What is another name for asymmetric key cryptography?

Public-key cryptography

Private-key cryptography

Symmetric cryptography

Hashing

Asymmetric encryption uses how many keys?

1

2

3

4

In asymmetric encryption, how is confidentiality ensured?

By encrypting with the senders private key

By encrypting with the recipients public key

By hashing the message

By using symmetric keys

Which asymmetric algorithm is widely used for digital signatures?

RSA

DES

AES

MD5

What is the purpose of the Diffie-Hellman algorithm?

Encrypt messages

Decrypt messages

Securely exchange keys

Hash data

What does message integrity ensure?

Confidentiality of the message

The message has not been altered during transmission

The message is encrypted

The message is deleted after transmission

Which of the following does NOT provide message integrity?

Hash functions

Digital signatures

Message Authentication Codes (MACs)

Plaintext transmission

Which of the following can be used for message authentication?

Digital Signature

Message Authentication Code (MAC)

Both a and b

None of the above

A Message Authentication Code (MAC) requires which type of key?

Private key

Symmetric key

Public key

No key is required

Which of the following is a cryptographic hash function?

RSA

SHA-256

AES

DES

What is the primary use of the private key in asymmetric cryptography?

To encrypt messages

To share secret keys

To decrypt messages and sign data

To generate random numbers

What is the main disadvantage of asymmetric encryption?

It is slower than symmetric encryption

It does not provide authentication

It does not work over networks

It requires a VPN

In digital signatures, what ensures the integrity of the message?

Public key encryption

Private key encryption

Hash function

Symmetric key

What happens if a private key is compromised?

The system remains secure

Encrypted data can still be safe

Confidentiality and authenticity are lost

The public key must be changed

What does ECC stand for in cryptography?

Electronic Cryptographic Cipher

Elliptic Curve Cryptography

Enhanced Cipher Code

Encrypted Code Calculation

Which technique is commonly used to verify message integrity?

Hash functions

Symmetric encryption

Asymmetric encryption

Compression algorithms

Message authentication ensures that a message comes from a:

Trusted source

Random sender

Secure channel

Symmetric algorithm

Which method does NOT provide message authentication?

HMAC

AES encryption

Digital signature

Message digest without a key

If a hash function produces the same output for two different inputs, it is called a:

Collision

One-way function

Pre-image attack

Hash expansion

Key management in cryptography refers to:

Securely generating, storing, and distributing cryptographic keys

Encrypting messages with random keys

Using the same key for all users

Creating passwords for users

What is the main purpose of key agreement protocols?

To encrypt messages

To securely share a symmetric encryption key

To generate a random number

To sign digital documents

Which entity is responsible for verifying public keys in a PKI?

Certification Authority (CA)

Internet Service Provider (ISP)

Firewall

Symmetric Key Server

Which of the following can be used for public-key distribution?

Digital certificates

Secure email

Blockchain

All of the above

Which of the following is a primary function of PGP?

Encrypting files and emails

Compressing large files

Creating digital certificates

Generating symmetric keys

What is the purpose of SSL/TLS?

Encrypting email messages

Providing secure communication over the internet

Preventing physical attacks on servers

Encrypting hard drives

What is the primary function of IPsec?

Encrypting emails

Securing internet communication at the network layer

Managing user authentication

Compressing data packets

Which two modes does IPsec operate in?

Stream mode and Block mode

Authentication mode and Encryption mode

Transport mode and Tunnel mode

Secure mode and Unsecure mode

Which file extension is commonly used for PGP public keys?

.pgp

.p12

.crt

.pem

Which hashing algorithm is commonly used in PGP for integrity verification?

MD5

SHA-256

RC4

Blowfish

What is the main purpose of the Diffie-Hellman algorithm?

a) Encrypting messages

b) Exchanging cryptographic keys securely

c) Hashing data

d) Creating digital signatures

Which mathematical concept is the foundation of the Diffie-Hellman algorithm?

a) Prime factorization

b) Elliptic curve cryptography

c) Discrete logarithm problem

d) Hash functions

What is a major security risk of Diffie-Hellman key exchange?

a) Susceptibility to brute-force attacks

b) Man-in-the-middle (MITM) attacks

c) Weak encryption strength

d) Lack of authentication

What type of cryptography does Diffie-Hellman use?

a) Symmetric-key cryptography

b) Asymmetric-key cryptography

c) Hybrid cryptography

d) Hashing

Which of the following parameters are publicly shared in Diffie-Hellman key exchange?

a) Private keys of both parties

b) Prime number and generator

c) Encrypted message

d) Hash function

Which cryptographic technique is used to generate a digital signature?

a) Symmetric encryption

b) Public key cryptography

c) Hashing only

d) Steganography

Which of the following is NOT a property of digital signatures?

a) Integrity

b) Authentication

c) Non-repudiation

d) Anonymity

Which algorithm is commonly used for digital signatures?

a) AES

b) RSA

c) DES

d) Blowfish

What is the role of the private key in digital signatures?

a) Encrypting the message

b) Verifying the signature

c) Signing the message

d) Generating a hash

Which of the following is required to verify a digital signature?

a) The senders private key

b) The recipients private key

c) The senders public key

d) A shared secret key

What is the primary function of S/MIME?

a) Encrypting web traffic

b) Securing email communication

c) Protecting files from viruses

d) Managing network traffic

Which cryptographic techniques does S/MIME use?

a) Only symmetric encryption

b) Only asymmetric encryption

c) Both symmetric and asymmetric encryption

d) Only hashing

Which of the following is NOT a feature of S/MIME?

a) Digital signatures

b) Message encryption

c) Email filtering

d) Key management

S/MIME relies on which infrastructure for key management?

a) Blockchain

b) Certificate Authority (CA)

c) Hash tables

d) Kerberos

What standard email format does S/MIME extend?

a) SMTP

b) MIME

c) POP3

d) IMAP

What is PGP mainly used for?

a) Encrypting entire networks

b) Secure email communication and file encryption

c) Protecting websites from hacking

d) Storing passwords

What cryptographic approach does PGP use?

a) Only symmetric encryption

b) Only asymmetric encryption

c) A combination of symmetric and asymmetric encryption

d) Hashing only

Which of the following is used for authentication in PGP?

a) Shared secret keys

b) Digital certificates

c) Web of Trust

d) Biometric

What is the primary function of IPsec?

a) Securing IP communications

b) Encrypting emails

c) Hashing passwords

d) Blocking malware

Which two main protocols does IPsec use?

a) AES and SHA

b) HTTP and HTTPS

c) AH and ESP

d) FTP and SFTP

What is the role of a digital certificate in SSL/TLS?

Encrypts messages end-to-end

Authenticates the servers identity

Replaces public-key cryptography

Hides IP addresses

Which of the following is a challenge in key management?

Key distribution

Key revocation

Key storage

All of the above

Which of the following is a symmetric-key agreement protocol?

RSA

Diffie-Hellman

AES

ECC

Which protocol is commonly used to distribute public keys securely on the internet?

SSL/TLS

WPA2

DES

OTP

What does PGP stand for in cryptography?

Private Guard Protocol

Pretty Good Privacy

Public Guard Protection

Protected General Privacy

TLS provides which of the following security features?

Confidentiality

Integrity

Authentication

All of the above

Which layer of the OSI model does SSL/TLS operate on?

Network layer

Transport layer

Application layer

Data link layer

Which protocol is used in IPsec for authentication?

SHA-256

AES

AH (Authentication Header)

RSA

Which of the following is an attack against system security?

Denial-of-Service (DoS) attack

Man-in-the-middle attack

Phishing attack

All of the above

S/MIME requires a:

Public Key Infrastructure (PKI)

Pre-shared secret key

Blockchain-based authentication

Hardware security module

What is the primary function of IPsec in network security?

Encrypts entire network packets for secure communication

Protects against phishing attacks

Provides firewall protection

Blocks malware from being downloaded