Sardar Patel Institute of Technology

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

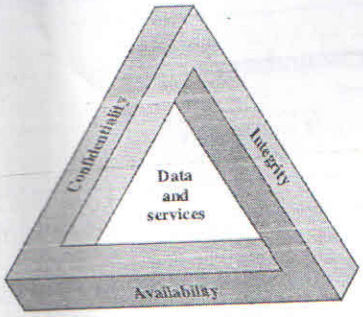
End Semester Examination

Nov 2018

Max. Marks: 60 **Duration: 3 hr**
Class: B.E. **Semester:** VII
Course Code: CPC702 **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**
Q 1.a)	**Diffusion:** In diffusion, the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits; generally, this is equivalent to having each ciphertext digit be affected be many plaintext digits. An example of diffusion is to encrypt a message M = m 1 , m 2 , m 3 , . . . of characters with an averaging operation: $y_n = \left(\sum_{i=1}^{k} m_{n+i}\right) \bmod 26$ adding k successive letters to get a ciphertext letter y n . One can show that the statistical structure of the plaintext has been dissipated. In a binary block cipher, diffusion can be achieved by repeatedly performing some permutation on the data followed by applying a function to that permutation; the effect is that bits from different positions in the original plaintext contribute to a single bit of ciphertext. ***The mechanism of diffusion seeks to make the statistical relationship between the plaintext and ciphertext as complex as possible in order to thwart attempts to deduce the key.*** **Confusion:** ***Confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key*** as complex as possible, again to thwart attempts to discover the key. Thus, even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was used to produce that ciphertext is so complex as to make it difficult to deduce the key. This is achieved by the use of a complex substitution algorithm. In contrast, a simple linear substitution function would add little confusion. **Marks Distribution:** Explained the tern diffusion properly using the technical term ---------------- **2.5mks**	05

	Explained the tern confusion properly using the technical term ---------------- **2.5mks**	
Q 1.b)	Three key objectives that are at the heart of computer security are: 1. Confidentiality 2. Availability 3. Integrity • **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.  Confidentiality Integrity Data and services Availability Figure 1.1 The Security Requirements Triad • **Integrity**: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.\ • **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. **Marks Distribution:** What are the three key objectives / goals of computer security?-------- 01mks Explained all three goals properly with diagram------------------------ 04mks Explained all three goals properly without diagram------------------------ 03mks	05mks

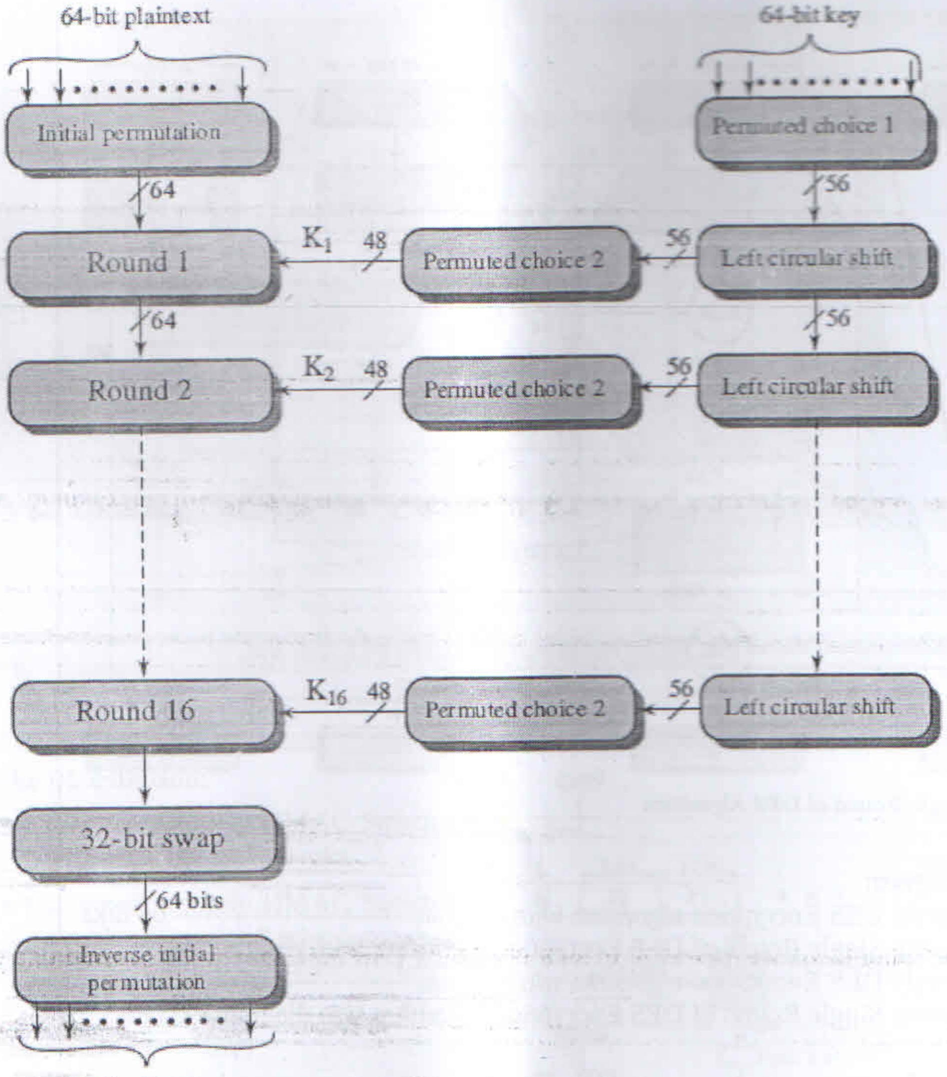
<table>
<tr>
<td>Q 2)</td>
<td>


Figure 3.5 General Depiction of DES Encryption Algorithm
</td>
<td>10</td>
</tr>
</table>

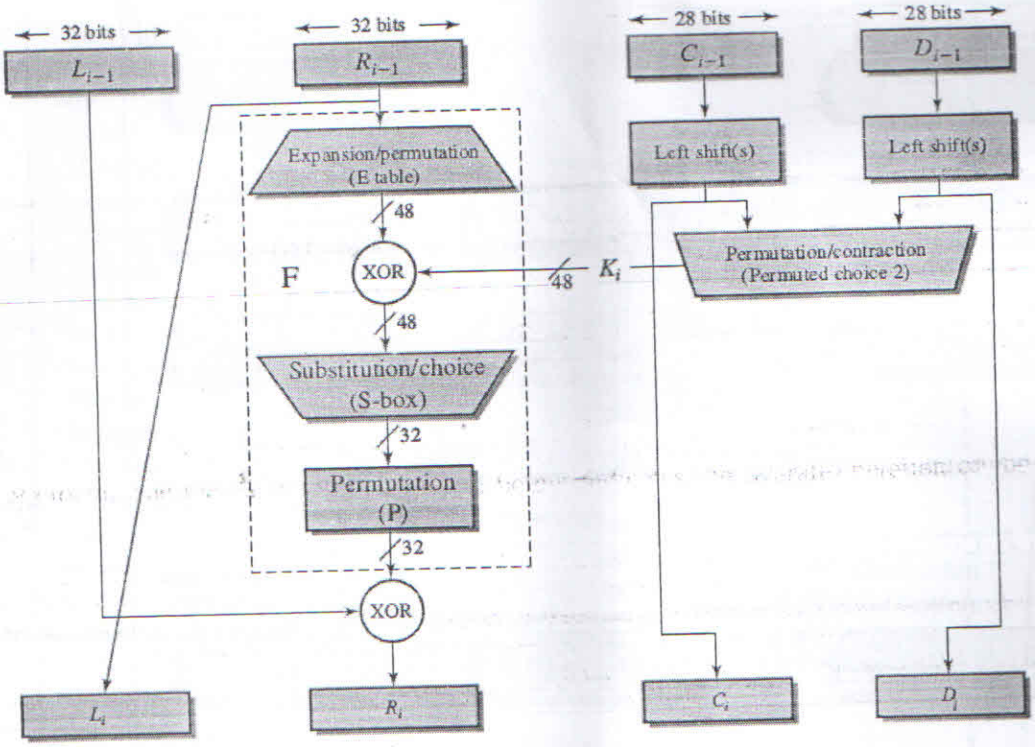


Figure 3.6 Single Round of DES Algorithm

Marks Distribution:

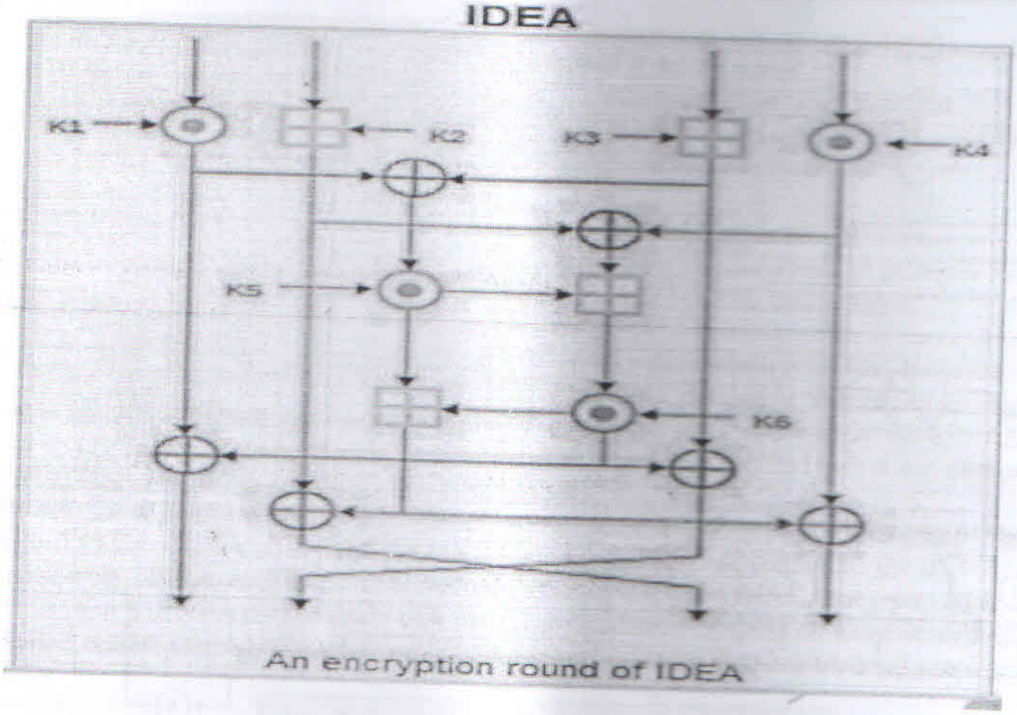
Explained properly DES Encryption algorithm with diagram ---------------------- 05 mks
Explained properly Single Round of DES Encryption algorithm with diagram --- 05 mks
Explained properly DES Encryption algorithm w/o diagram ---------------------- 03 mks
Explained properly Single Round of DES Encryption algorithm w/o diagram --03 mks

OR

Marks Distribution:

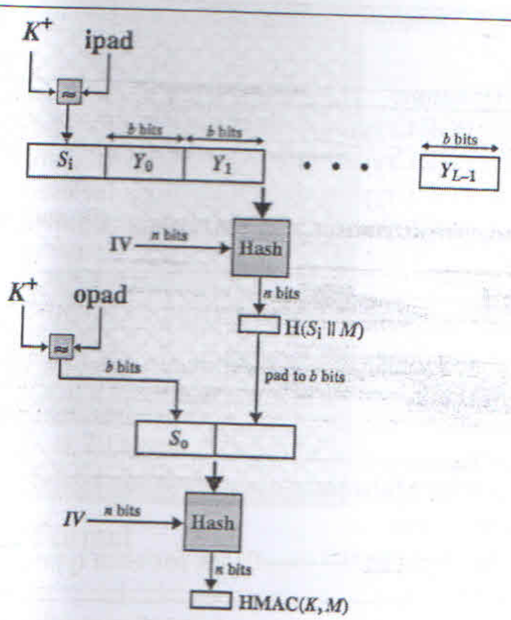
Explained properly IDEA and its subkey generation algorithm with diag ----- 10 mks
Explained properly IDEA and its subkey generation algorithm w/o diag----- 08 mks
Explained properly IDEA algo but not its subkey generation algo with diag----- 07 mks
Explained properly IDEA algo but not its subkey generation algo w/o diag--- 05 mks

<table>
<tr>
<td></td>
<td>
IDEA

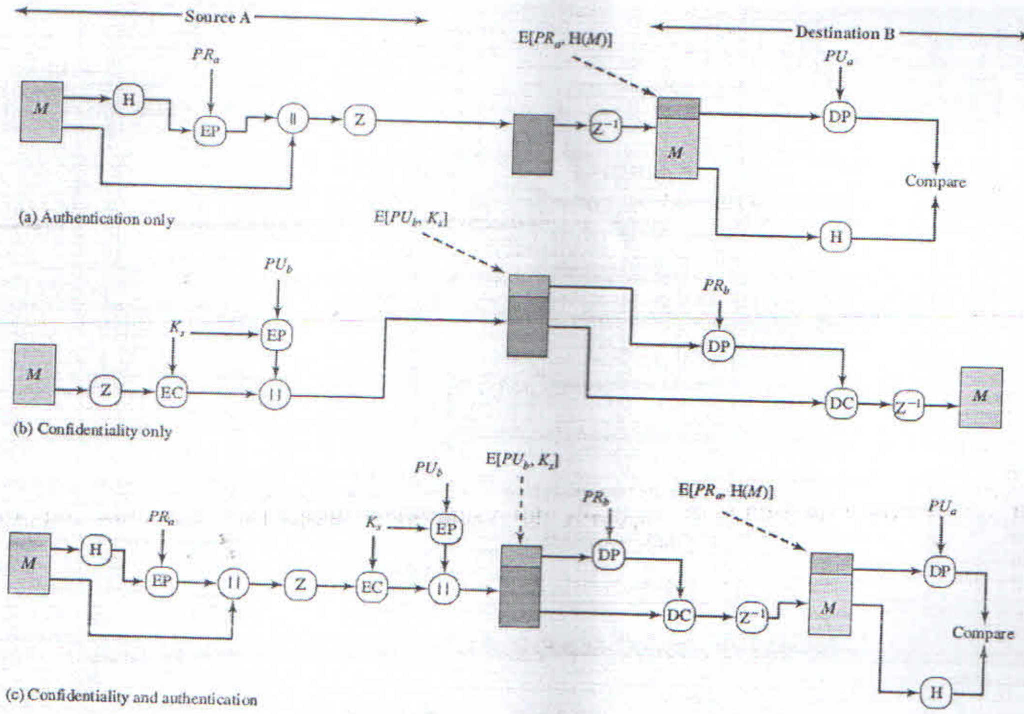


An encryption round of IDEA
</td>
<td></td>
</tr>
<tr>
<td>Q3</td>
<td>
<b>Marks Distribution:</b>

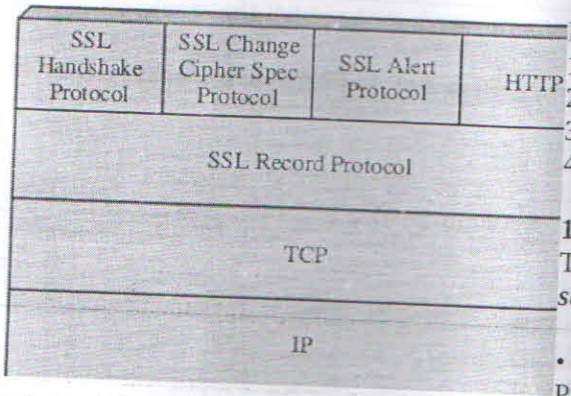
- Explained properly HMAC Structure with diagram ----- 10 mks
- Explained properly HMAC Structure w/o diagram ----- 7 mks



</td>
<td>10</td>
</tr>
</table>

Q4. a)	 Source A Destination B PR_a M H EP || Z Z^{-1} $E[PR_a, H(M)]$ PU_a DP Compare $E[PU_b, K_s]$ PU_b K_s EC PR_b DC (a) Authentication only (b) Confidentiality only (c) Confidentiality and authentication **Figure 18.1** PGP Cryptographic Functions **Marks Distribution:** Explained the PGP Cryptographic Functions for authentication with diagram-----1.5mks Explained the PGP Cryptographic Functions for confidentiality with diagram-----1.5mks Explained the PGP Cryptographic Functions for confidentiality and authentication both with diagram-----02mks	05
Q4. b)	Types of Malicious Software are as follows: 1. Backdoor / trapdoor 2. Logic bomb 3. Trojan Horses 4. Mobile Code 5. Multiple-Threat Malware **Marks Distribution:** Explained all five types ----------01mk for each type	05

Q5. a) 10



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.

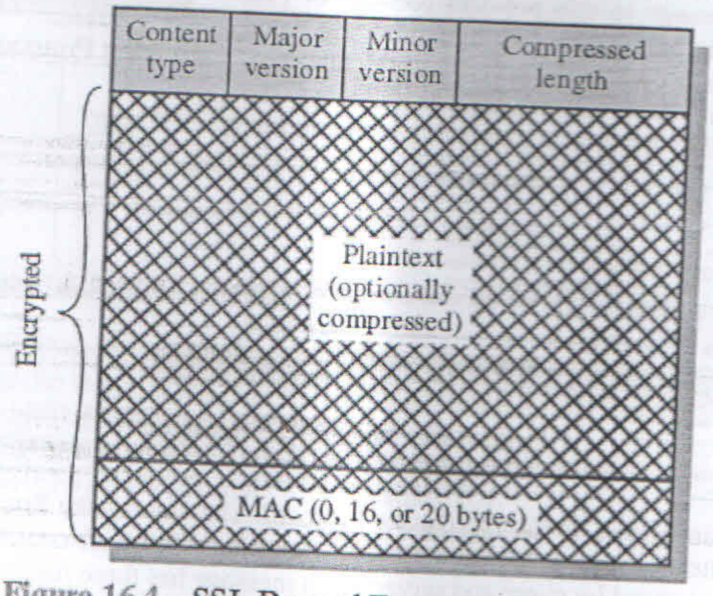


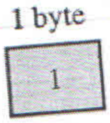
Figure 16.4 SSL Record Format

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

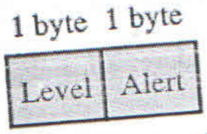
The Change Cipher Spec Protocol is one of the three SSL-specific protocols that use the SSL Record Protocol, and it is the simplest. This protocol consists of a single message shown in the fig below, which consists of a single byte with the value 1.



(a) Change Cipher Spec Protocol

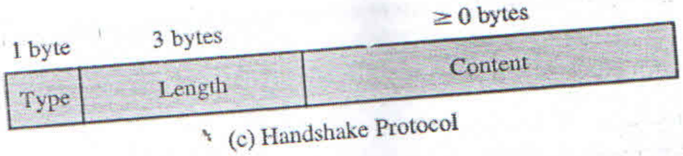
3. Alert Protocol

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.

Client and Sever establish an SSL connection:

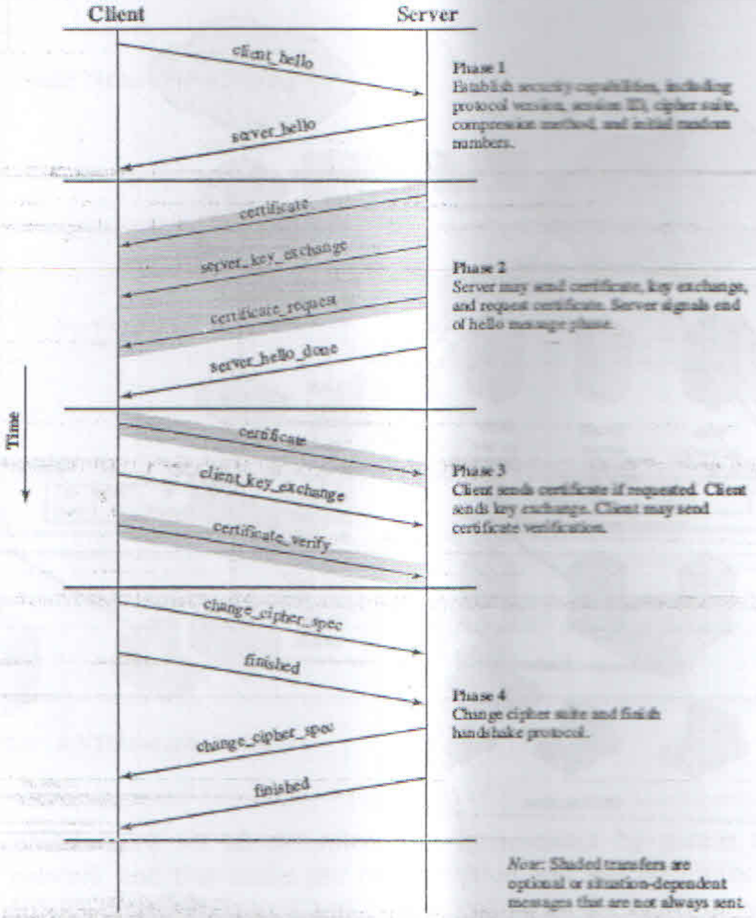

Client
Server
client_hello
server_hello
Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.
certificate
server_key_exchange
certificate_request
server_hello_done
Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.
Time
certificate
client_key_exchange
certificate_verify
Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.
change_cipher_spec
finished
change_cipher_spec
finished
Phase 4
Change cipher suite and finish handshake protocol.
Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

Figure 16.6 Handshake Protocol Action

The initial exchange needed to establish a logical connection between client and server. The exchange can be viewed as having four phases.

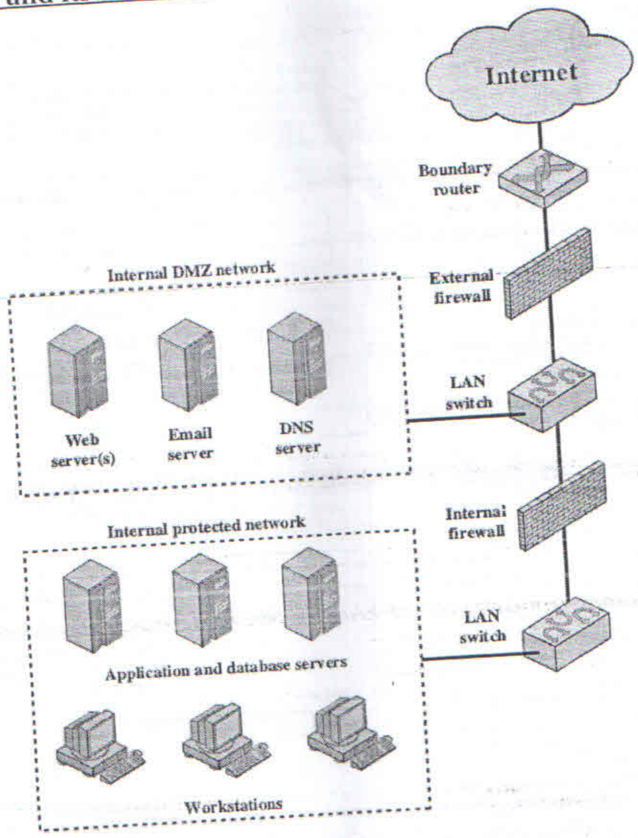
1. ESTABLISH SECURITY CAPABILITIES
2. SERVER AUTHENTICATION AND KEY EXCHANGE
3. CLIENT AUTHENTICATION AND KEY EXCHANGE
4. FINISH

Marks Distribution:

Explained all four protocols with required diagrams --------------- 07 mks
Explained all four protocols without required diagrams --------------- 04 mks
Explained client and sever establishing an SSL connection with diag ------- 03mks
Explained client and sever establishing an SSL connection without diag ------- 02mks

Q5. b) **Firewall Configuration and its Location** 10mks

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.

Virtual Private Networks (VPN)

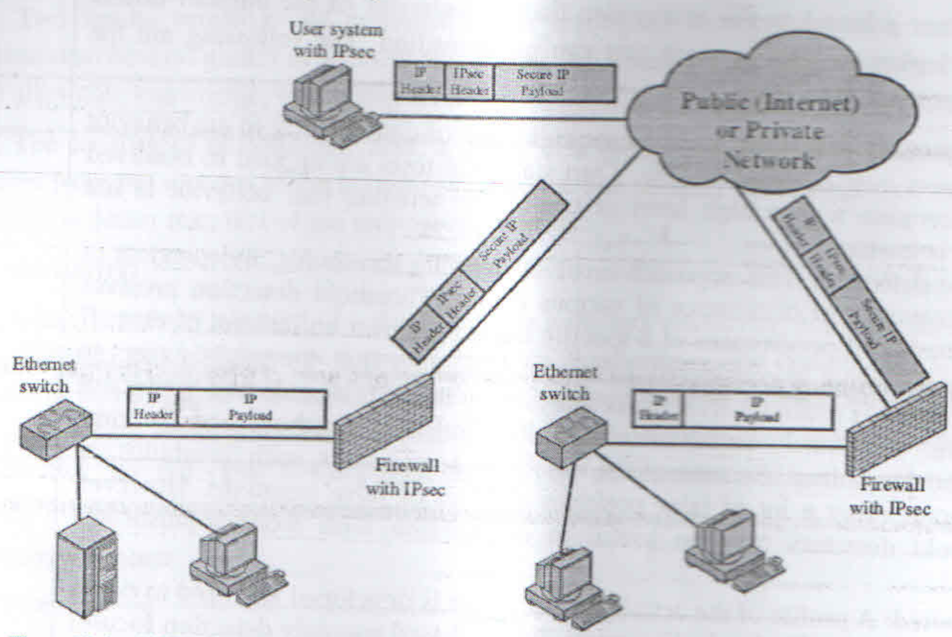


Figure 22.4 A VPN Security Scenario

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.

Marks Distribution:

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

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

	OR	
Q5. b)	**i. Intrusion Detection** Intrusion detection is based on the assumption that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified. The following are the approaches to intrusion detection: **1. Statistical anomaly detection**: Involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior. ***a. Threshold detection:*** This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events. Threshold detection involves counting the number of occurrences of a specific event type over an interval of time. If the count surpasses what is considered a reasonable number that one might expect to occur, then intrusion is assumed. Threshold analysis, by itself, is a crude and ineffective detector of even moderately sophisticated attacks. Both the threshold and the time interval must be determined. Because of the variability across users, such thresholds are likely to generate either a lot of false positives or a lot of false negatives. However, simple threshold detectors may be useful in conjunction with more sophisticated techniques. ***b. Profile based:*** A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts. Profile-based anomaly detection focuses on characterizing the past behavior of individual users or related groups of users and then detecting significant deviations. A profile may consist of a set of parameters, so that deviation on just a single parameter may not be sufficient in itself to signal an alert. **2. Rule-based detection**: Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder. ***a. Anomaly detection:*** Rules are developed to detect deviation from previous usage patterns. With the rule-based approach, historical audit records are analyzed to identify usage patterns and to generate automatically rules that describe those patterns. Rules may represent past behavior patterns of users, programs, privileges, time slots, terminals, and so on. ***b. Penetration identification:*** An expert system approach that searches for suspicious behavior. The key feature of such systems is the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses. Rules can also be defined that identify suspicious behavior, even when the behavior is within the bounds of established patterns of usage. **ii. Multilevel Databases** The following are the three characteristics of database security:	10

1. The security of a single element may be different from the security of other elements of the same record or from other values of the same attribute. That is, the security of one element may differ from that of other elements of the same row or column. This situation implies that security should be implemented for each individual element.

2. Two levels- sensitive and nonsensitive are inadequate to represent some security situations. Several grades of security may be needed. These grades may represent ranges of allowable knowledge, which may overlap.

3. The security of an aggregate sum, a count, or a group of values in a database may differ from the security of the individual elements. The security of the aggregate may be higher or lower than that of the individual elements.

Granularity:

Not only can every element of a database have a distinct sensitivity, every combination of elements can also have a distinct sensitivity. Furthermore, the combination can be more or less sensitive than any of its elements. First, we need an access control policy to dictate which users may have access to what data. Second, we need a means to guarantee that the value has not been changed by an unauthorized person. These two requirements address both confidentiality and integrity.

Security Issues:

1. Integrity

In the case of multilevel databases, integrity becomes both more important and more difficult to achieve. Because of the *-property for access control, a process that reads high-level data is not allowed to write a file at a lower level. Applied to databases, however, this principle says that a high-level user should not be able to write a lower-level data element.

2. Confidentiality

Users trust that a database will provide correct information, meaning that the data are consistent and accurate. In the multilevel case, two different users operating at two different levels of security might get two different answers to the same query. To preserve confidentiality, precision is sacrificed. Enforcing confidentiality also leads to unknowing redundancy.

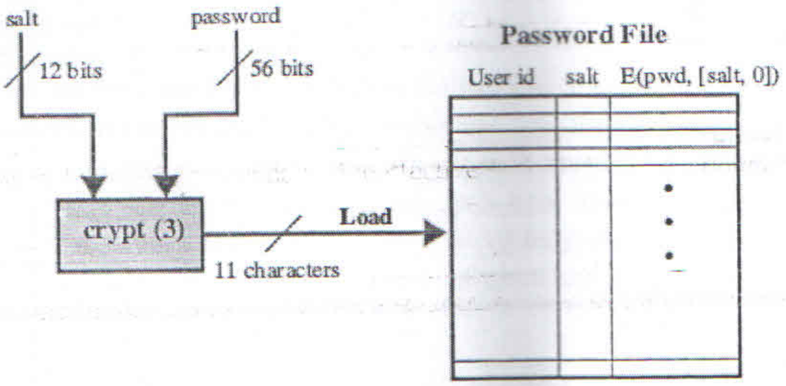
iii. Password Management:

Password Protection

The front line of defense against intruders is the password system. The password serves to authenticate the ID of the individual logging on to the system. In turn, the ID provides security in the following ways:

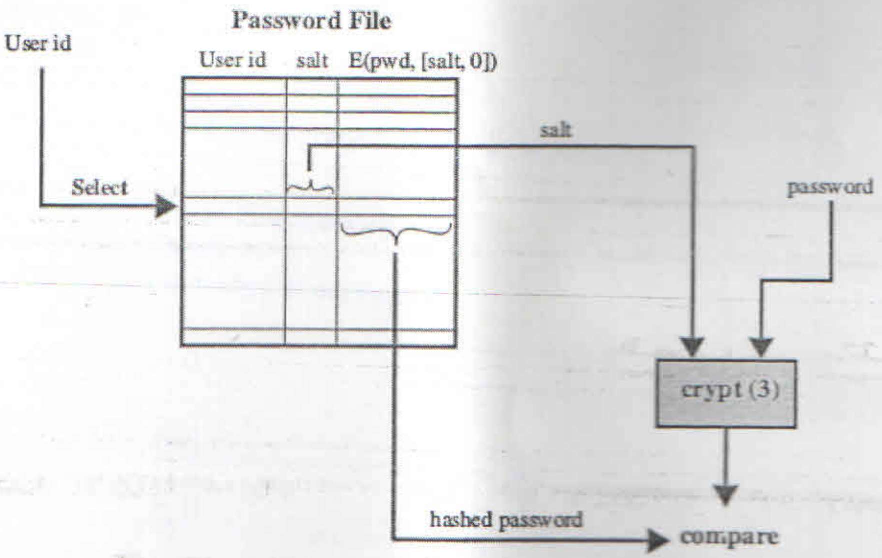
- The ID determines whether the user is authorized to gain access to a system.
- The ID determines the privileges accorded to the user.
- The ID is used in what is referred to as discretionary access control.

Each user selects a password of up to eight printable characters in length. This is converted into a 56-bit value (using 7-bit ASCII) that serves as the key input to an encryption routine. The encryption routine, known as crypt(3), is based on DES. The DES algorithm is modified using a 12-bit "salt" value.



(a) Loading a new password

When a user attempts to log on to a UNIX system, the user provides an ID and a password. The operating system uses the ID to index into the password file and retrieve the plaintext salt and the encrypted password. The salt and user-supplied password are used as input to the encryption routine. If the result matches the stored value, the password is accepted.



(b) Verifying a password

Password Selection Strategies:

Four basic techniques are in use:

- **User education :** Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords. This user education strategy is unlikely to succeed at most installations, particularly where there is a large user population or a lot of turnover.

- Computer-generated passwords: If the passwords are quite random in nature, users will not be able to remember them. Even if the password is pronounceable, the user may have difficulty remembering it and so be tempted to write it down. In general, computer-generated password schemes have a history of poor acceptance by users.

- Reactive password checking :strategy is one in which the system periodically runs its own password cracker to find guessable passwords. The system cancels any passwords that are guessed and notifies the user.
- Proactive password checking : The most promising approach to improved password security is a proactive password checker. In this scheme, a user is allowed to select his or her own password. However, at the time of selection, the system checks to see if the password is allowable and, if not, rejects it.