CMR INSTITUTE OF TECHNOLOGY

USN | | | | | | | | | | |

Internal Assesment Test – II

| Sub: | Network and Cyber Security | | Sec | *ALL* | | Code: | 15EC835 |
|---|---|---|---|---|---|---|---|
| Date: | 20 / 04 / 2019 | Duration: | 90 mins | Max Marks: 50 | Sem: VIII | Branch: | ECE |

Scheme of Evaluation

| | Marks | OBE CO | OBE RBT |
|---|---|---|---|
| 1 What is PGP? Explain with neat diagrams the Authentication only, Confidentiality only and confidentiality & authentication with relevant diagrams. | 10 | CO 1 | L2 |
| ***Defnition with Explanantion*** | 5 | | |

PGP is a remarkable phenomenon, PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.

1. It is available free worldwide in versions that run on a variety of platforms, including Windows, UNIX, Macintosh, and many more.
2. It is based on algorithms that have survived extensive public review and are considered extremely secure. Specifically, the package includes RSA, DSS, and Diffie-Hellman for public-key encryption; CAST-128, IDEA, and 3DES for symmetric encryption; and SHA-1 for hash coding.
3. It has a wide range of applicability, from corporations that wish to select and enforce a standardized scheme for encrypting files and messages to individuals who wish to communicate securely with others worldwide over the Internet and other networks.
4. It was not developed by, nor is it controlled by, any governmental or standards organization. For those with an instinctive distrust of "the establishment," this makes PGP attractive.
5. PGP is now on an Internet standards track (RFC 3156; MIME Security with OpenPGP). Nevertheless, PGP still has an aura of an anti-establishment endeavor.

| | | | |
|---|---|---|---|
| ***Neat diagram*** | 5 | | |

***Authentication:***

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.

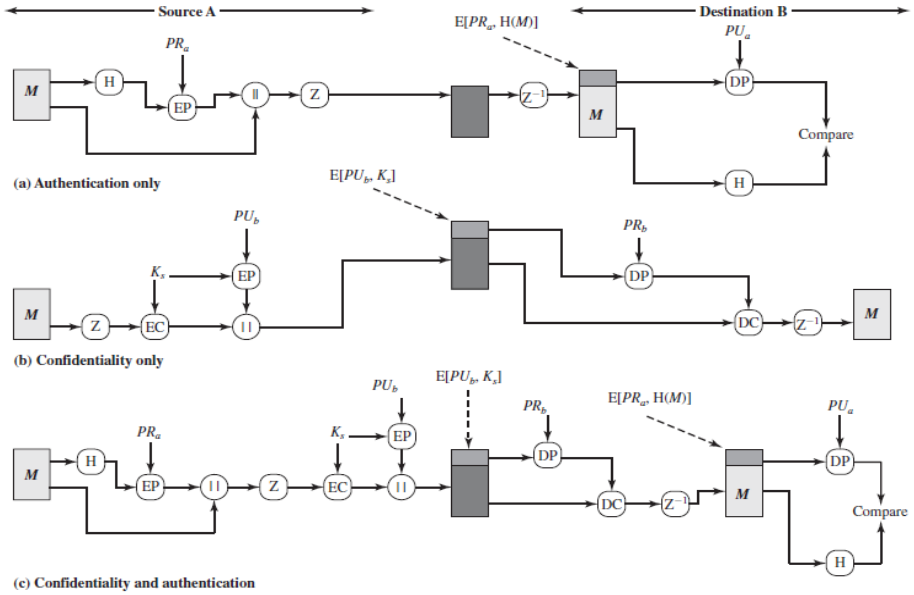
***Confidentiality:***

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.

***Confidentiality and Authentication:***

First, a signature is generated for the plaintext message and prepended to the message. Then the plaintext message plus signature is encrypted using CAST-128 (or IDEA or 3DES), and the session key is encrypted using RSA . This sequence is preferable to the opposite: encrypting the message and then generating a signature for the encrypted message. If the signature is performed first, a third party need not be concerned with the symmetric key when verifying the signature.




| | | | |
|---|---|---|---|
| 2 Explain S/MIME functionality indicating all the functions and cryptographic algorithms. | 10 | CO 1 | L2 |

## S/MIME functionality — 5

S/MIME provides the following functions.

• **Enveloped data:** This consists of encrypted content of any type and encrypted content encryption keys for one or more recipients.

• **Signed data:** A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer. The content plus signature are then encoded using base64 encoding. A signed data message can only be viewed by a recipient with S/MIME capability.

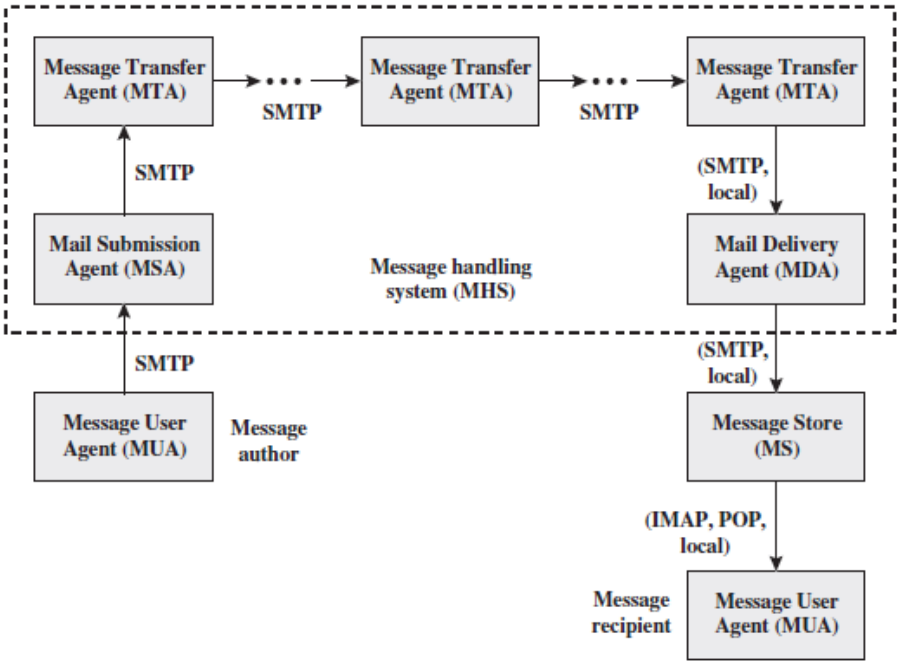
• **Clear-signed data:** As with signed data, a digital signature of the content is formed. However, in this case, only the digital signature is encoded using

## Cryptographic algorithms — 5

| Function | Requirement |
|---|---|
| Create a message digest to be used in forming a digital signature. | MUST support SHA-1.<br>Receiver SHOULD support MD5 for backward compatibility. |
| Encrypt message digest to form a digital signature. | Sending and receiving agents MUST support DSS.<br>Sending agents SHOULD support RSA encryption.<br>Receiving agents SHOULD support verification of RSA signatures with key sizes 512 bits to 1024 bits. |
| Encrypt session key for transmission with a message. | Sending and receiving agents SHOULD support Diffie-Hellman.<br>Sending and receiving agents MUST support RSA encryption with key sizes 512 bits to 1024 bits. |
| Encrypt message for transmission with a one-time session key. | Sending and receiving agents MUST support encryption with tripleDES.<br>Sending agents SHOULD support encryption with AES.<br>Sending agents SHOULD support encryption with RC2/40. |
| Create a message authentication code. | Receiving agents MUST support HMAC with SHA-1.<br>Sending agents SHOULD support HMAC with SHA-1. |

| | | | |
|---|---|---|---|
| 3 With the help of a neat diagram explain the function modules and standardised protocols used between them in the internet mail architecture. | 10 | CO 1 | L3 |

## Function modules diagram — 5




*Explanantion of each term* — 5

**Message User Agent (MUA):** Operates on behalf of user actors and user applications. It is their representative within the e-mail service.

**Mail Submission Agent (MSA):** Accepts the message submitted by an MUA and enforces the policies of the hosting domain and the requirements of Internet standards. This function may be located together with the MUA or as a separate functional model. In the latter case, the Simple Mail Transfer Protocol (SMTP) is used between the MUA and the MSA.

**Message Transfer Agent (MTA):** Relays mail for one application-level hop. It is like a packet switch or IP router in that its job is to make routing assessments and to move the message closer to the recipients. Relaying is performed by a sequence of MTAs until the message reaches a destination MDA. An MTA also adds trace information to the message header. SMTP is used between MTAs and between an MTA and an MSA or MDA.

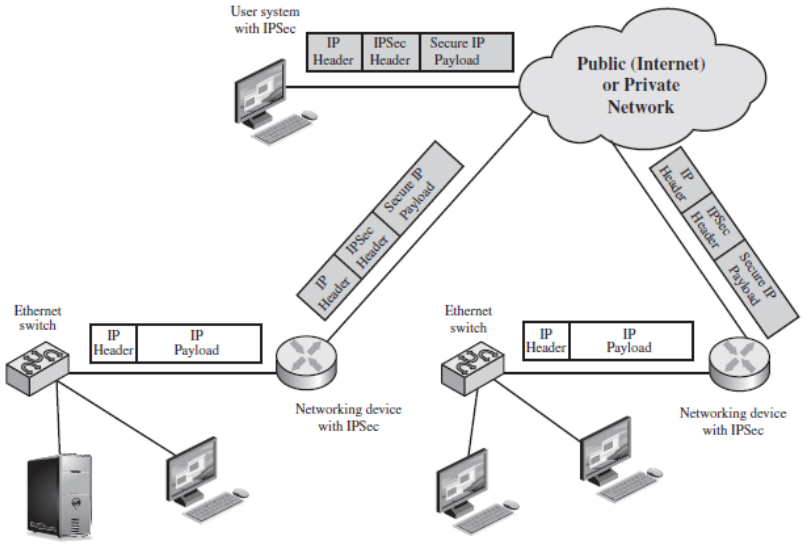
**Mail Delivery Agent (MDA):** Responsible for transferring the message from the MHS to the MS.

**Message Store (MS):** An MUA can employ a long-term MS. An MS can be located on a remote server or on the same machine as the MUA. Typically, an MUA retrieves messages from a remote server using POP (Post Office Protocol) or IMAP (Internet Message Access Protocol).

An **administrative management Domain (ADMD)** is an Internet e-mail provider.

4 What are the applications of IP security? With the help of a neat diagram explain IP security scenario. — 10 — CO 1 — L3

*IP security diagram* — 5



## Applications of Ipsec

5

IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.

• **Secure branch office connectivity over the Internet:** A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.

• **Secure remote access over the Internet:** An end user whose system is equipped with IP security protocols can make a local call to an Internet Service Provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.

• **Establishing extranet and intranet connectivity with partners:** IPsec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

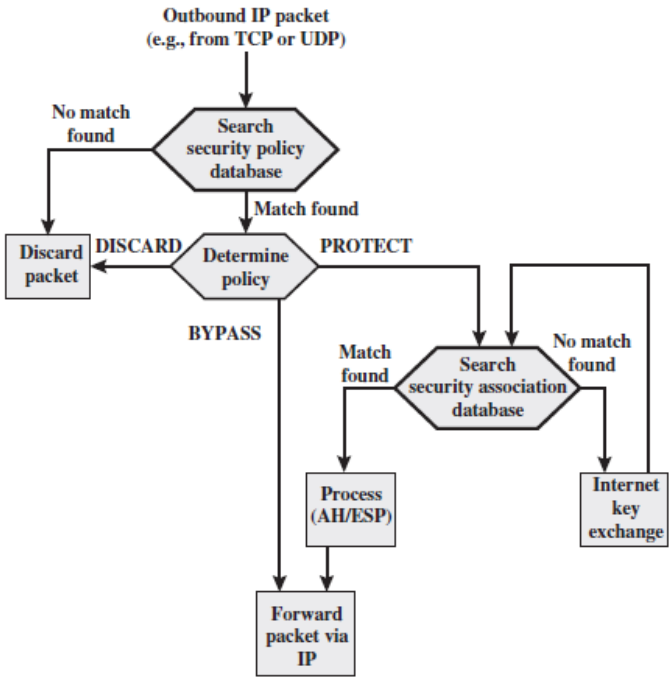
• **Enhancing electronic commerce security:** Even though some Web and electronic commerce applications have built-in security protocols, the use of IPsec enhances that security. IPsec guarantees that all traffic designated by the network administrator is both encrypted and authenticated, adding an additional layer of security to whatever is provided at the application layer. The principal feature of IPsec that enables it to support these varied applications is that it can encrypt and/or authenticate *all* traffic at the IP level. Thus, all distributed applications (including remote logon, client/server, e-mail, file transfer, Web access, and so on) can be secured.

5 What is IP Traffic Processing? Explain the Outbound and Inbound packets with the help of processing models.

10 | CO 1 | L2

## Explanantion with neat diagram for processing model for outbound packets

5

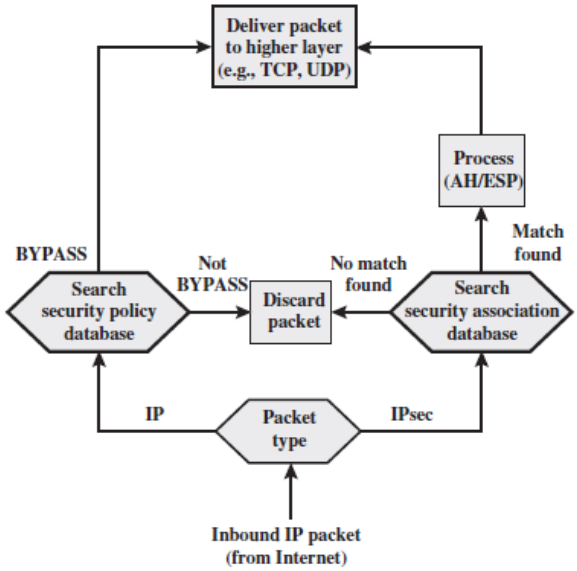



The following steps occur:

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.

5

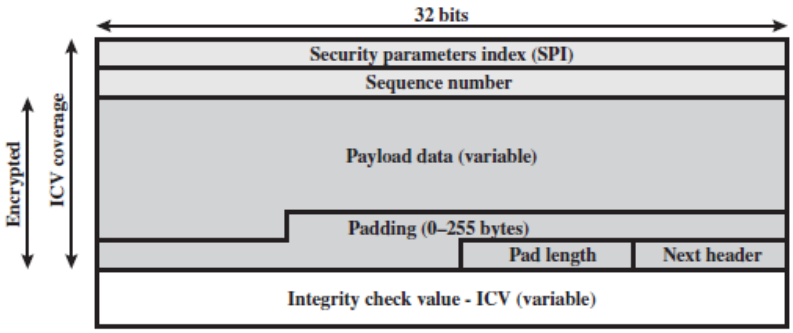
*Explanantion with neat diagram for processing model for inbound packets*



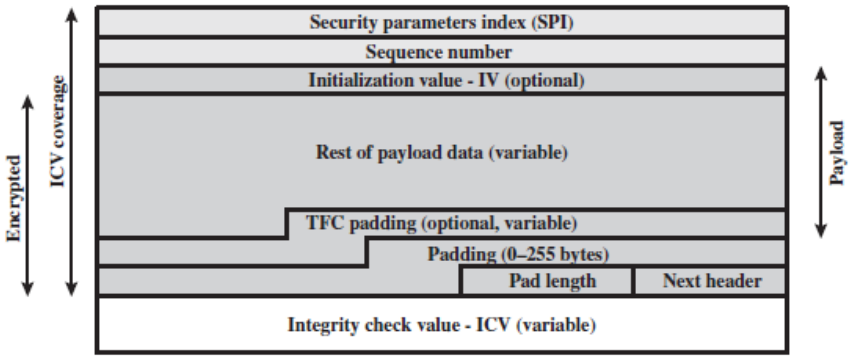

1. IPsec determines whether this is an unsecured IP packet or one that has ESP or AH headers/trailers, by examining the IP Protocol field (IPv4) or Next Header field (IPv6).
2. If the packet is unsecured, IPsec searches the SPD for a match to this packet. If the first matching entry has a policy of BYPASS, 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.

| | | | | |
|---|---|---|---|---|
| 6 | Explain in detail the Encapsulating Structure Payload, with the help of ESP packet format. | 10 | CO 1 | L2 |

*Diagrams for ESP packet format* — 5




(a) Top-level format of an ESP Packet




(b) Substructure of payload data

| | | | |
|---|---|---|---|
| *Explanantion*<br>It contains the following fields.<br>• **Security Parameters Index (32 bits):** Identifies a security association.<br>• **Sequence Number (32 bits):** A monotonically increasing counter value; this provides an anti-replay function, as discussed for AH.<br>• **Payload Data (variable):** This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.<br>• **Padding (0–255 bytes):** The purpose of this field is discussed later.<br>• **Pad Length (8 bits):** Indicates the number of pad bytes immediately preceding this field.<br>• **Next Header (8 bits):** Identifies the type of data contained in the payload data field by identifying the first header in that payload (e.g., an extension header in IPv6, or an upper-layer protocol such as TCP).<br>• **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.<br>An **initialization value (IV)**, or nonce, is present if this is required by the encryption or authenticated encryption algorithm used for ESP<br>If tunnel mode is being used, then the IPsec implementation may add **traffic flow confidentiality (TFC)** padding after the Payload Data and before the Padding field, as explained subsequently | 5 | | |

| Signature of CI | Signature of CCI |
|---|---|