

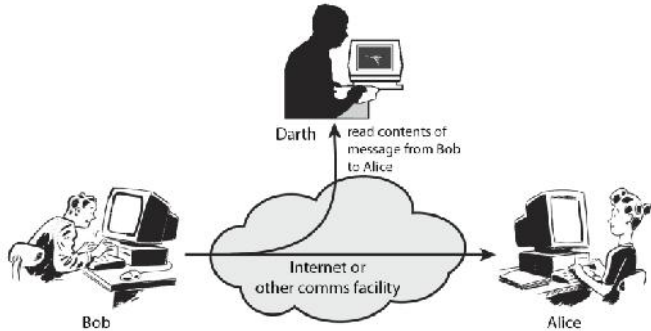
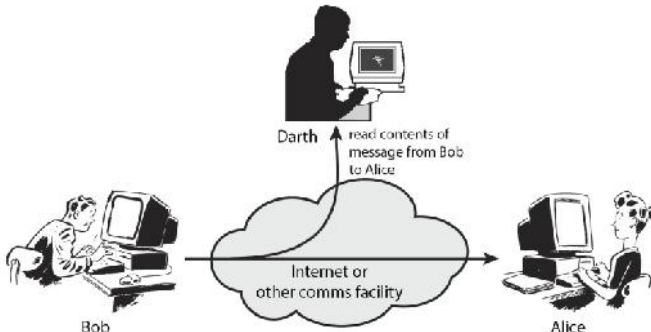
Internal Assessment Test 11- May 2017 SCHEME OF EVALUATION

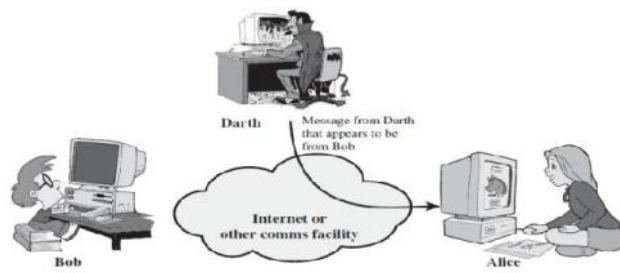
Sub: Information Network Security
Date: 10/05/2017 **Duration:** 90 mins **Max Marks:** 50 **Sem:** VIII

Code: 10CS835
Branch: CSE

Note : Answer any 5 questions

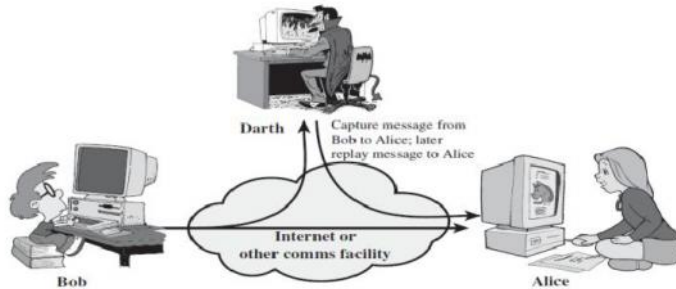
Total marks: 50

	Answer any 5 full questions	Marks	OBE	
			CO	RBT
1	<p>Explain in details the different security attacks? What are the difference between Active and Passive attacks</p> <p>Security Attacks: Security attacks, used both in X.800 and RFC 2828, are classified as a) passive attacks b) active attacks.</p> <p>[Definition with types and diagram] 3M</p> <p>A passive attack attempts to learn or make use of information from the system but does not affect system resources.</p> <p>Two types of passive attacks are release of message contents and traffic analysis.</p> <p>1) Release of message Contents</p>  <p>2) Traffic analysis.</p>  <p>[Definition with types and diagrams] 5M</p> <ul style="list-style-type: none"> ➤ 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 A masquerade attack usually includes one of the other forms of active attack. 	[10]	CO5	L4



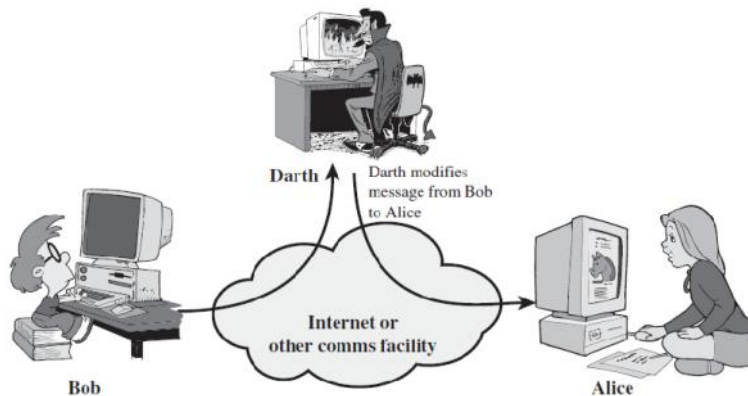
(a) Masquerade

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



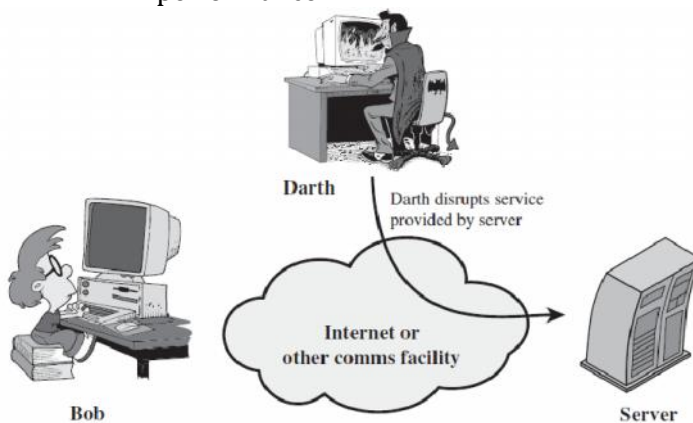
(b) Replay

- **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.



(c) Modification of messages

- The **denial of service** prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target. Another form of service denial is the disruption of an entire network—either by disabling the network or by overloading it with messages so as to degrade performance.



(d) Denial of service

[Difference between Active and Passive attacks Mention any Two] 2M

Passive Attacks	Active attacks
It is indirect attack	It is direct attack
Very difficult to detect because they do not involve any alteration of data	Comparatively not very difficult to detect
Measures are available to prevent their success, usually by means of encryption	Quite difficult to prevent absolutely because it requires physical protection of all communication facilities and paths at all times
Involves eavesdropping on, or monitoring of, transmission	Involve some modification of the data stream or the creation of a false stream
Two types → release of message contents and traffic analysis	Four categories → masquerade, replay, modification of messages and denial of service
Goal → prevention rather than detection	Goal → detect and recover from any disruption or delays caused by them

2

Explain the Security Services and Mechanisms w.r.t X.800
[There are 5 Security Service each Carry 1M]

5*1=5M

[10]

CO5

L4

Table 1.2 Security Services (X.800)

<p style="text-align: center;">AUTHENTICATION</p> <p>The assurance that the communicating entity is the one that it claims to be.</p> <p>Peer Entity Authentication Used in association with a logical connection to provide confidence in the identity of the entities connected.</p> <p>Data-Origin Authentication In a connectionless transfer, provides assurance that the source of received data is as claimed.</p> <p style="text-align: center;">ACCESS CONTROL</p> <p>The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).</p> <p style="text-align: center;">DATA CONFIDENTIALITY</p> <p>The protection of data from unauthorized disclosure.</p> <p>Connection Confidentiality The protection of all user data on a connection.</p> <p>Connectionless Confidentiality The protection of all user data in a single data block.</p> <p>Selective-Field Confidentiality The confidentiality of selected fields within the user data on a connection or in a single data block.</p> <p>Traffic-Flow Confidentiality The protection of the information that might be derived from observation of traffic flows.</p>	<p style="text-align: center;">DATA INTEGRITY</p> <p>The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).</p> <p>Connection Integrity with Recovery Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.</p> <p>Connection Integrity without Recovery As above, but provides only detection without recovery.</p> <p>Selective-Field Connection Integrity Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.</p> <p>Connectionless Integrity Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.</p> <p>Selective-Field Connectionless Integrity Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.</p> <p style="text-align: center;">NONREPUDIATION</p> <p>Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.</p> <p>Nonrepudiation, Origin Proof that the message was sent by the specified party.</p> <p>Nonrepudiation, Destination Proof that the message was received by the specified party.</p>
--	--

There are 5 Security Mechanism each Carry 1M]

5*1=5M

Table L.3 Security Mechanisms (X.800)

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
<p>May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.</p>	<p>Mechanisms that are not specific to any particular OSI security service or protocol layer.</p>
<p>Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.</p>	<p>Trusted Functionality That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).</p>
<p>Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).</p>	<p>Security Label The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.</p>
<p>Access Control A variety of mechanisms that enforce access rights to resources.</p>	<p>Event Detection Detection of security-relevant events.</p>
<p>Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.</p>	<p>Security Audit Trail Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.</p>
<p>Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.</p>	<p>Security Recovery Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.</p>
<p>Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.</p>	
<p>Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.</p>	
<p>Notarization The use of a trusted third party to assure certain properties of a data exchange.</p>	

3

With the neat diagram explain the Kerberos version 4 message exchanges

KERBEROS [Definition 2 M]

Kerberos is a key distribution and user authentication service developed at MIT. In particular, the following three threats exist:

1. A user may gain access to a particular workstation and pretend to be another user operating from that workstation.
2. A user may alter the network address of a workstation so that the requests sent from the altered workstation appear to come from the impersonated workstation.
3. A user may eavesdrop on exchanges and use a replay attack to gain entrance to a server or to disrupt operations. Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. Kerberos relies exclusively on symmetric encryption, making no use of public-key encryption.

Kerberos Version 4

Version 4 of Kerberos makes use of DES, in a rather elaborate protocol, to provide the authentication service.

- ❖ **A Simple Authentication Dialogue**
- ✓ In an unprotected network environment, any client can apply to any server for service.
- ✓ The obvious security risk is that of impersonation.
- ✓ An opponent can pretend to be another client and obtain unauthorized privileges on server machines.

[10]

CO6

L2

- ✓ To counter this threat, servers must be able to confirm the identities of clients who request service.
- ✓ An alternative is to use an **authentication server (AS)** that knows the passwords of all users and stores these in a centralized database.

(1) $C \rightarrow AS: ID_C || P_C || ID_V$

(2) $AS \rightarrow C: Ticket$

(3) $C \rightarrow V: ID_C || Ticket$

$Ticket = E(K_v, [ID_C || AD_C || ID_V])$

In this scenario, the user logs on to a workstation and requests access to server V.

- The client module C in the user's workstation requests the user's password and then sends a message to the AS that includes the user's ID, the server's ID, and the user's password.
- The AS checks its database to see if the user has supplied the proper password for this user ID and whether this user is permitted access to server V.
- If both tests are passed, the AS accepts the user as authentic and must now convince the server that this user is authentic.
- To do so, the AS creates a **ticket** that contains the user's ID and network address and the server's ID.
- This ticket is encrypted using the secret key shared by the AS and this server.
- This ticket is then sent back to C.
- Because the ticket is encrypted, it cannot be altered by C or by an opponent.
- With this ticket, C can now apply to V for service.
- C sends a message to V containing C's ID and the ticket.
- V decrypts the ticket and verifies that the user ID in the ticket is the same as the unencrypted user ID in the message.
- If these two match, the server considers the user authenticated and grants the requested service.

[Message Exchange 4M]

Once per user logon session:

(1) $C \rightarrow AS: ID_C || ID_{tgs}$

(2) $AS \rightarrow C: E(K_c, Ticket_{tgs})$

Once per type of service:

(3) $C \rightarrow TGS: ID_C || ID_V || Ticket_{tgs}$

(4) $TGS \rightarrow C: Ticket_v$

Once per service session:

(5) $C \rightarrow V: ID_C || Ticket_v$

$Ticket_{tgs} = E(K_{tgs}, [ID_C || AD_C || ID_{tgs} || TS_1 || Lifetime_1])$

$Ticket_v = E(K_v, [ID_C || AD_C || ID_v || TS_2 || Lifetime_2])$

[Diagram with Explanation 4 M]

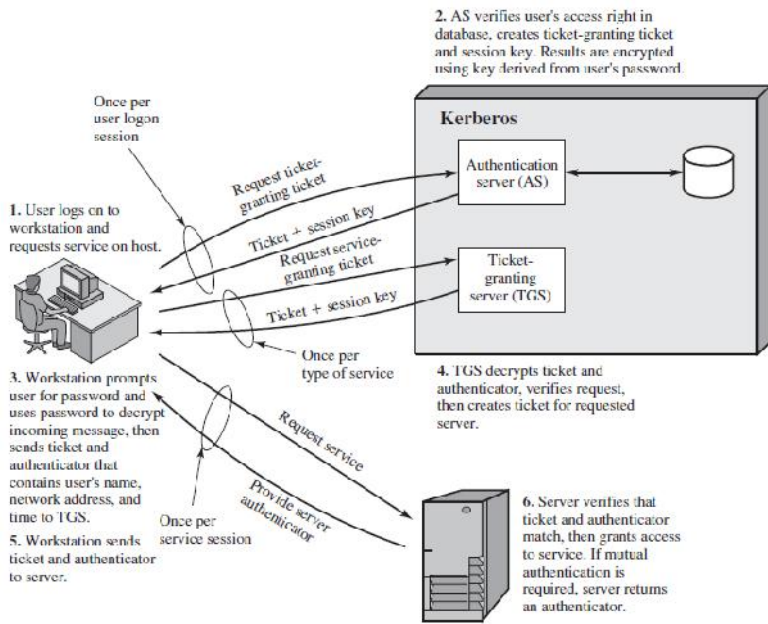
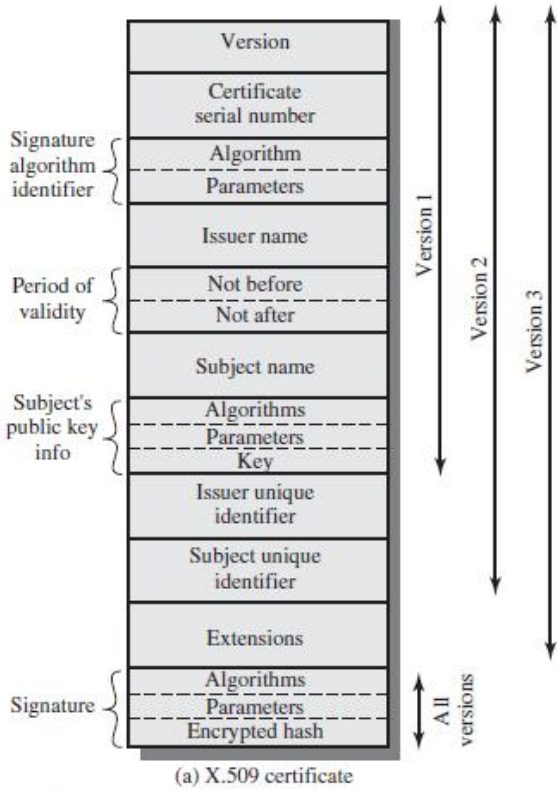


Figure 4.1 Overview of Kerberos

4a

Explain the general format of a X.509 public key certificate

[Diagram with Explanation 4 M+3M]



(a) X.509 certificate

Figure 4.4 X.509 Formats

- **Version:** Differentiates among successive versions of the certificate format; the default is version 1. If the Issuer Unique Identifier or Subject Unique Identifier are present, the value must be version 2. If one or more extensions are present, the version must be version 3.
- **Serial number:** An integer value, unique within the issuing CA, that is unambiguously associated with this certificate.
- **Signature algorithm identifier:** The algorithm used to sign the certificate, together with any associated parameters. Because this information is repeated in the Signature field at the end of the certificate, this field has little, if any, utility.
- **Issuer name:** X.500 name of the CA that created and signed this certificate.
- **Period of validity:** Consists of two dates: the first and last on which the certificate is valid.
- **Subject name:** The name of the user to whom this certificate refers. That is, this certificate certifies the public key of the subject who holds the corresponding private key.
- **Subject's public-key information:** The public key of the subject, plus an identifier of the

[07]

CO6

L4

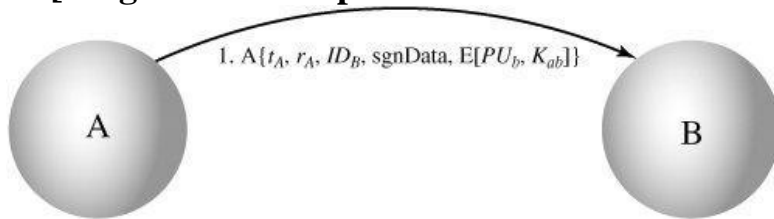
algorithm for which this key is to be used, together with any associated parameters.

- **Issuer unique identifier:** An optional bit string field used to identify uniquely the issuing CA in the event the X.500 name has been reused for different entities.
- **Subject unique identifier:** An optional bit string field used to identify uniquely the subject in the event the X.500 name has been reused for different entities.
- **Extensions:** A set of one or more extension fields. Extensions were added in version 3 and are discussed later in this section.
- **Signature:** Covers all of the other fields of the certificate; it contains the hash code of the other fields encrypted with the CA's private key. This field includes the signature algorithm identifier.

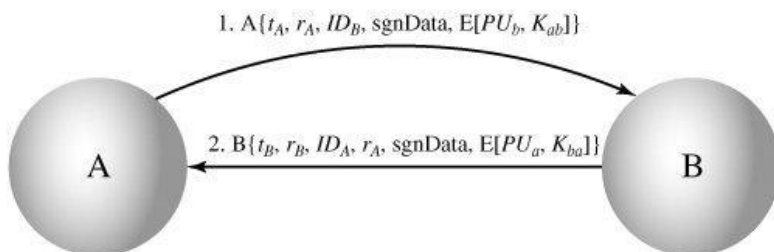
4b Explain the different Authentication procedures of X.509

[Diagram with Explanation Each Carries 1M]

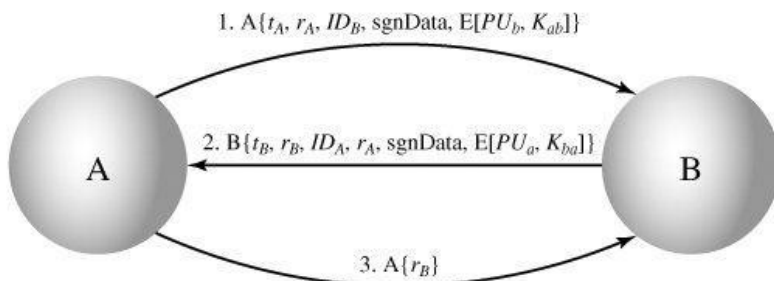
3*1=3M



(a) One-way authentication



(b) Two-way authentication



(c) Three-way authentication

alternative authentication procedures:

- One-Way Authentication
- Two-Way Authentication
- Three-Way Authentication

All use public-key signatures.

❖ **One-way Authentication**

1 message (A->B) used to establish

- the identity of A and that message is from A
- message was intended for B
- integrity & originality of message

❖ **Two-way Authentication**

2 messages (A->B, B->A) which also establishes in addition:

- the identity of B and that reply is from B
- that reply is intended for A
- integrity & originality of reply

[03]

CO6

L4

❖ **Three-way Authentication**

3 messages (A->B, B->A, A->B) which enables above authentication without synchronized clocks

5a

Describe PGP Message Generation from user A and user B with a block schematic diagram?

[Diagram with Explanation of steps 4M+2M]

3+4=6M

PGP message Generation

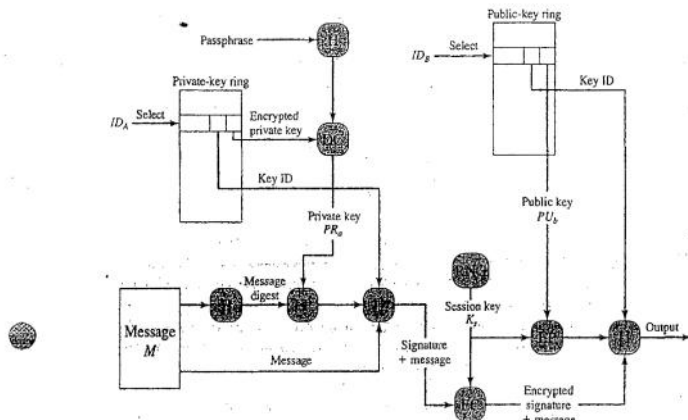


Figure 5.5 PGP Message Generation (from User A to User B; no compression or radix 64 conversion)

* The sending PGP entity performs the following steps:

1. Signing the message:

- a) PGP retrieves the sender's private key from the private key ring using your_userid as an index. If your_userid is not provided in the command, the first private key on the ring is retrieved.
- b) PGP prompts the user for the passphrase to recover the unencrypted private key.
- c) The signature component of the message is constructed.

[06]

CO6

L2

9. Encrypting the message.

- a) PGP generates a session key and encrypts the message.
- b) PGP retrieves the recipient's public key from the public-key ring using her-userid as an index.
- c) The session key component of the message is constructed.

5b What is S/MIME? Mentions the functions provided by S/MIME

[Definition carries 1M]

1M

S/MIME is a security enhancement to the MIME Internet email format standard, based on technology from RSA data security.

- > S/MIME will emerge as the industry standard for commercial and organizational use.
- > PGP will remain the choice for personal e-mail security for many users.

[Mention any 3 Function each carries 1M]

3*1=3M

[04]

CO6

L1

* S/MIME provides the following functions.

- Enveloped Data: Consists of encrypted contents and encrypted session keys for recipients.
- Signed Data: A digital signature is formed by taking the message digest of the content to be signed and then encrypting that ~~the~~ with the private key of the signer.
- clear-signed Data: Signed, but not encrypted.
- Signed and Enveloped Data: Signed-only and encrypted-only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted.

6 What are the five principal services provided by PGP? Explain the operational description of PGP?

[Diagram with Explanation 5 Operation each Carries 2M] 5*2=10M

[10]

CO6

L1

- | | | | |
|--|--|--|--|
| <ol style="list-style-type: none">1. Authentication.2. Confidentiality3. Compression.4. Email compatibility.5. Segmentation. | | | |
|--|--|--|--|

69 135

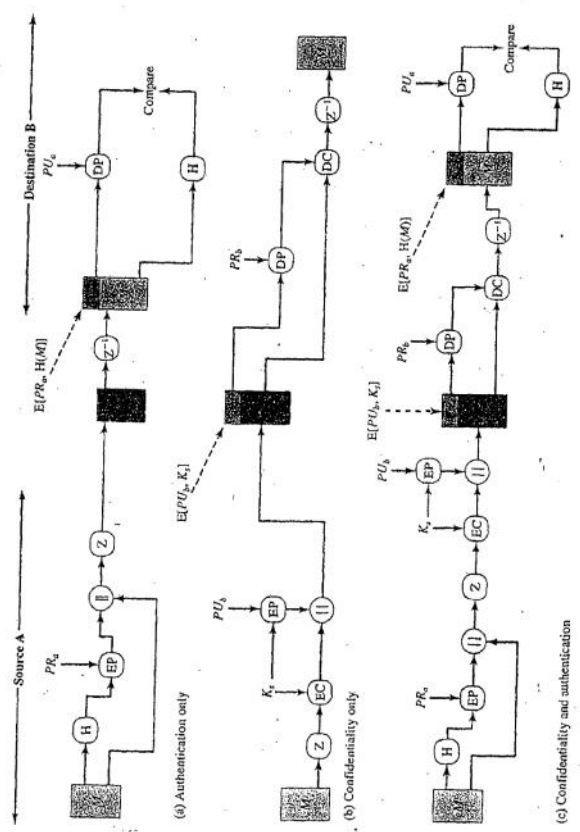


Figure 5.1 PGP Cryptographic Functions

7a Define IP Security ? With neat diagram and Mention the benefits of IPsec
[Diagram with Explanation Carries 2M] **2M**

[05]

CO6

L2

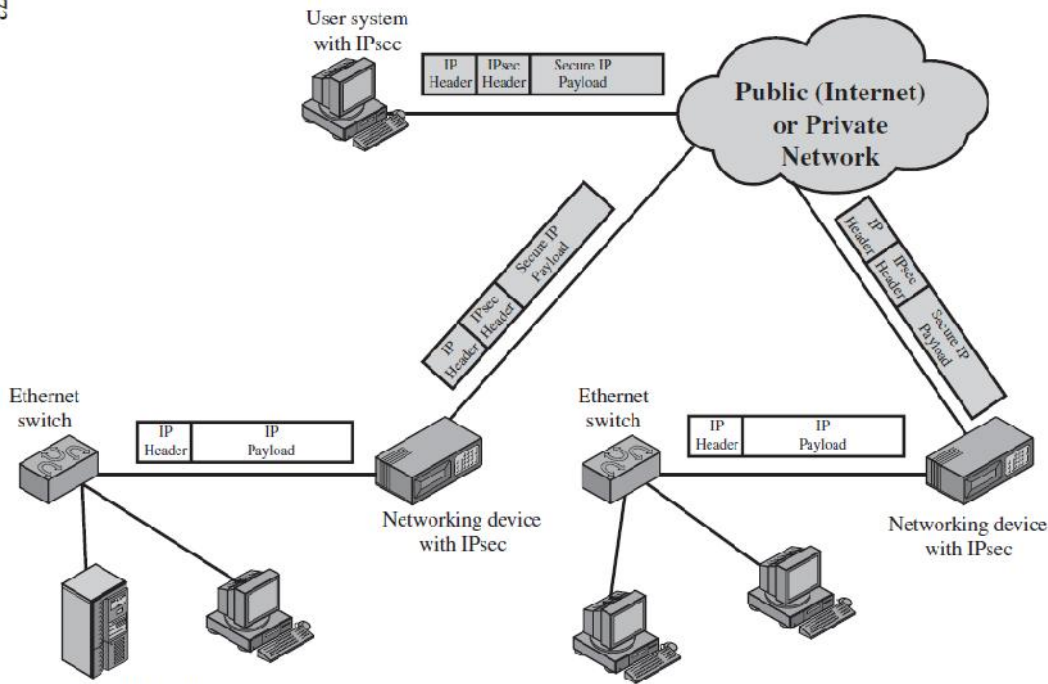


Figure 8.1 An IP Security Scenario

[Mention any 3 Benefits each carries 1M]**3*1=3M**

- When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.
- IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.
- IPsec is below the transport layer (TCP, UDP) and so is transparent to applications.
- IPsec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.
- IPsec can provide security for individual users if needed.

7b Define Security Associations? And explain the SA parameters

[Definition carries 1M]**1M**

An association is a one-way logical connection between a sender and a receiver that affords security services to the traffic carried on it.

[Mention any 8 parameter each carries 0.5M]**8*0.5=4M****Security Association Database (SA Parameter)**

A security association is normally defined by the following parameters in an SAD entry. • **Security Parameter Index:** A 32-bit value selected by the receiving end of an SA to uniquely identify the SA.

- **Sequence Number Counter:** A 32-bit value used to generate the Sequence Number field in AH or ESP headers.
- **Sequence Counter Overflow:** A flag indicating whether overflow of the Sequence Number Counter should generate an auditable event and prevent further transmission of packets on this SA
- **Anti-Replay Window:** Used to determine whether an inbound AH or ESP packet is a replay.
- **AH Information:** Authentication algorithm, keys, key lifetimes, and related parameters being used with AH
- **ESP Information:** Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP
- **Lifetime of this Security Association:** A time interval or byte count after which an SA must be replaced with a new SA or terminated, plus an indication of which of these actions should occur.
- **IPsec Protocol Mode:** Tunnel, transport, or wildcard.
- **Path MTU:** Any observed path maximum transmission unit and aging variables

[05]

CO6

L2