is 3.
- Minor Version (8 bits): Indicates minor version in use. For SSLv3, the value is 0.
- Compressed Length (16 bits): The length in bytes of the plaintext fragment (or compressed fragment if compression is used). The maximum value is 2 14 +2048 .

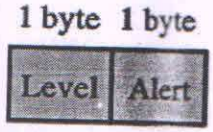
2. Change Cipher Spec Protocol

The Change Cipher Spec Protocol is one of the three SSL-specific protocols that use the SSL Record Protocol, and it is the simplest. This protocol consists of a single message shown in the fig below, which consists of a single byte with the value 1.

(a) Change Cipher Spec Protocol

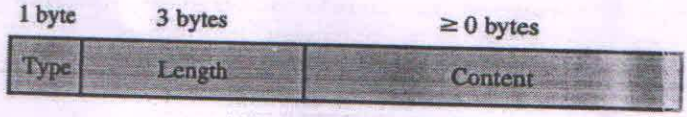
3. Alert Protocol

The Alert Protocol is used to convey SSL-related alerts to the peer entity. As with other applications that use SSL, alert messages are compressed and encrypted, as specified by the current state. Each message in this protocol consists of two bytes depicted in the fig below. The first byte takes the value warning (1) or fatal (2) to convey the severity of the message. If the level is fatal, SSL immediately terminates the connection. The second byte contains a code that indicates the specific alert.



(b) Alert Protocol

4. Handshake Protocol



(c) Handshake Protocol

The most complex part of SSL is the Handshake Protocol. The Handshake Protocol is used before any application data is transmitted. The Handshake Protocol consists of a series of messages exchanged by client and server. Each message has three fields:

- Type (1 byte): Indicates one of 10 messages.

hello_request, client_hello, server_hello, certificate, server_key_exchange, certificate_request, server_done , certificate_verify , client_key_exchange, finished

- Length (3 bytes): The length of the message in bytes.
- Content (Ú 0 bytes): The parameters associated with this message.

Marks Distribution:

Explained all four protocols with required diagrams ---------- 10 mks
Explained all four protocols without required diagrams ---------- 06 mks

Q4.

Generic Model

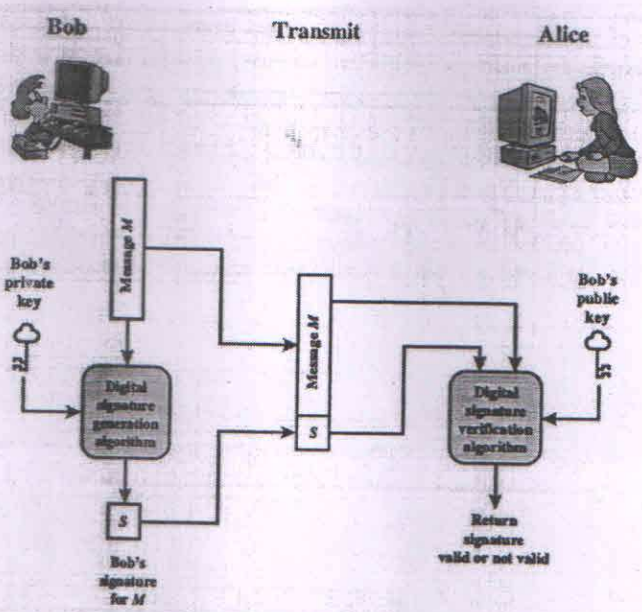


Figure 13.1 Generic Model of Digital Signature Process

Elgamal Scheme: 06

As with ElGamal encryption, the global elements of **ElGamal digital signature** are a prime number q and α, which is a primitive root of q. User A generates a private/public key pair as follows.

1. Generate a random integer X_A, such that $1 < X_A < q - 1$.
2. Compute $Y_A = \alpha^{X_A} \bmod q$.
3. A's private key is X_A; A's pubic key is $\{q, \alpha, Y_A\}$.

To sign a message M, user A first computes the hash $m = \mathrm{H}(M)$, such that m is an integer in the range $0 \le m \le q - 1$. A then forms a digital signature as follows.

1. Choose a random integer K such that $1 \le K \le q - 1$ and $\gcd(K, q - 1) = 1$. That is, K is relatively prime to $q - 1$.
2. Compute $S_1 = \alpha^K \bmod q$. Note that this is the same as the computation of C_1 for ElGamal encryption.
3. Compute $K^{-1} \bmod (q - 1)$. That is, compute the inverse of K modulo $q - 1$.
4. Compute $S_2 = K^{-1}(m - X_A S_1) \bmod (q - 1)$.
5. The signature consists of the pair (S_1, S_2).

Any user B can verify the signature as follows.

1. Compute $V_1 = \alpha^m \bmod q$.
2. Compute $V_2 = (Y_A)^{S_1}(S_1)^{S_2} \bmod q$.

The signature is valid if V 1 = V 2 .

Marks Distribution:

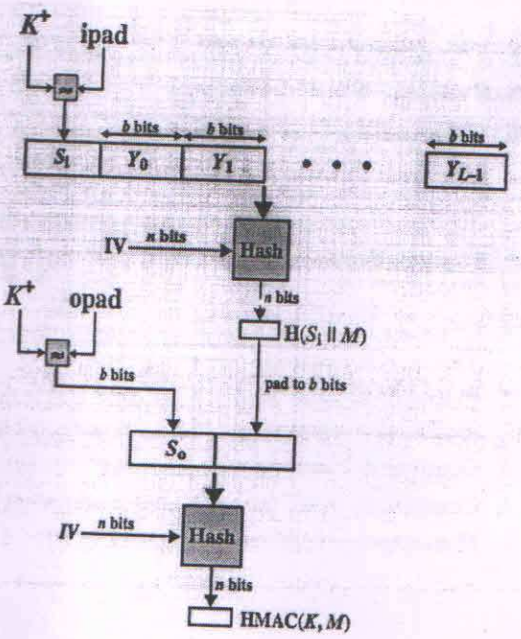
Generic Model of Digital Signature Process--------- 02 mks

Elgamal Signature Scheme ---------- 04mks

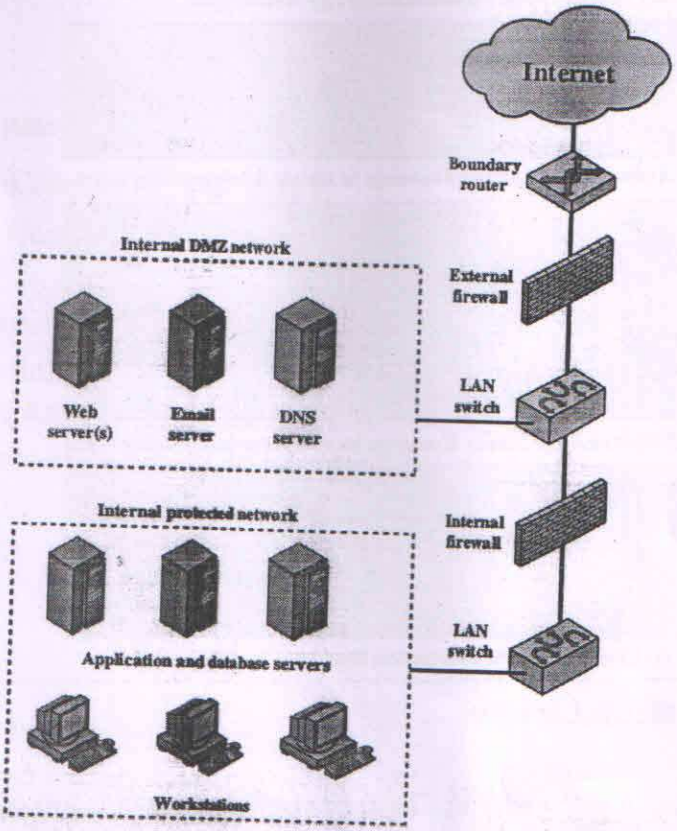
OR

Marks Distribution:

- Explained properly HMAC Structure with diagram -----06 mks
- Explained properly HMAC Structure w/o diagram ----04 mks



Q5.a.	**Table 15.1 Summary of Kerberos Version 4 Message Exchanges** (1) C → AS $ID_c \| ID_{tgs} \| TS_1$ (2) AS → C $E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$ $Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$ **(a) Authentication Service Exchange to obtain ticket-granting ticket** (3) C → TGS $ID_v \| Ticket_{tgs} \| Authenticator_c$ (4) TGS → C $E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$ $Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$ $Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$ $Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$ **(b) Ticket-Granting Service Exchange to obtain service-granting ticket** (5) C → V $Ticket_v \| Authenticator_c$ (6) V → C $E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication) $Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$ $Authenticator_c = E(K_{c,v}, [ID_C \| AD_C \| TS_5])$ **(c) Client/Server Authentication Exchange to obtain service**	10
Q5.b.	**Firewall Configuration and its Location** **DMZ Networks:** An external firewall is placed at the edge of a local or enterprise network, just inside the boundary router that connects to the Internet or some wide area network (WAN). Between these two types of firewalls are one or more networked devices in a region referred to as a DMZ (demilitarized zone) network. The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity. In this type of configuration, internal firewalls serve three purposes: 1. The internal firewall adds more stringent filtering capability, compared to the external firewall, in order to protect enterprise servers and workstations from external attack. 2. The internal firewall provides two-way protection with respect to the DMZ. First, the internal firewall protects the remainder of the network from attacks launched from DMZ systems. Second, an internal firewall can protect the DMZ systems from attack from the internal protected network. 3. Multiple internal firewalls can be used to protect portions of the internal network from each other.	10



Virtual Private Networks (VPN)

A VPN consists of a set of computers that interconnect by means of a relatively unsecure network and that make use of encryption and special protocols to provide security. A VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet. The most common protocol mechanism used for this purpose is at the IP level and is known as IPsec. A logical means of implementing an IPsec is in a firewall, as shown in Figure 22.4. If IPsec is implemented in a separate box behind (internal to) the firewall, then VPN traffic passing through the firewall in both directions is encrypted. In this case, the firewall is unable to perform its filtering function or other security functions, such as access control, logging, or scanning for viruses.

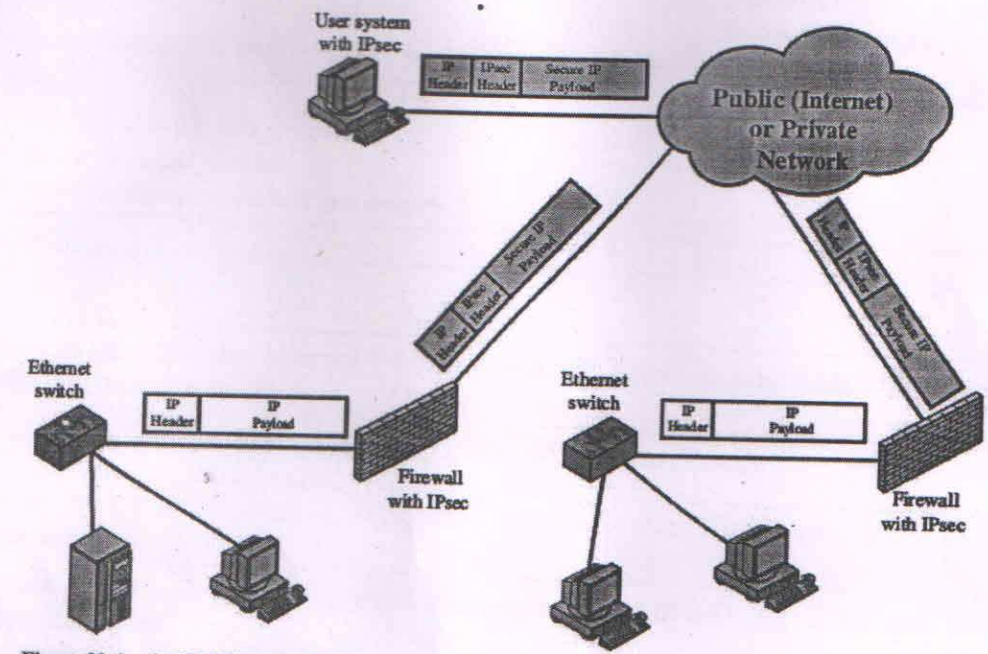


Figure 22.4 A VPN Security Scenario

Marks Distribution:

Explained properly both DMZ and VPN with diagrams---------- 05mks for each configuration

Explained properly both DMZ and VPN without diagrams ------ 03mks for each configuration