IAT-3 SOLUTION

Sub: Cryptography

1. a. **What are the different ways to authenticate a user's identity? Explain replay attack and how to handle replay attack.**

Ans: There are four general means of authenticating a user's identity, which can be used alone or in combination:
1. Something the individual knows: Examples include a password, a personal identification number (PIN), or answers to a prearranged set of questions.
2. Something the individual possesses: Examples include cryptographic keys, electronic keycards, smart cards, and physical keys. This type of authenticator is referred to as a token.
3. Something the individual is (static biometrics): Examples include recognition by fingerprint, retina, and face.
4. Something the individual does (dynamic biometrics): Examples include recognition by voice pattern, handwriting characteristics, and typing rhythm.

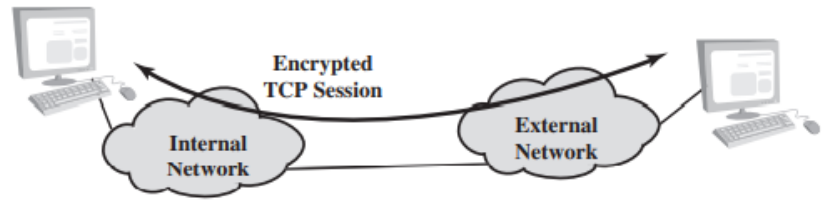
REPLAY ATTACK:
Central to the problem of authenticated key exchange are two issues: confidentiality and timeliness.
1. The timeliness issue, is important because of the threat of message replays. Such replays, at worst, could allow an opponent to compromise a session key or successfully impersonate another party. At minimum, a successful replay can disrupt operations by presenting parties with messages that appear genuine but are not.
The following examples of replay attacks:
1. The simplest replay attack is one in which the opponent simply copies a message and replays it later.
2. An opponent can replay a timestamped message within the valid time window. If both the original and the replay arrive within then time window, this incident can be logged.
3. As with example (2), an opponent can replay a timestamped message within the valid time window, but in addition, the opponent suppresses the original message. Thus, the repetition cannot be detected.
4. Another attack involves a backward replay without modification. This is a replay back to the message sender. This attack is possible if symmetric encryption is used and the sender cannot easily recognize the difference between messages sent and messages received on the basis of content.

One approach to coping with replay attacks is to attach a sequence number to each message used in an authentication exchange. A new message is accepted only if its sequence number is in the proper order. The difficulty with this approach is that it requires each party to keep track of the last sequence number for each claimant it has dealt with. Because of this overhead, sequence numbers are generally not used for authentication and key exchange.
Instead, one of the following two general approaches is used:

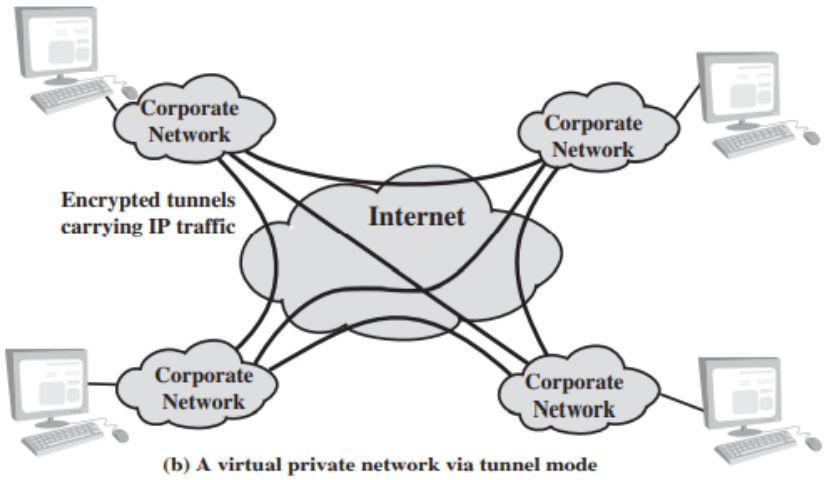
• **Timestamps:** Party A accepts a message as fresh only if the message contains a timestamp that, in A's judgment, is close enough to A's knowledge of current time. This approach requires that clocks among the various participants be synchronized.
• **Challenge/response:** Party A, expecting a fresh message from B, first sends B a nonce (challenge) and requires that the subsequent message (response) received from B contain the correct nonce value.

1. b. **Explain the transport and the tunnel mode encryption technique with neat diagram.**

Ans: Figure 20.7 shows two ways in which the IPsec ESP service can be used. In the upper part of the figure, encryption (and optionally authentication) is provided directly between two hosts. Figure 20.7b shows how tunnel mode operation can be used to set up a virtual private network. In this example, an organization has four private networks interconnected across the Internet



(a) Transport-level security

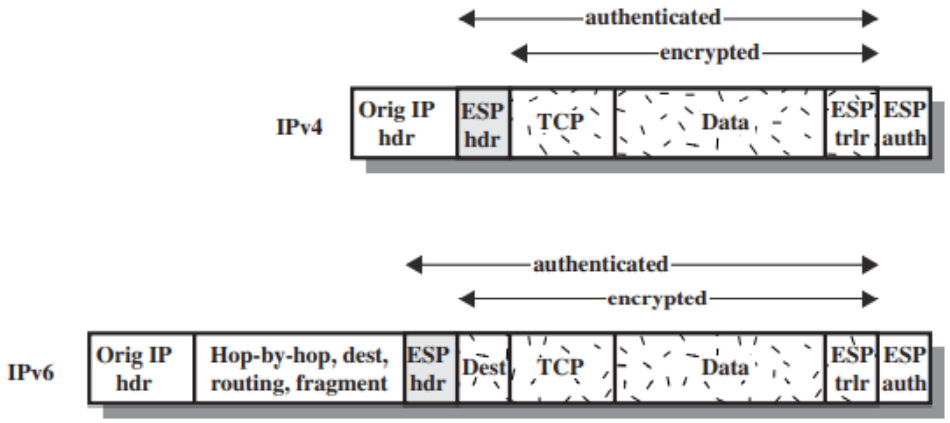


(b) A virtual private network via tunnel mode

Figure 20.7 Transport-Mode versus Tunnel-Mode Encryption

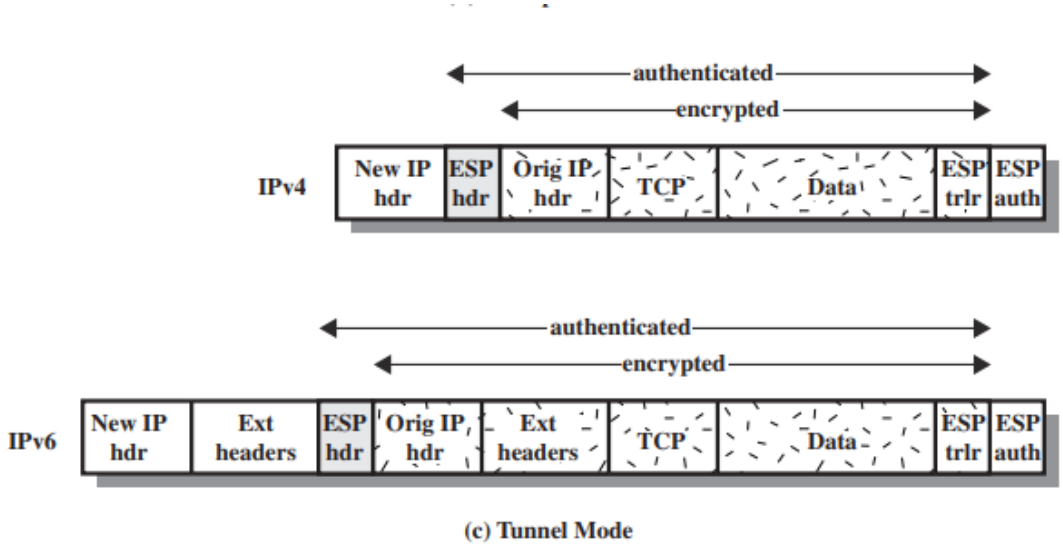
TRANSPORT MODE ESP: Transport mode ESP is used to encrypt and optionally authenticate the data carried by IP (e.g., a TCP segment), as shown in Figure 20.8b. For this mode using IPv4, the ESP header is inserted into the IP packet immediately prior to the

transport-layer header (e.g., TCP, UDP, ICMP), and an ESP trailer (Padding, Pad Length, and Next Header fields) is placed after the IP packet. If authentication is selected, the ESP Authentication Data field is added after the ESP trailer. The entire transport-level segment plus the ESP trailer is encrypted. Authentication covers all of the ciphertext plus the ESP header.



(b) Transport Mode

TUNNEL MODE ESP: Tunnel mode ESP is used to encrypt an entire IP packet (Figure 20.8c). For this mode, the ESP header is prefixed to the packet and then the packet plus the ESP trailer is encrypted. This method can be used to counter traffic analysis. Because the IP header contains the destination address and possibly source routing directives and hop-by-hop option information, it is not possible simply to transmit the encrypted IP packet prefixed by the ESP header. Intermediate routers would be unable to process such a packet. Therefore, it is necessary to encapsulate the entire block (ESP header plus ciphertext plus Authentication Data, if present) with a new IP header that will contain sufficient information for routing but not for traffic analysis.



(c) Tunnel Mode

Q.2. How the sequence of messages exchanged between the client, the Kerberos servers, and the requested servers? Explain with diagrams in Kerberos version 4.

Ans: 1. Version 4 of Kerberos makes use of DES, in a rather elaborate protocol, to provide the authentication service.
2. The table below shows the technique for distributing the session key. As before, the client sends a message to the AS requesting access to the TGS.
3. The AS responds with a message, encrypted with a key derived from the user's password (Kc), that contains the ticket. The encrypted message also contains a copy of the session key, Kc, tgs, where the subscripts indicate that this is a session key for C and TGS.
4. Because this session key is inside the message encrypted with Kc, only the user's client can read it. The same session key is included in the ticket, which can be read only by the TGS. Thus, the session key has been securely delivered to both C and the TGS.

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

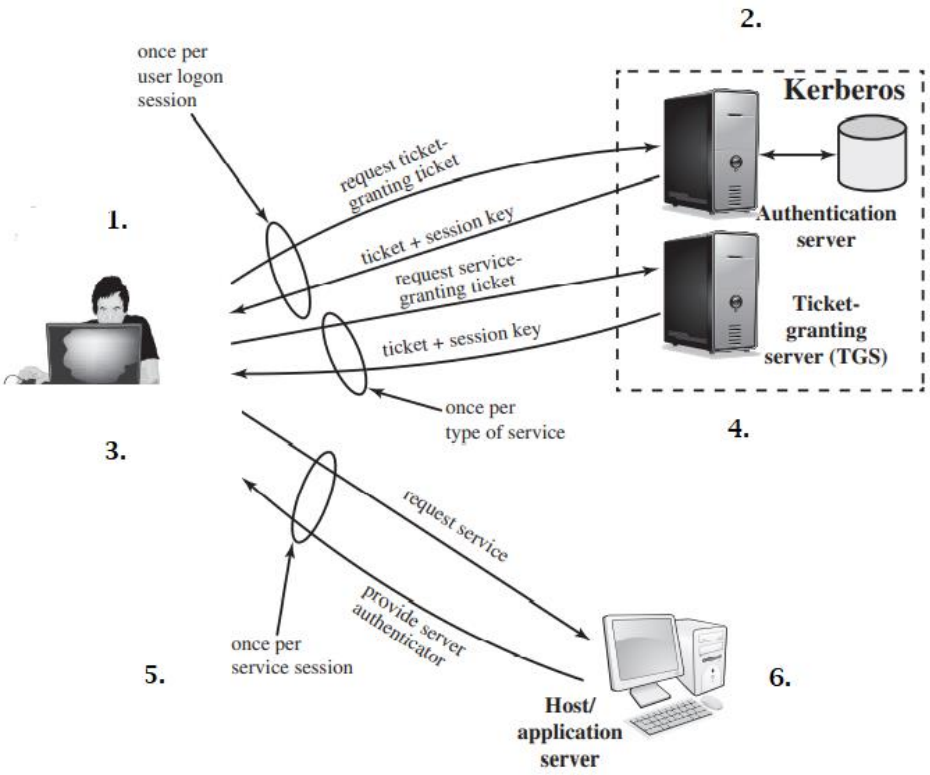


Figure 15.1 Overview of Kerberos

1. User logs on to workstation and requests service on host.

2. AS verifies user's access right in database, and creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.

3. Workstation prompts user for password to decrypt incoming message, and then send ticket and authenticator that contains user's name, network address, and time to TGS.

4. TGS decrypts ticket and authenticator, verifies request, and then creates ticket for requested application server.

5. Workstation sends ticket and authenticator to host.

6. Host verifies that ticket and authenticator match, and then grants access to service. If mutual authentication is required, server returns an authenticator.

Q.3. **Explain the IP traffic processing (outbound and inbound packets).**

Ans: IPsec is executed on a packet-by-packet basis.

2. When IPsec is implemented, each outbound IP packet is processed by the IPsec logic before transmission, and each inbound packet is processed by the IPsec logic after reception and before passing the packet contents on to the next higher layer (e.g., TCP or UDP).

Outbound Packets Figure 20.3 highlights the main elements of IPsec processing for outbound traffic. A block of data from a higher layer, such as TCP, is passed

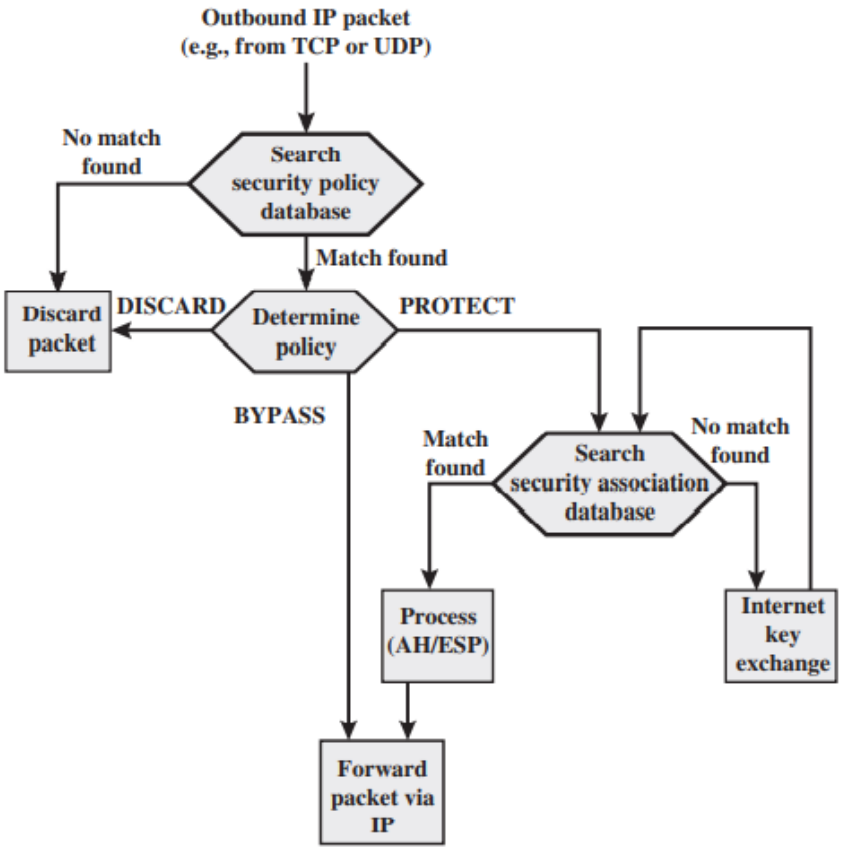


Figure 20.3 Processing Model for Outbound Packets

down to the IP layer and an IP packet is formed, consisting of an IP header and an IP body. Then the following steps occur:

1. IPsec searches the SPD for a match to this packet.
2. If no match is found, then the packet is discarded and an error message is generated.
3. If a match is found, further processing is determined by the first matching entry in the SPD. If the policy for this packet is DISCARD, then the packet is discarded. If the policy is BYPASS, then there is no further IPsec processing; the packet is forwarded to the network for transmission.
4. If the policy is PROTECT, then a search is made of the SAD for a matching entry. If no entry is found, then IKE is invoked to create an SA with the appropriate keys and an entry is made in the SA.
5. The matching entry in the SAD determines the processing for this packet. Either encryption, authentication, or both can be performed, and either transport or tunnel mode can be used. The packet is then forwarded to the network for transmission.

Inbound Packets Figure 20.4 highlights the main elements of IPsec processing for inbound traffic. An incoming IP packet triggers the IPsec processing. The following steps occur:

1. IPsec determines whether this is an unsecured IP packet or one that has ESP or AH headers/trailers, by examining the IP Protocol field (IPv4) or Next Header field (IPv6).

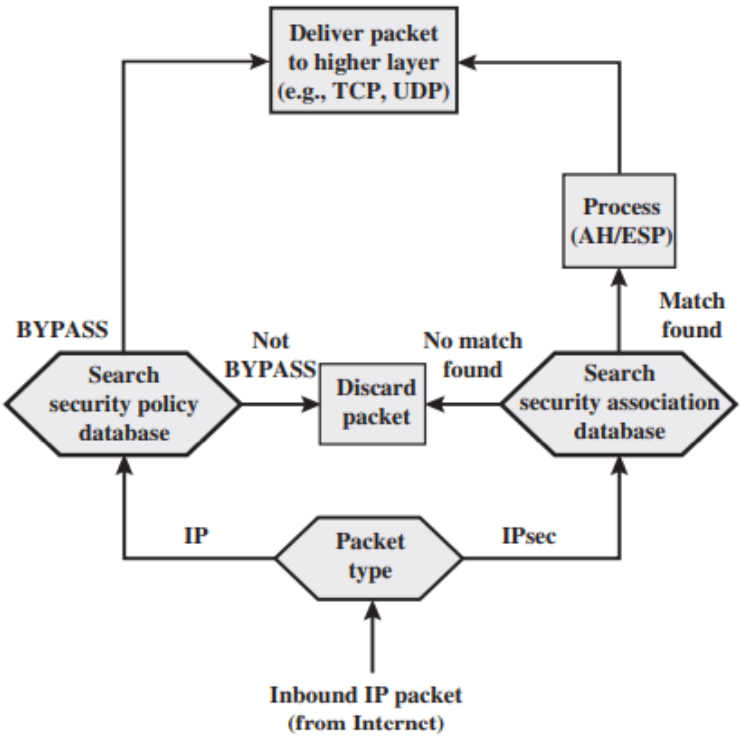


Figure 20.4 Processing Model for Inbound Packets

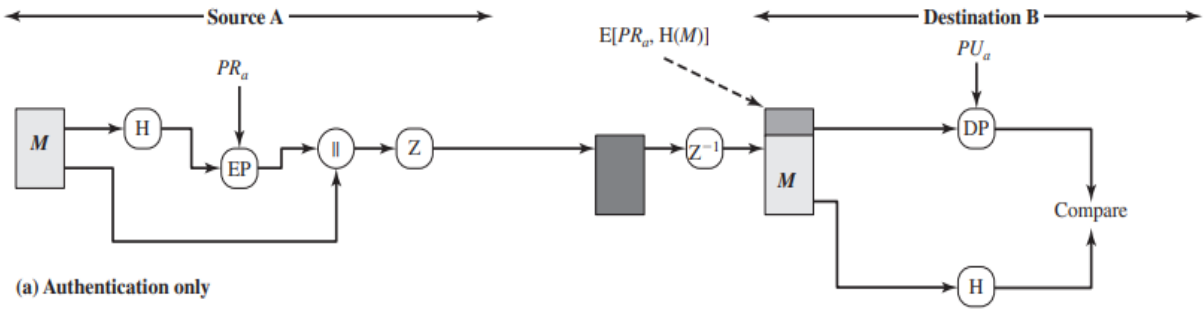
2. If the packet is unsecured, IPsec searches the SPD for a match to this packet. If the first matching entry has a policy of BYPASS, the IP header is processed and stripped off and the packet body is delivered to the next higher layer, such as TCP. If the first matching entry has a policy of PROTECT or DISCARD, or if there is no matching entry, the packet is discarded.
3. For a secured packet, IPsec searches the SAD. If no match is found, the packet is discarded. Otherwise, IPsec applies the appropriate ESP or AH processing. Then, the IP header is processed and stripped off and the packet body is delivered to the next higher layer, such as TCP.

Q.4. **How does PGP provide authentication and confidentiality for email services and for file transfer applications? Draw the block diagram and explain the components.**

Ans: **Authentication:**

Figure below illustrates the digital signature service provided by PGP. This is the digital signature scheme. The sequence is as follows.

1. The sender creates a message.
2. SHA-1 is used to generate a 160-bit hash code of the message.
3. The hash code is encrypted with RSA using the sender's private key, and the result is prepended to the message.
4. The receiver uses RSA with the sender's public key to decrypt and recover the hash code.
5. The receiver generates a new hash code for the message and compares it with the decrypted hash code. If the two match, the message is accepted as authentic.

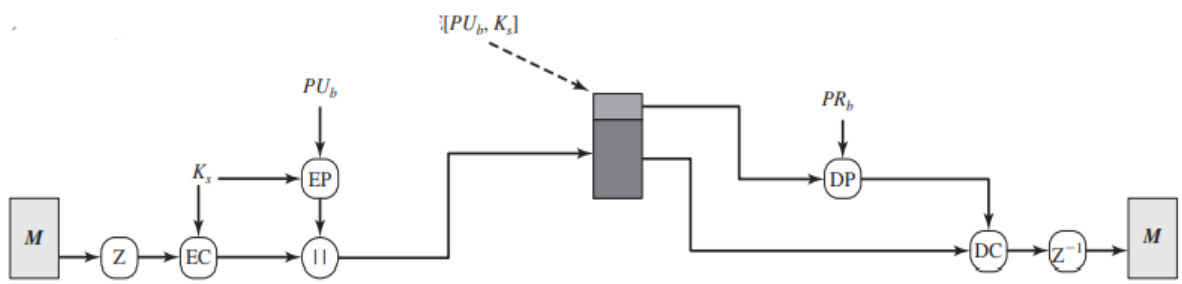


(a) Authentication only

The combination of SHA-1 and RSA provides an effective digital signature scheme. Because of the strength of RSA, the recipient is assured that only the possessor of the matching private key can generate the signature. Because of the strength of SHA-1, the recipient is assured that no one else could generate a new message that matches the hash code and, hence, the signature of the original message. As an alternative, signatures can be generated using DSS/SHA-1

Confidentiality

Another basic service provided by PGP is confidentiality, which is provided by encrypting messages to be transmitted or to be stored locally as files. In both cases, the symmetric encryption algorithm CAST-128 may be used. Alternatively, IDEA or 3DES may be used. The 64-bit cipher feedback (CFB) mode is used.



(b) Confidentiality only

As always, one must address the problem of key distribution. In PGP, each symmetric key is used only once. That is, a new key is generated as a random 128-bit number for each message. Thus, although this is referred to in the documentation as a session key, it is in reality a one-

time key. Because it is to be used only once, the session key is bound to the message and transmitted with it. To protect the key, it is encrypted with the receiver's public key. Figure 19.1b illustrates the sequence, which can be described as follows.

1. The sender generates a message and a random 128-bit number to be used as a session key for this message only.
2. The message is encrypted using CAST-128 (or IDEA or 3DES) with the session key.
3. The session key is encrypted with RSA using the recipient's public key and is prepended to the message.
4. The receiver uses RSA with its private key to decrypt and recover the session key.
5. The session key is used to decrypt the message. As an alternative to the use of RSA for key encryption, PGP provides an option referred to as Diffie-Hellman

Q.5. **Explain the concept of remote user authentication using asymmetric encryption.**

Ans:

Mutual authentication.

-> This protocol assumes that each of two parties is in possession of the current public key of the other.

-> It may not be practical to require this assumption

-> The protocol

A → KDC : $ID_A \| ID_B$

KDC → A : $E(PR_{auth}, [ID_B \| PU_b])$

A → B : $E(PU_b, [N_a \| ID_A])$

B → KDC : $ID_A \| ID_B \| E(PU_{auth}, N_a)$

KDC → B : $E(PR_{auth}, [ID_A \| PU_a]) \| E(PU_b, E(PR_{auth}, [N_a \| K_s \| ID_B]))$

B → A : $E(PU_a, [E(PR_{auth}, [N_a \| K_s \| ID_B]) \| N_b])$

A → B : $E(K_s, N_b)$

-> A says KDC to establish secure connection with B

-> KDC returns A the public key certification of B

-> Using Public key B, A informs to send a nonce to communicate

-> B will ask KDC the public key certification of A and request a session key

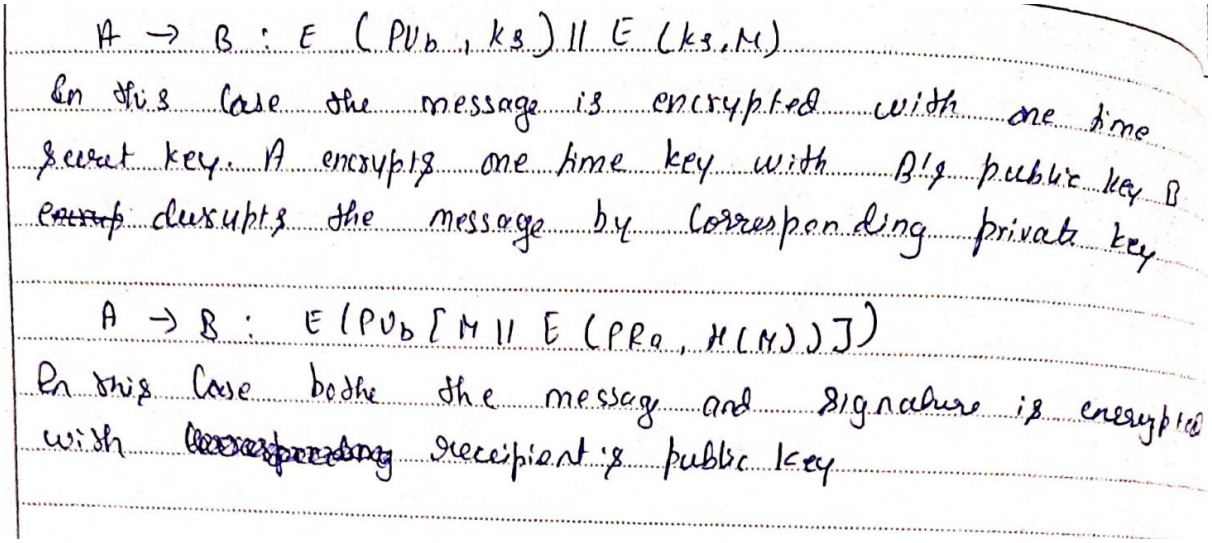
-> KDC returns public key certification of A with the session key K_s hed with Nonce N_a

-> The triple N_a, K_s, ID_B is encrypted with the KDC's private key and Nonce of B is sent to A

-> A sends Encryption of Session & Nonce of B to B

One way authentication:

-> this approaches require that either the sender knows the recipient's public key, the recipient know the senders public key or both

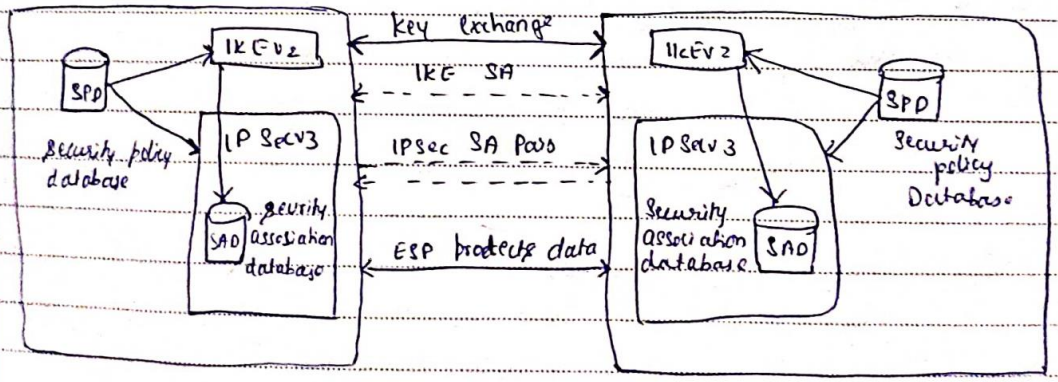


Q.6. **Explain IP Security protocols in detail.**

Ans:

Ans -> The IP Security is a standard suite of protocol between 2 communication points across the IP network that provide data authentication, Integrity and Confidentiality.

-> It also defines the encrypted, decrypted & authenticated packets



Security Associations : -> A key concept that appears in both authentication and confidentiality mechanism for IP is the security association (SA)

-> It uniquely identifies 3 parameters:

- Security parameter index (SPI) : A 32 bit unsigned integer assigned to this SA having logical significance only
- IP destination address : address of destination endpoint of SA

•> Security protocol identifier : it is from outer IP header indicates whether association in an AH or ESP Security association.

Security Association Database :-> It is a central repository containing the activities SAs for both inbound and outbound traffic with each entry defining the parameters for a specific SA

-> SA entry maintains following information

•> Security parameter index : A unique identifier generated by the creator of SA, used to distinguish among SA of IPsec protocol terminating at the same destination node

•> Destination address : address of destination node which SA entry as applied

•> Sequence number : counter for generating sequence number

•> Anti replay window : A counter and mapping information to determine whether a packet is being replayed

•> IP Security protocol : the type of the IP Security protocol which is used to process packet. Either authentication header / Encapsulating Security payload can be specified

•> Algorithm : it is used by IP Security protocol specified by that IP security protocol parameter

•> key : it is used by algorithm

•> SA lifetime : Expressed in either time or byte count. At the expiration of lifetime the SA must be replaced with a new SA and new SPI, or the SA is terminated

•> IPsec : protocol mode of operation. Tunnel mode or Transport mode

Security policy Database :-> It contains a set of rules that determines whether a packet is subject to IPsec processing and governs the processing details

-> Each SPD entry is defined by a set of IP and upper layer protocol field values, called Selectors.

- The following Selectors determine an SPD entry:

• Remote IP Address: This may be single IP address an enumerated list or range of address.

• Local IP Address: This may be single IP address an enumerated list or range of address.

• Next layer protocol: The IP protocol header includes a field that designates the protocol operating over.

• Name: A user's identifier from OS.

• Local & remote ports: These may be individual TCP or UDP port values.