UNIT IV

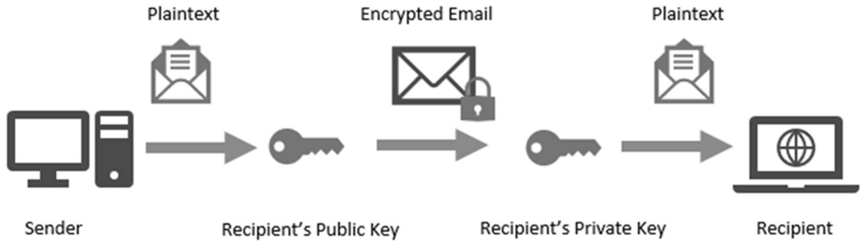
Email Security:

S/MIME:

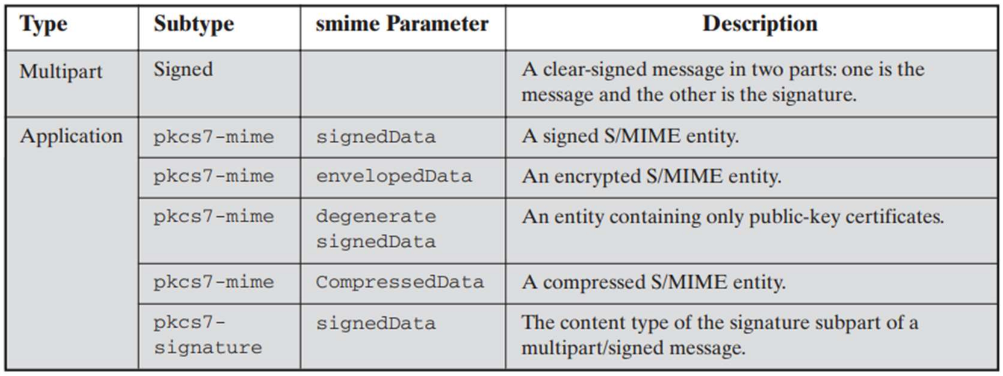
Operational Description:

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard that provides end-to-end encryption for email messages.

- It is based on public-key cryptography and uses digital certificates to verify the identity of email senders and recipients.
- When a sender wants to send an encrypted email message, their email client (such as Microsoft Outlook) generates a random symmetric key and uses it to encrypt the message.
- The sender then encrypts the symmetric key with the recipient's public key (obtained from their digital certificate) and includes it in the email message.
- When the recipient receives the email message, their email client decrypts the encrypted symmetric key using their private key (which is protected by a passphrase).
- The recipient's email client can then use the symmetric key to decrypt the encrypted message.
- S/MIME also provides for message authentication and digital signing.
- When a sender wants to digitally sign an email message, their email client generates a hash of the message content and encrypts the hash with their private key.
- The sender then includes the encrypted hash (called a digital signature) in the email message.
- When the recipient receives the digitally signed email message, their email client can verify the digital signature using the sender's public key.
- If the digital signature is valid, the recipient can be assured that the message has not been altered in transit and that it originated from the claimed sender.

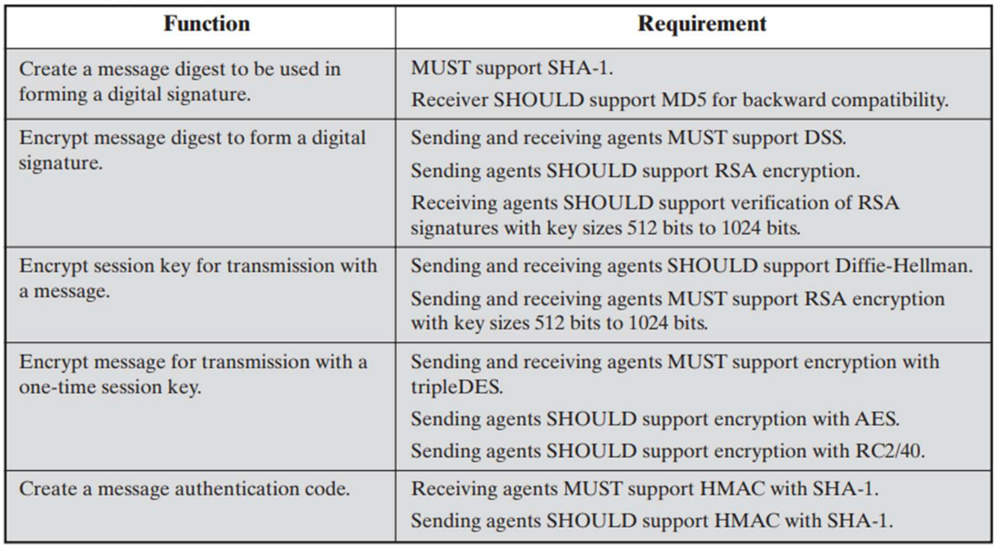


Message Content Types:



Type	Subtype	smime Parameter	Description
Multipart	Signed		A clear-signed message in two parts: one is the message and the other is the signature.
Application	pkcs7-mime	signedData	A signed S/MIME entity.
	pkcs7-mime	envelopedData	An encrypted S/MIME entity.
	pkcs7-mime	degenerate signedData	An entity containing only public-key certificates.
	pkcs7-mime	CompressedData	A compressed S/MIME entity.
	pkcs7-signature	signedData	The content type of the signature subpart of a multipart/signed message.

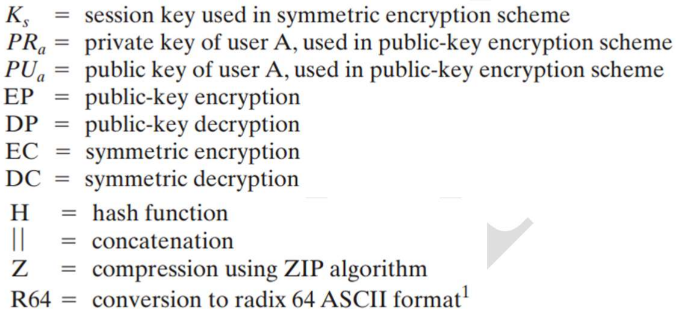
Approved Cryptographic Algorithms:



Function	Requirement
Create a message digest to be used in forming a digital signature.	MUST support SHA-1. Receiver SHOULD support MD5 for backward compatibility.
Encrypt message digest to form a digital signature.	Sending and receiving agents MUST support DSS. Sending agents SHOULD support RSA encryption. 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. 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. Sending agents SHOULD support encryption with AES. Sending agents SHOULD support encryption with RC2/40.
Create a message authentication code.	Receiving agents MUST support HMAC with SHA-1. Sending agents SHOULD support HMAC with SHA-1.

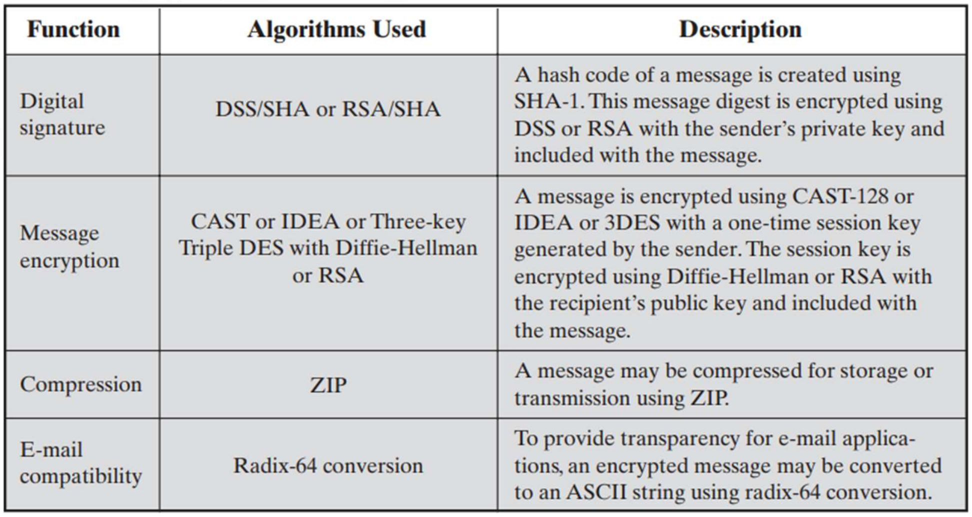
Pretty Good Privacy:

Notations:



K_s	=	session key used in symmetric encryption scheme
PR_a	=	private key of user A, used in public-key encryption scheme
PU_a	=	public key of user A, used in public-key encryption scheme
EP	=	public-key encryption
DP	=	public-key decryption
EC	=	symmetric encryption
DC	=	symmetric decryption
H	=	hash function
||	=	concatenation
Z	=	compression using ZIP algorithm
R64	=	conversion to radix 64 ASCII format[1]

Operational Description:



Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed for storage or transmission using ZIP.
E-mail compatibility	Radix-64 conversion	To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.

IP Security Overview:

IPsec is a set of protocols used to secure network communications across LANs, WANs, and the internet.

Applications:

- It can encrypt and authenticate traffic at the IP level, allowing for secure remote access, branch office connectivity, and e-commerce security.
- IPsec can be implemented in networking devices like routers and firewalls, and is transparent to workstations and servers.
- Users accessing the network remotely must implement IPsec protocols for security.

Benefits:

- Provides strong security for all traffic crossing a perimeter when implemented in a firewall or router.
- Resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet.
- Transparent to applications since it operates below the transport layer, so there is no need to change software on user or server systems.
- Transparent to end users, so there is no need for user training or per-user keying material management.
- Can provide security for individual users, making it useful for offsite workers and setting up a secure virtual subnetwork for sensitive applications.

IPsec Documents:

The IPsec specification is complex and spread across many documents.

- The IPsec document roadmap can help understand it.
- The IPsec documents are divided into groups:
    1. **Architecture:** The Architecture covers general concepts, security requirements, definitions, and mechanisms.
    2. **Authentication Header (AH):** AH provides message authentication but is deprecated.
    3. **Encapsulating Security Payload (ESP**): ESP provides encryption and authentication.
    4. **Internet Key Exchange (IKE):** IKE manages the keys used in IPsec.
    5. **Cryptographic algorithms:** Cryptographic algorithms define encryption, authentication, PRFs, and key exchange.
    6. **Other** documents cover security policy and MIB content.

IPsec Services:

- Access control
- Integrity
- Authentication
- Rejection of replayed packets
- Confidentiality
- Limited traffic flow confidentiality

Transport Mode:

Transport mode protects upper-layer protocols.

- It is typically used for end-to-end communication between two hosts.
- Transport mode is used for AH or ESP over IPv4 or IPv6.
- ESP in transport mode encrypts and optionally authenticates the IP payload.
- AH in transport mode authenticates the IP payload and selected portions of the IP header.

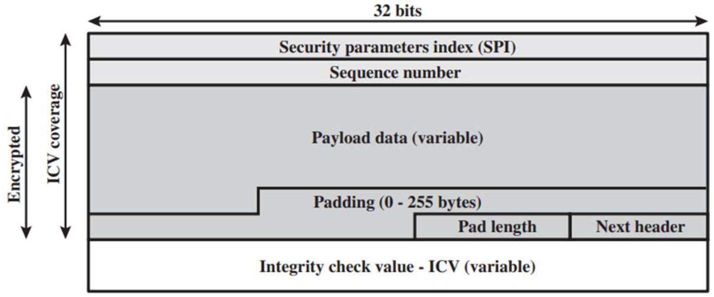
Tunnel Mode:
Tunnel mode protects the entire IP packet, including the header and payload.

- The packet is encapsulated with an outer IP header and travels through a tunnel from one point of an IP network to another.
- Tunnel mode is used when one or both ends of a security association are a security gateway, such as a firewall or router that implements IPsec.
- Intermediate routers along the way cannot examine the inner IP header.
- ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header.
- AH in tunnel mode authenticates the entire inner IP packet and selected portions of the outer IP header.

Encapsulating Security Payload:

ESP can provide confidentiality, data origin authentication, integrity, anti-replay, and limited traffic flow confidentiality, depending on options selected, and supports various encryption and authentication algorithms, including authenticated encryption like GCM.

ESP Format:



(a) Top-level format of an ESP Packet

- ESP packet format contains several fields, including Security Parameters Index, Sequence Number, Payload Data, Padding, Pad Length, Next Header, and Integrity Check Value.
- The Initialization Value or Nonce may be present if required by the encryption or authenticated encryption algorithm used for ESP.
- In tunnel mode, the IPsec implementation may add Traffic Flow Confidentiality (TFC) padding after the Payload Data and before the Padding field.

Encryption and Authentication Algorithms:
Payload Data, Padding, Pad Length, and Next Header fields are encrypted by ESP.

- An IV may be included at the beginning of the Payload Data field for encryption.
- ICV field is optional and is present only if the integrity service is selected.
- The ICV is computed after encryption and is used to detect replayed or bogus packets.
- A keyed integrity algorithm must be employed to compute the ICV.

Padding:
The Padding field is used to expand the plaintext to meet encryption algorithm requirements and ensure alignment within a 32-bit word.

- Additional padding may also be added for partial traffic-flow confidentiality.

Anti-Replay Service:

- A replay attack is when an attacker sends a copy of an authenticated packet to the intended destination.
- Sequence numbers are used to prevent replay attacks.
- The sender increments a counter and places the value in the Sequence Number field for each packet sent.
- If anti-replay is enabled, the sender must not cycle past the value of 2^32 – 1 to prevent multiple valid packets with the same sequence number.
- The receiver implements a window of size 64.
- The receiver marks the corresponding slot in the window for any packet received within the window and correctly authenticated.
- Inbound processing proceeds based on the position of the received packet relative to the window and whether authentication succeeds or fails.

Transport Mode:

Transport mode operation involves encrypting the ESP trailer plus the entire transport-layer segment, replacing the plaintext with its cipher text, and adding authentication if selected.

- The packet is then routed to the destination, with intermediate routers only examining the IP header and any plaintext extension headers.
- The destination node decrypts the packet based on the SPI in the ESP header and recovers the plaintext transport-layer segment.
- Transport mode provides confidentiality for all applications using it, avoiding the need to implement it in every individual application.
- One drawback to this mode is not providing protection against some attacks, such as attacks from intermediate routers.

Tunnel Mode:

Tunnel mode ESP encrypts an entire IP packet, including the IP header.

- Encrypted IP packets must be encapsulated with a new IP header to allow for routing.
- Tunnel mode is useful for protecting internal networks from external networks.
- Encryption only occurs between external hosts and security gateways or between two security gateways.
- Using tunnel mode simplifies key distribution and thwarts traffic analysis based on ultimate destination.

Malicious Software:

Types:

Malicious software can be divided into two categories: parasitic (need a host program) and independent.

- Parasitic malware includes viruses, logic bombs, and backdoors.
- Independent malware includes worms and bot programs.
- Malware can be categorized as either replicating or non-replicating.
- Replicating malware can produce copies of itself to be activated later on the same or different system.
- Key categories of malicious software include adware, spyware, Trojan horses, and ransomware.

Viruses:

A computer virus is a software that can infect other programs by modifying them and injecting them with a routine to make copies of the virus program.

- Computer viruses first appeared in the early 1980s and are similar to biological viruses in that they carry instructions to make copies of themselves.
- The typical virus becomes embedded in a program on a computer and spreads by passing into new programs whenever the infected computer comes into contact with an uninfected piece of software.
- A virus can do anything that other programs do and can perform any function, such as erasing files and programs that is allowed by the privileges of the current user.

Backdoor:

A backdoor is a secret entry point into a program that allows access without going through security procedures.

- Backdoors are used legitimately by programmers for debugging and testing.
- Backdoors become threats when unscrupulous programmers use them to gain unauthorized access.
- It is difficult to implement operating system controls for backdoors, so security measures must focus on program development and software updates.

Logic Bomb:

A logic bomb is a type of program threat that predates viruses and worms.

- It is code embedded in a legitimate program that is set to "explode" when certain conditions are met.
- Examples of triggers include the presence or absence of certain files, a specific date, or a particular user running the application.
- Once triggered, a logic bomb may cause damage to data or entire files, halt a machine, or cause other damage.

Trojan Horses:

A Trojan horse is a program that appears to be useful but performs unwanted or harmful functions when executed.

- It can be used to gain unauthorized access or destroy data.
- It can be disguised as a useful program or application.
- Trojan horses can be difficult to detect, such as when a compiler is modified to insert code into programs.
- Trojan horses can fit into three models: performing a separate malicious activity, modifying the original function, or completely replacing it.

Firewalls:

The Need for Firewalls:

Computer networks have evolved from centralized mainframes to internet-connected systems.

- Internet connectivity is essential but also creates a threat to the organization's security.
- Equipping each system with strong security features may not be sufficient or cost-effective.
- Firewalls provide an additional layer of defence by establishing a controlled link between the premises network and the internet.
- Firewalls act as an outer security wall or perimeter to protect the premises network from internet-based attacks and provide a single choke point for security and auditing.
- The firewall follows the military doctrine of "defence in depth" for IT security.

Characteristics:

- All traffic from inside to outside, and vice versa, must pass through the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- The firewall itself is immune to penetration.
- Firewalls use four general techniques to control access and enforce the site's security policy: service control, direction control, user control, and behaviour control.
- A firewall defines a single choke point that keeps unauthorized users out of the protected network.
- A firewall provides a location for monitoring security-related events.
- A firewall can serve as the platform for IPsec.
- Firewalls have limitations, including the inability to protect against attacks that bypass the firewall.

Types of Firewalls:

Packet Filtering Firewall:

A packet filtering firewall is a type of firewall that examines each packet of data that passes through it and selectively blocks or allows packets based on a set of predefined rules.

- The firewall operates by examining the header information of each packet and comparing it against a set of filtering rules.
- If a packet matches a rule that allows it to pass, it is forwarded to its destination.
- If a packet matches a rule that blocks it, the firewall discards the packet and may generate an alert to the network administrator.

Stateful Inspection Firewalls:

Stateful inspection firewalls, also known as dynamic packet filtering firewalls, are a type of firewall that is designed to inspect and evaluate the state of network connections.

- This means that instead of simply examining individual packets like packet filtering firewalls, stateful inspection firewalls monitor the status of each network connection to ensure that it is legitimate and authorized.
- Stateful inspection firewalls maintain a state table that tracks the status of each network connection, including the source and destination IP addresses, ports, and sequence numbers.

Application-Level Gateway (Proxy Firewall):

Proxy Firewall is a type of firewall that operates at the application layer of the network protocol stack.

- It is designed to provide a higher level of security by examining the contents of the application data rather than just the headers of packets
- When a client initiates a connection to a server, the gateway acts as a proxy, establishing a new connection with the server on behalf of the client.

Circuit-Level Gateway:

Circuit-Level Gateway works at the session layer of the OSI model and operates by creating a virtual circuit between the sender and receiver.

- It doesn't look into the contents of the packets, but it only checks if the session is authorized or not.
- Once the session is authorized, the Circuit-Level Gateway allows traffic to flow freely between the two hosts until the session is closed.