1	C	R	2	1	I	S			

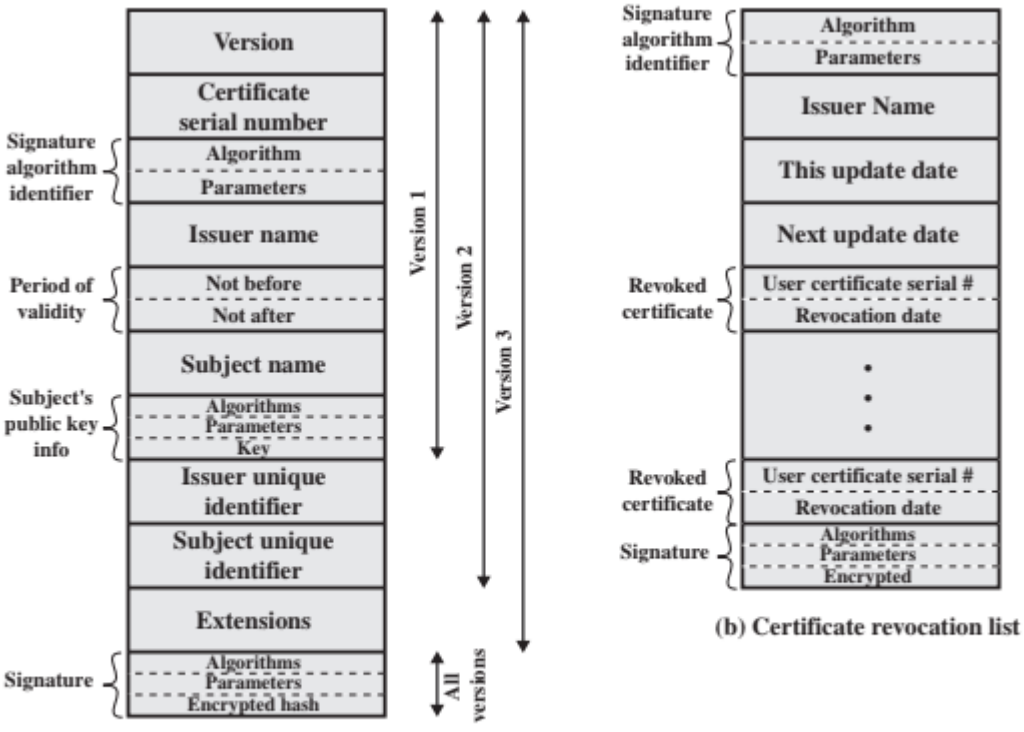
USN

Internal Assessment Test 3- Oct. 2024

Sub:	Cryptography and Network Security					Sub Code:	21IS71	Branch:	ISE
Date:	/12/2024	Duration:	90 mins	Max Marks:	50	Sem/ Sec:	VII/ A,B, C		OBE

	Answer any FIVE FULL questions	MARKS	CO	RBT
1	Describe the key components of an X.509 certificate	[10]	CO4	L2
2	Explain the architecture of IP Security.	[10]	CO4	L2
3	Explain the concept of transaction and tunnel modes.	[10]	CO5	L2
4	Discuss the principles and working of Pretty Good Privacy (PGP) in electronic mail security.	[10]	CO5	L2
5	Explain ESP packet format.	[10]	CO5	L2
6	Discuss the different types of IP Security policies.	[06]	CO5	L2
	How does an IPsec policy ensure the security of communication between hosts and networks?	[04]	CO5	L2

1.Describe the key components of an X.509 certificate



(a) X.509 certificate

(b) Certificate revocation list

Figure 14.15 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.

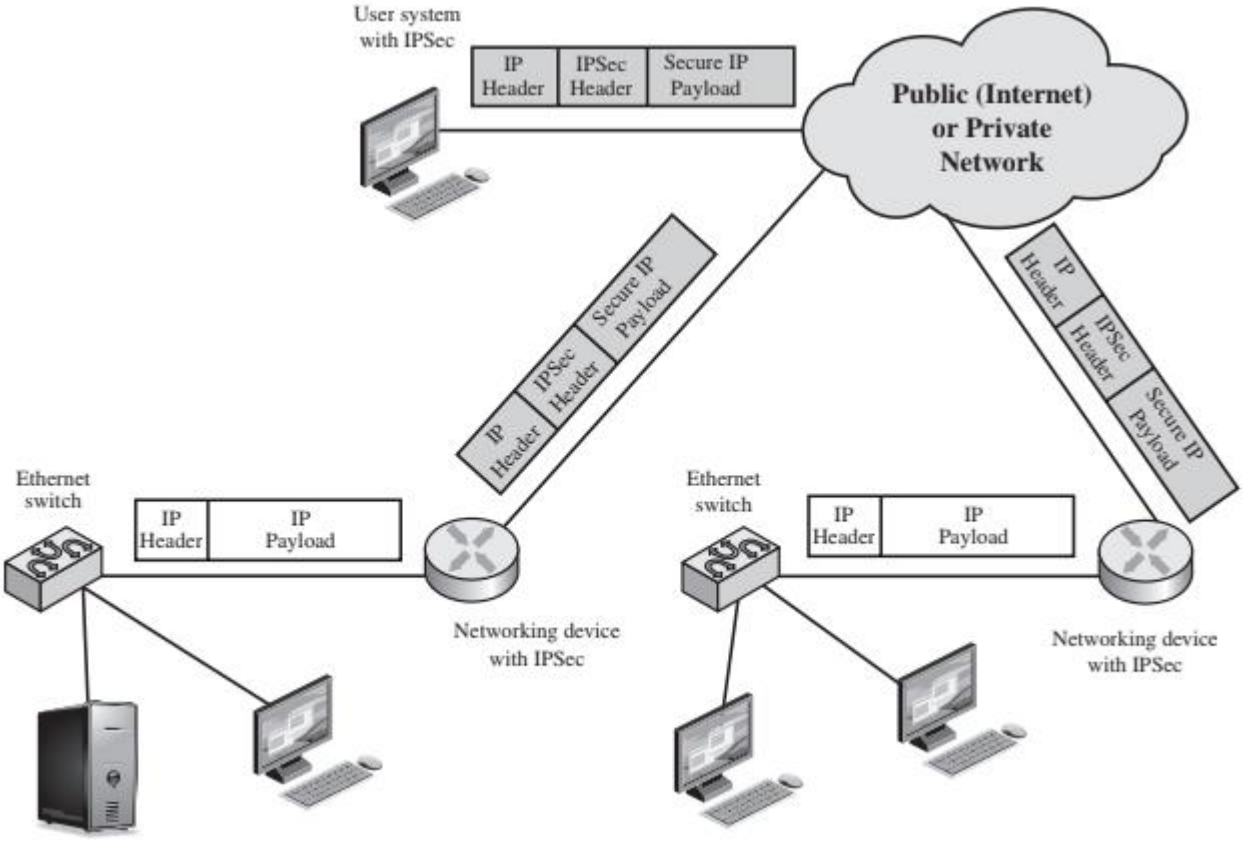
• Period of validity: Consists of two dates: the first and last on which the certificate is valid.

• 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.

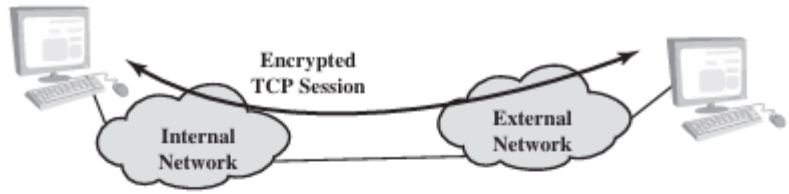
• Subject's public-key information: The public key of the subject, plus an identifier of the algorithm for which this key is to be used, together with any associated parameters.

• 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.

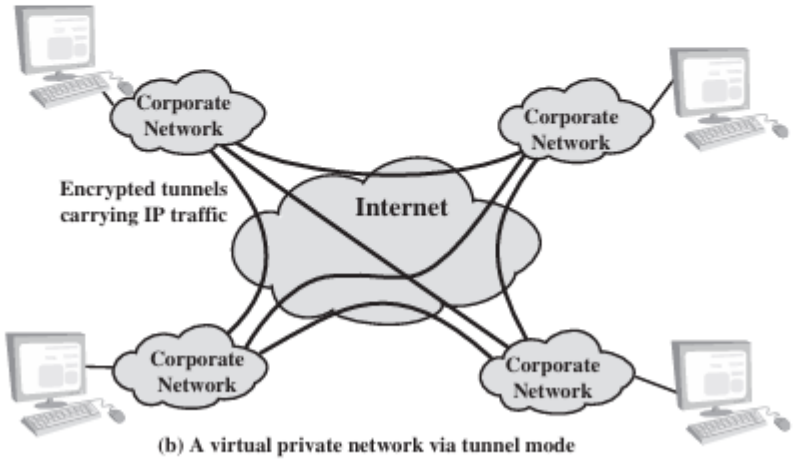
2.Explain the architecture of IP Security.



3.Explain the concept of transport and tunnel modes.



(a) Transport-level security



(b) A virtual private network via tunnel mode

Figure 20.7 Transport-Mode versus Tunnel-Mode Encryption

4.Discuss the principles and working of Pretty Good Privacy (PGP) in electronic mail security.

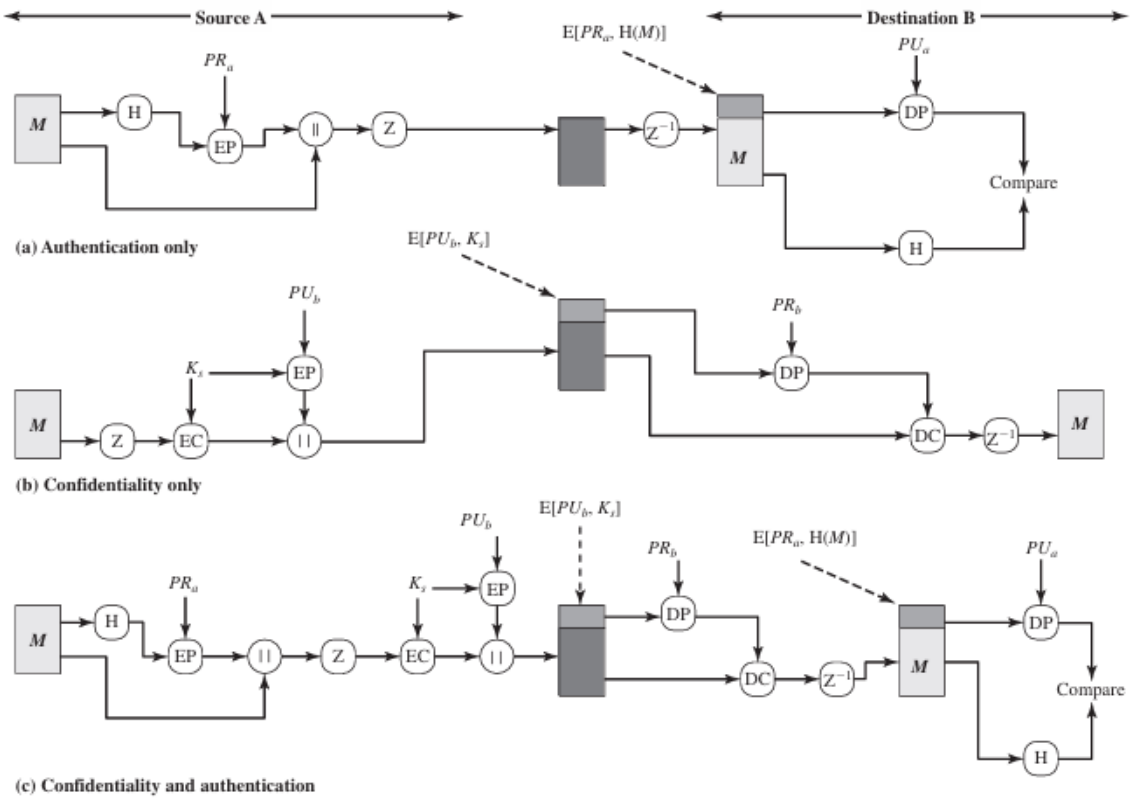
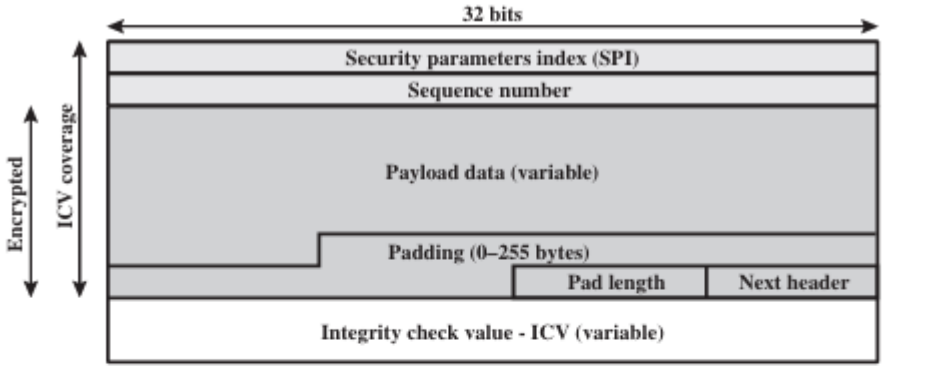
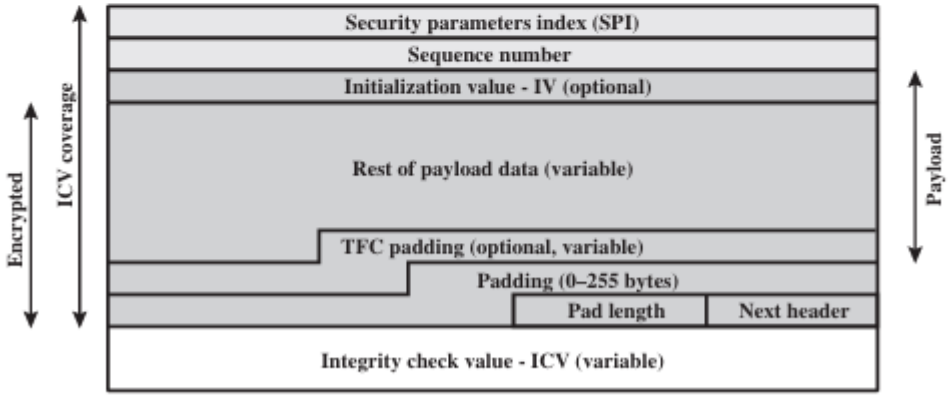


Figure 19.1 PGP Cryptographic Functions

5.Explain ESP packet format.



(a) Top-level format of an ESP Packet



(b) Substructure of payload data

Figure 20.5 ESP Packet Format

6.a.Discuss the different types of IP Security policies.

Fundamental to the operation of IPsec is the concept of a security policy applied to each IP packet that transits from a source to a destination. IPsec policy is de termined primarily by the interaction of two databases, the security association database (SAD) and the security policy database (SPD)

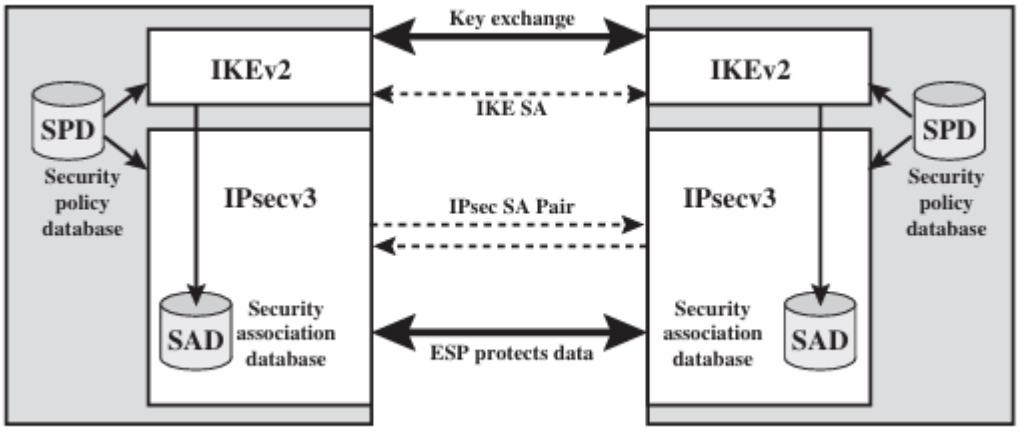


Figure 20.2 IPsec Architecture

6.b.How does an IPsec policy ensure the security of communication between hosts and networks?

A security association is uniquely identified by three parameters.

- Security Parameters Index (SPI): A 32-bit unsigned integer assigned to this SA and having local significance only. The SPI is carried in AH and ESP head ers to enable the receiving system to select the SA under which a received packet will be processed.
- IP Destination Address: This is the address of the destination endpoint of the SA, which may be an end-user system or a network system such as a firewall or router
. • Security Protocol Identifier: This field from the outer IP header indicates whether the association is an AH or ESP security association.

Table 20.2 Host SPD Example

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet