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- SET 2

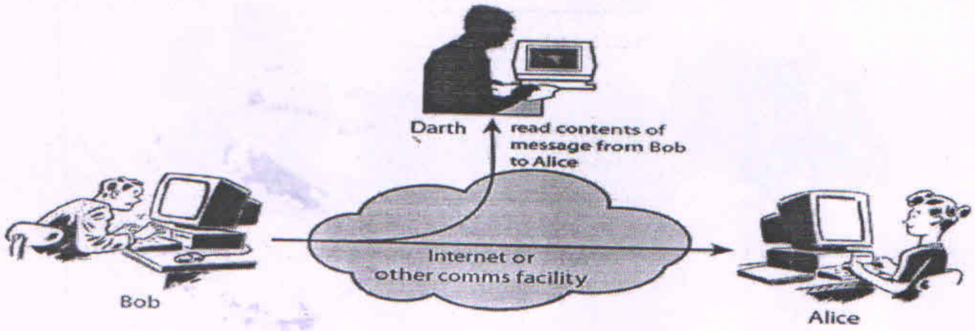
Nov 2018

Max. Marks: 60
Class: B.E.
Course Code: CPC702
Name of the Course: Cryptography and System Security

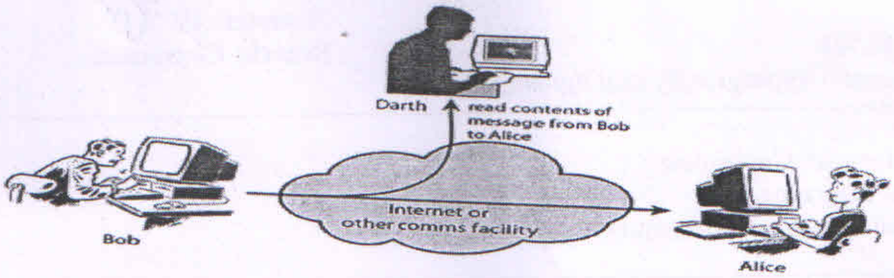
Duration: 3 hr
Semester: IV
Branch: Computer.

Instructions:

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

Q. No.		**Max Mks**
Q 1 (a)	**Marks Distribution:** What are block ciphers?----------------------------- 01mks Explained properly the CBC and ECB modes of block ciphers with the help of diagrams---- 02mks for each mode	05
Q 1 (b)	There are two types of security attacks: **1. Passive Attack** 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.  Darth read contents of message from Bob to Alice Internet or other comms facility Bob Alice 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	05

traffic so that opponents, even if they captured the message, could not extract the information from the message.


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Traffic Analysis

Fig 2:

2. Active Attack

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

- A **masquerade** takes place when one entity pretends to be a different entity represented in Fig. 3. A masquerade attack usually includes one of the other forms of active attack.

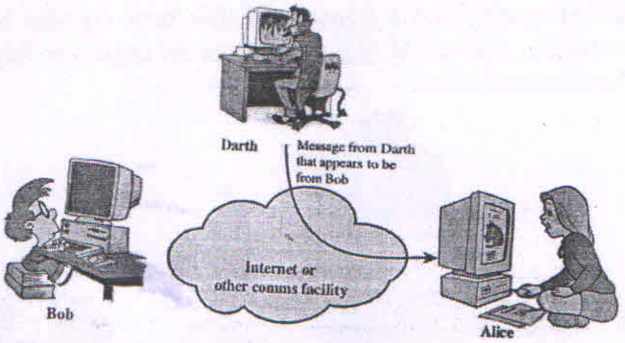

Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

Fig. 3: Masquerade

- **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect represented in Fig. 4

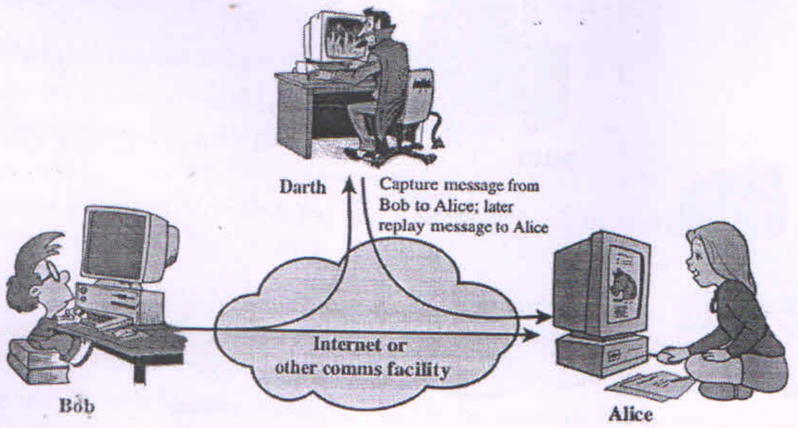

Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Fig. 4: Replay

- **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 represented in Fig. 5

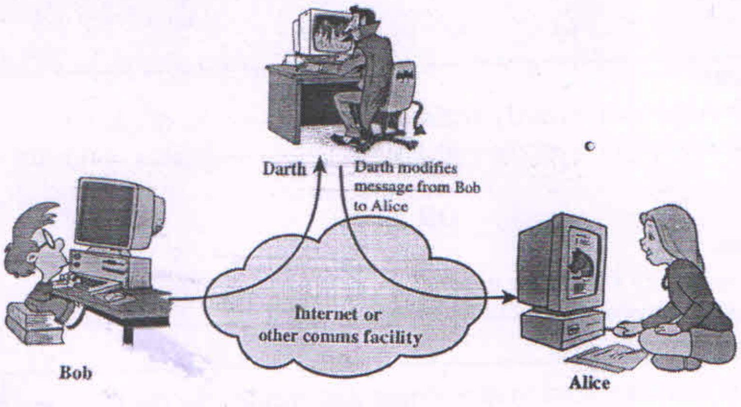
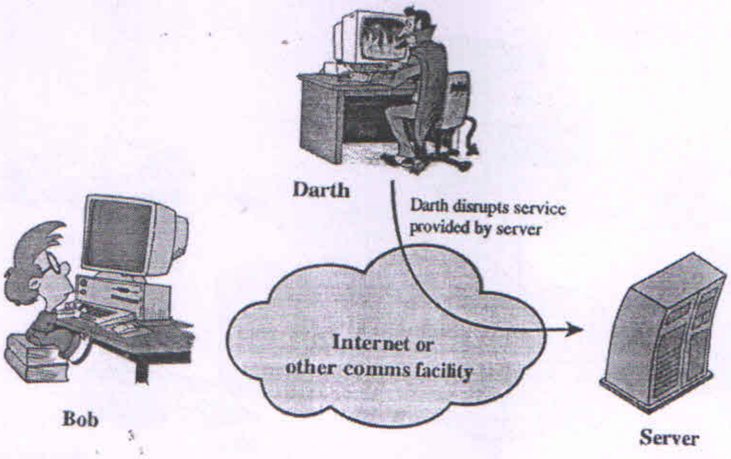

Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

Fig. 5: Modification of messages

- The **denial of service** prevents or inhibits the normal use or management of communications facilities represented in Fig. 6


Darth
Darth disrupts service provided by server
Bob
Internet or other comms facility
Server

Marks Distribution:
Explained properly both the attacks with all its sub categories with diagram ------ 5mks
Explained properly any one attack with all its sub categories with diagram ----- 2.5mks
Explained properly both the attacks with all its sub categories without diagram --- 3mks
Explained properly any one attack with all its sub categories without diagram--- 1.5mks

Q2

Marks Distribution:
Explained Blowfish Algorithm properly without diagram ----------- 07mks
Explained Blowfish Algorithm properly with diagram ----------- 10mks

10

OR

Marks Distribution:
Explain Diffie Hellman Key Exchange algorithm ---------------- 07mks
Solve one correct example of it----------------- 03nks

Q3

A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. Typically the signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message.

10

ElGamal signature scheme:

The ElGamal signature scheme involves the use of the private key for encryption and the public key for decryption. 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 $0 \leq m \leq q - 1$. A then forms a digital signature as follows.

1. Choose a random integer K such that $1 \leq K \leq q - 1$ 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:

What are the Digital Signatures?-- 02 mks

Explained properly ElGamal signature scheme with all formulae correct----------- 08mks

Q4 (a) 10

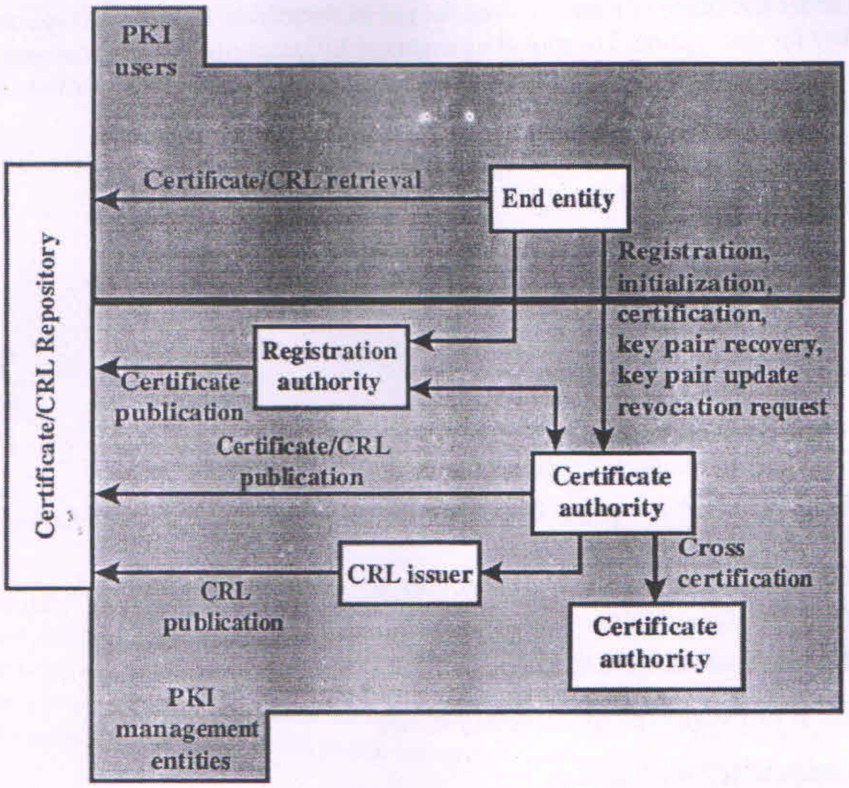

PKI users
Certificate/CRL retrieval
End entity
Registration, initialization, certification, key pair recovery, key pair update revocation request
Certificate/CRL Repository
Registration authority
Certificate publication
Certificate/CRL publication
Certificate authority
CRL issuer
Cross certification
CRL publication
Certificate authority
PKI management entities

Figure 14.16 PKIX Architectural Model

Figure 14.16 shows the interrelationship among the key elements of the PKIX model. These elements are • End entity: A generic term used to denote end users, devices (e.g., servers, routers), or any other entity that can be identified in the subject field of a public key certificate. End entities typically consume and/or support PKI-related services.

• **Certification authority (CA):** The issuer of certificates and (usually) certificate revocation lists (CRLs). It may also support a variety of administrative functions, although these are often delegated to one or more Registration Authorities.

- **Registration authority (RA):** An optional component that can assume a number of administrative functions from the CA.The RA is often associated with the end entity registration process but can assist in a number of other areas as well.
- **CRL issuer:** An optional component that a CA can delegate to publish CRLs.

- **Repository:** A generic term used to denote any method for storing certificates and CRLs so that they can be retrieved by end entities.

PKIX Management Functions

PKIX identifies a number of management functions that potentially need to be supported by management protocols. These are indicated in Figure 14.16 and include the following:

- **Registration:** This is the process whereby a user first makes itself known to a CA prior to that CA issuing a certificate or certificates for that user. Registration begins the process of enrolling in a PKI.
- **Initialization:** Before a client system can operate securely, it is necessary to install key materials that have the appropriate relationship with keys stored elsewhere in the infrastructure. For example, the client needs to be securely initialized with the public key and other assured information of the trusted CA(s), to be used in validating certificate paths.
- **Certification:** This is the process in which a CA issues a certificate for a user's public key, returns that certificate to the user's client system, and/or posts that certificate in a repository.
- **Key pair recovery**: Key pairs can be used to support digital signature creation and verification, encryption and decryption, or both. When a key pair is used for encryption/decryption, it is important to provide a mechanism to recover the necessary decryption keys when normal access to the keying material is no longer possible, otherwise it will not be possible to recover the encrypted data.
- **Key pair update:** All key pairs need to be updated regularly and new certificates issued. Update is required when the certificate lifetime expires and as a result of certificate revocation.
- **Revocation request:** An authorized person advises a CA of an abnormal situation requiring certificate revocation. Reasons for revocation include private key compromise, change in affiliation, and name change.
- **Cross certification:** Two CAs exchange information used in establishing a cross-certificate. A cross-certificate is a certificate issued by one CA to another CA that contains a CA signature key used for issuing certificates.

PKIX Management Protocols:

The PKIX working group has defines two alternative management protocols between

PKIX entities that support the management functions listed in the preceding subsection. It defines the Certificate Management Protocols (CMP). Within CMP, each of the management functions is explicitly identified by specific protocol exchanges. CMP is designed to be a flexible protocol able to accommodate a variety of technical, operational, and business models.

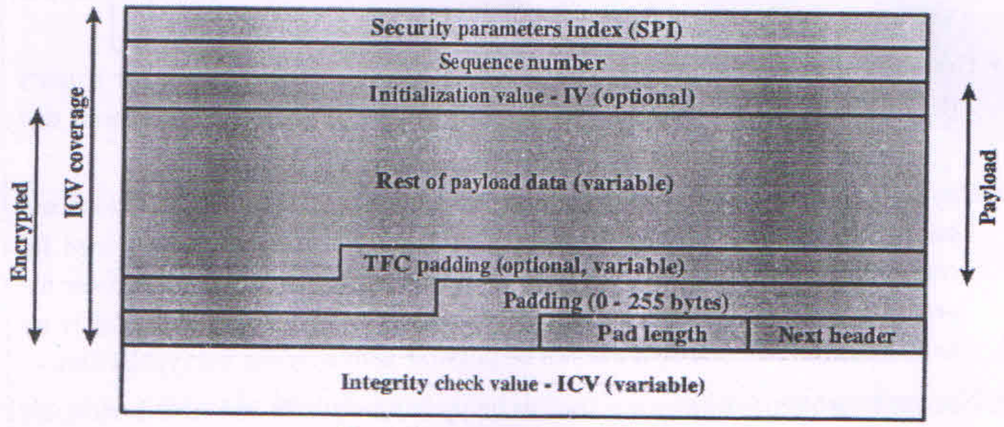
Marks Distribution:

PKIX Architectural Model with diagram -------------------- 04mks

PKIX Management Functions ------------------------------ 04mks

PKIX Management Protocols ------------------------------- 02mks

OR


Security parameters index (SPI)
Sequence number
Initialization value - IV (optional)
Rest of payload data (variable)
TFC padding (optional, variable)
Padding (0 - 255 bytes)
Pad length
Next header
Integrity check value - ICV (variable)
Encrypted
ICV coverage
Payload

(b) Substructure of payload data

Figure 19.5 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.
- 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:

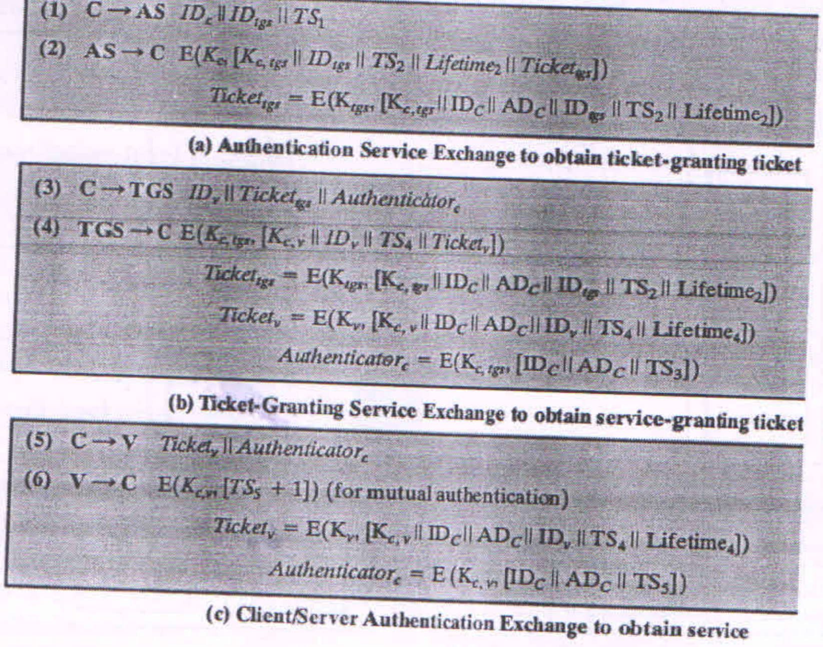
Explained properly ESP Packet Format with diagram -------- 10 mks

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

Q4
(b)

10

Table 15.1 Summary of Kerberos Version 4 Message Exchanges



(1) $C \rightarrow AS \quad ID_c \| ID_{tgs} \| TS_1$

(2) $AS \rightarrow C \quad E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) $C \rightarrow TGS \quad ID_v \| Ticket_{tgs} \| Authenticator_c$

(4) $TGS \rightarrow C \quad E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) $C \rightarrow V \quad Ticket_v \| Authenticator_c$

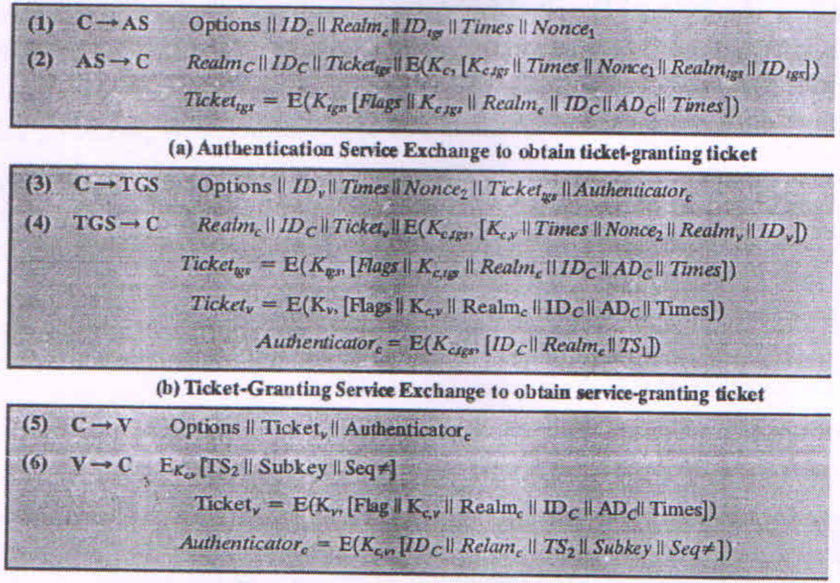
(6) $V \rightarrow C \quad E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,v}, [ID_C \| AD_C \| TS_5])$

(c) Client/Server Authentication Exchange to obtain service

Table 15.3 Summary of Kerberos Version 5 Message Exchanges



(1) C → AS $\quad$ $\text{Options} \| ID_c \| Realm_c \| ID_{tgs} \| Times \| Nonce_1$

(2) AS → C $\quad$ $Realm_C \| ID_C \| Ticket_{tgs} \| \text{E}(K_c, [K_{c,tgs} \| Times \| Nonce_1 \| Realm_{tgs} \| ID_{tgs}])$

$$Ticket_{tgs} = \text{E}(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) C → TGS $\quad$ $\text{Options} \| ID_v \| Times \| Nonce_2 \| Ticket_{tgs} \| Authenticator_c$

(4) TGS → C $\quad$ $Realm_c \| ID_C \| Ticket_v \| \text{E}(K_{c,tgs}, [K_{c,v} \| Times \| Nonce_2 \| Realm_v \| ID_v])$

$$Ticket_{tgs} = \text{E}(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$$

$$Ticket_v = \text{E}(\text{K}_v, [\text{Flags} \| \text{K}_{c,v} \| \text{Realm}_c \| \text{ID}_C \| \text{AD}_C \| \text{Times}])$$

$$Authenticator_c = \text{E}(K_{c,tgs}, [ID_C \| Realm_c \| TS_1])$$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) C → V $\quad$ $\text{Options} \| \text{Ticket}_v \| \text{Authenticator}_c$

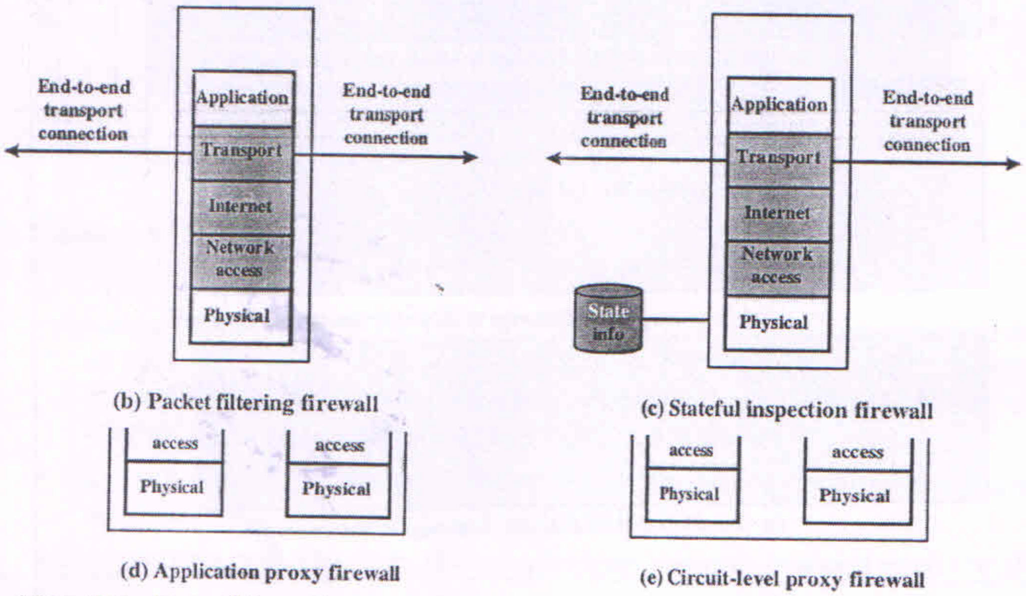
(6) V → C $\quad$ $\text{E}_{K_{c,v}}[\text{TS}_2 \| \text{Subkey} \| \text{Seq}\neq]$

$$\text{Ticket}_v = \text{E}(\text{K}_v, [\text{Flag} \| \text{K}_{c,v} \| \text{Realm}_c \| \text{ID}_C \| \text{AD}_C \| \text{Times}])$$

$$Authenticator_c = \text{E}(K_{c,v}, [ID_C \| Relam_c \| TS_2 \| Subkey \| Seq\neq])$$

(c) Client/Server Authentication Exchange to obtain service

Q5 a) 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., 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	