UNIT-III : Cryptographic Hash Functions and Digital Signatures

1. A cryptographic hash function takes an input of arbitrary length and produces:
a) An output of the same length as input
b) A fixed-length output called a hash value or message digest
c) An encrypted version of the input
d) A variable-length output
Answer: b

2. A key property of a good cryptographic hash function is that it should be computationally infeasible to:
a) Compute the hash quickly
b) Find two different inputs that produce the same hash output (collision resistance)
c) Apply it to large files
d) Use it for encryption
Answer: b

3. The property that it should be infeasible to find any input that produces a given hash output is called:
a) Collision resistance
b) Pre-image resistance (one-way property)
c) Weak collision resistance
d) Avalanche effect
Answer: b

4. Message authentication is primarily concerned with protecting against:
a) Loss of confidentiality
b) Attacks that affect message integrity and source authenticity
c) Slow network speed
d) Hardware failure
Answer: b

5. Which of the following is NOT a typical requirement of message authentication?
a) Verifying the message has not been altered
b) Verifying the message came from the alleged sender
c) Verifying the message timing/sequence is proper
d) Compressing the message size
Answer: d

6. SHA-512 produces a message digest of:
a) 128 bits b) 256 bits
c) 384 bits d) 512 bits
Answer: d

7. SHA-512 processes the input message in blocks of:
a) 512 bits
b) 1024 bits
c) 256 bits
d) 2048 bits
Answer: b
8. SHA-512 uses words of size:
a) 32 bits
b) 64 bits
c) 16 bits
d) 128 bits
Answer: b
9. The number of rounds used in the SHA-512 compression function is:
a) 64
b) 80
c) 16
d) 128
Answer: b
10. Before processing, SHA-512 pads the message so that its length is congruent to:
a) 448 mod 512
b) 896 mod 1024
c) 0 mod 64
d) 512 mod 1024
Answer: b
11. A Message Authentication Code (MAC) is generated using:
a) Only the message
b) The message and a shared secret key
c) Only a public key
d) A random number generator without a key
Answer: b
12. Unlike a hash function, a MAC requires:
a) No key at all
b) A secret key shared between sender and receiver
c) Only a public key
d) Two independent hash functions
Answer: b

13. HMAC stands for:
a) Hashed Message Authentication Code
b) Hash-based Message Authentication Code
c) Hidden Message Authentication Cipher
d) High-speed Message Authentication Code
Answer: b
14. HMAC is constructed by combining a cryptographic hash function with:
a) A public key
b) A secret key, using nested hashing (inner and outer hash operations)
c) A digital certificate
d) A random IV only
Answer: b
15. The main advantage of HMAC over a simple keyed hash is:
a) It eliminates the need for any key
b) It is built to resist certain cryptanalytic attacks while reusing existing hash functions efficiently
c) It only works with SHA-512
d) It produces variable-length output
Answer: b
16. CMAC stands for:
a) Cipher-based Message Authentication Code
b) Combined Message Authentication Code
c) Certified Message Authentication Code
d) Compressed Message Authentication Code
Answer: a
17. CMAC is based on the use of:
a) A hash function only
b) A block cipher (such as AES) in a chaining mode to generate a MAC
c) Asymmetric encryption only
d) A stream cipher
Answer: b
18. A digital signature primarily provides which security services?
a) Confidentiality only
b) Authentication, integrity, and non-repudiation
c) Availability only
d) Compression

Answer: b

19. In a digital signature scheme, the sender signs a message using:
a) The receiver's public key
b) Their own private key
c) Their own public key
d) A shared symmetric key
Answer: b
20. To verify a digital signature, the receiver uses the:
a) Sender's private key
b) Sender's public key
c) Receiver's own private key
d) A shared secret key
Answer: b
21. The ElGamal digital signature scheme's security is based on the difficulty of:
a) Factoring large numbers
b) Solving the discrete logarithm problem
c) The knapsack problem
d) Reversing a hash function
Answer: b
22. In the ElGamal signature scheme, the signature on a message consists of:
a) A single value
b) A pair of values (r, s)
c) Three separate keys
d) The encrypted message only
Answer: b
Key Management and Distribution
23. Key management primarily deals with:
a) Generating, distributing, storing, and revoking cryptographic keys securely
b) Only encrypting messages
c) Only hashing passwords
d) Compressing data before transmission
Answer: a
24. In symmetric key distribution using symmetric encryption, a common approach uses a:
a) Public certificate authority
b) Key Distribution Center (KDC) that shares a master key with each party

c) Hash function only

d) Digital signature only

Answer: b

25. When symmetric key distribution uses asymmetric encryption, the public key system is mainly used to:

a) Encrypt all bulk data directly

b) Securely distribute/exchange the symmetric session key

c) Replace the need for symmetric keys entirely

d) Generate hash values

Answer: b

26. One method of public key distribution where keys are simply announced openly is called:

a) Public-key certificates

b) Public announcement

c) Publicly available directory

d) Public-key authority

Answer: b

27. A major weakness of public announcement of public keys is that:

a) It is too slow

b) Anyone can forge such a public announcement, enabling impersonation

c) It requires a trusted third party

d) It cannot be used at all

Answer: b

28. Using a publicly available directory to distribute public keys improves security by: a) Eliminating the need for any keys

b) Having a trusted authority maintain and update entries of {name, public key}

c) Removing the need for authentication entirely

d) Encrypting all directory entries with a private key

Answer: b

29. A public-key certificate binds a public key to an identity and is typically signed by: a) The key owner themselves only

b) A trusted Certification Authority (CA)

c) Any random user

d) No one; it is self-evident

Answer: b

30. Kerberos is primarily designed to provide:

a) Data compression

b) Authentication services in a distributed/networked environment using a trusted third party c) Encryption of hard disks

d) Routing protocols

Answer: b

31. Kerberos uses which type of cryptography as its primary mechanism?

a) Asymmetric (public key) cryptography only

b) Symmetric key cryptography with a trusted Key Distribution Center

c) Steganography

d) Hashing only, without keys

Answer: b

32. In Kerberos, the component responsible for issuing the initial ticket-granting ticket (TGT) is the:

a) Ticket Granting Server (TGS)

b) Authentication Server (AS)

c) Application Server

d) Client

Answer: b

33. In Kerberos, the Ticket Granting Server (TGS) is responsible for:

a) Verifying the user's original password

b) Issuing service tickets to access specific application servers after the user presents a valid TGT

c) Generating the user's public key

d) Storing user files

Answer: b

34. Kerberos tickets typically include a timestamp mainly to:

a) Improve compression

b) Limit the validity period and help prevent replay attacks

c) Identify the hash algorithm used

d) Encrypt the session key permanently

Answer: b

35. X.509 is a standard that defines the format for:

a) Symmetric session keys

b) Public key certificates

c) Hash digest values

d) Stream cipher keys

Answer: b

36. An X.509 certificate is digitally signed by the:

a) Certificate holder (subject) themselves

b) Issuing Certification Authority (CA)

c) Any intermediate router

d) The end user's browser

Answer: b

37. Which of the following fields is typically included in an X.509 certificate?

a) Subject's public key, issuer name, validity period, and serial number

b) Only the subject's private key

c) Only a password hash

d) The user's browsing history

Answer: a

38. X.509 certificates support a hierarchical trust model that allows certificates to be verified through:

a) A single isolated authority only

b) A chain of trust up to a trusted root CA

c) No verification at all

d) Direct user-to-user trust without any CA

Answer: b

39. Public Key Infrastructure (PKI) primarily refers to:

a) A single algorithm for encryption

b) The set of hardware, software, policies, and procedures needed to create, manage, distribute, and revoke digital certificates

c) A type of symmetric cipher

d) A hash function standard

Answer: b

40. In PKI, the entity responsible for issuing and verifying digital certificates is called the:

a) Registration Authority only

b) Certification Authority (CA)

c) End user

d) Key Distribution Center

Answer: b

41. The Registration Authority (RA) in a PKI primarily handles:

a) Issuing the final signed certificate

b) Verifying user identity and forwarding certificate requests to the CA

c) Generating the CA's private key

d) Revoking the CA's own certificate

Answer: b

42. A Certificate Revocation List (CRL) in PKI is used to:

a) List all valid certificates

b) Maintain a list of certificates that have been revoked before their expiry date

c) Generate new public keys

d) Store hash values of all messages

Answer: b

43. The primary reason a certificate might be revoked before expiry includes:

a) The certificate was never used

b) The private key has been compromised or the holder's affiliation has changed

c) The certificate's validity period started

d) The CA wants to issue more certificates

Answer: b

44. In PKI, a certificate chain (or trust chain) is verified by checking signatures up to a: a) Random intermediate CA

b) Trusted root CA whose certificate is self-signed and pre-installed/trusted

c) Any available public key

d) The end user's own certificate

Answer: b