Module 3 – Final Quiz: Cryptography and Security Protocols

1 - What is the primary purpose of cryptography?

A) Make data smaller for storage
B) Protect confidentiality, integrity, and authenticity of information
C) Speed up network traffic
D) Replace access control systems

2 - Which best describes symmetric encryption?

A) Uses a public key to encrypt and a private key to decrypt
B) Uses the same secret key for encryption and decryption
C) Stores passwords securely by hashing
D) Signs messages without encryption

3 - Which best describes asymmetric encryption?

A) The same key is shared by both parties
B) Uses a key pair: public key (encrypt/verify), private key (decrypt/sign)
C) Only used for hashing
D) Makes data integrity checks unnecessary

4 - In practice, why do systems use hybrid encryption?

A) Public-key crypto is faster for bulk data
B) Symmetric crypto is slower but more secure
C) Combine asymmetric (to exchange a session key) with symmetric (for data)
D) Hashing is required to encrypt data

5 - Which statement about hash functions is correct?

A) They are reversible with the right key
B) They map input to a fixed-size digest and are one-way
C) They always encrypt data
D) They require public/private keys

6 - Which property is most important for password hashing?

A) Collision resistance only
B) Being fast to compute
C) Being slow and salted (e.g., with PBKDF2/bcrypt/Argon2)
D) Using symmetric encryption instead

7 - Salting passwords helps primarily to:

A) Speed up logins
B) Prevent rainbow-table attacks by making hashes unique
C) Compress stored hashes
D) Replace two-factor authentication

8 - How does a digital signature provide assurance?

A) Confidentiality only
B) Integrity and origin authentication (and non-repudiation)
C) Anonymity
D) Compression

9 - What is a digital certificate?

A) A file that stores a user's password
B) A credential binding a public key to an identity, signed by a CA
C) A backup of private keys
D) A hashing configuration file

10 - What role does a Certificate Authority (CA) play?

A) Generates session keys for TLS
B) Verifies identities and signs certificates to establish trust
C) Stores encrypted emails
D) Routes network traffic securely

11 - Which is not a property of a good cryptographic hash?

A) Preimage resistance
B) Second-preimage resistance
C) Collision resistance
D) Easy reversibility

12 - What does ASLR or DEP have to do with cryptography?

A) They are encryption algorithms
B) They are OS mitigations; distinct from cryptography but help security
C) They are hashing algorithms
D) They are VPN protocols

13 - Which protocol combination most accurately secures web browsing?

A) HTTP + MD5
B) HTTPS (HTTP over TLS)
C) FTP over UDP
D) Telnet with AES

14 - Which scenario best justifies using asymmetric encryption directly?

A) Encrypting multi-GB backups local to disk
B) One-time secure distribution of a small secret to a new user
C) Streaming video encryption
D) Full-disk encryption on laptops

15 - A message arrives with a signature that verifies under Alice's public key, but the ciphertext was readable by anyone. What security was achieved?

A) Confidentiality only
B) Integrity and authentication without confidentiality
C) Availability only
D) No guarantees at all

Lab 3.1 – Encrypting, Hashing, and Signing Files with GPG

16 - Which command generates a new key pair in GPG?

A) gpg --gen-key
B) gpg --new-hash
C) gpg --make-cert
D) gpg --create-salt

17 - To encrypt a file for a recipient using their public key, which is correct?

A) gpg --sign file.txt
B) gpg --encrypt --recipient alice@example.com file.txt
C) gpg --hash sha256 file.txt
D) gpg --export-secret-keys

18 - Which command verifies the integrity of a file via SHA-256 (typical GNU tools)?

A) sha256sum file.txt
B) gpg --verify file.txt
C) gpg --armor file.txt
D) openssl enc -aes-256-cbc -in file.txt

19 - What is a detached signature in GPG?

A) Signature bundled inside the encrypted file
B) Signature stored separately (e.g., file.txt.sig)
C) An unsigned file
D) A revoked key certificate

20 - Which command verifies a detached signature?

A) gpg --verify file.txt.sig file.txt
B) gpg --decrypt file.txt.sig
C) gpg --list-keys file.txt.sig
D) gpg --clearsign file.txt

Lab 3.2 – Exploring HTTPS and Digital Certificates in Practice

21 - The browser padlock primarily indicates:

A) The site is safe and honest
B) The connection to the site is encrypted and a certificate validated
C) The site has no vulnerabilities
D) The site is government-approved

22 - When inspecting a certificate, which fields most help confirm identity?

A) File size and checksum
B) Subject and Subject Alternative Name (SAN) hostnames
C) Cipher suite list length
D) Key pinning count

23 - Which is a common certificate error that triggers a warning?

A) Perfect forward secrecy enabled
B) Certificate expired or hostname mismatch
C) CA is widely trusted
D) TLS 1.3 in use

24 - What does the chain of trust show in a browser's certificate viewer?

A) Hash algorithm history
B) Path from server cert → intermediate(s) → root CA
C) All previous owners of the domain
D) Encrypted cookies list

25 - If a site shows "Your connection is not private" due to an untrusted issuer, what is the safest action?

A) Ignore and proceed to the site
B) Add a permanent exception immediately
C) Do not proceed; verify the URL/cert and try again later
D) Disable HTTPS-only mode

Answer Key

1. **B** – Crypto protects confidentiality, integrity, authenticity.
2. **B** – Symmetric = same secret key both ways.
3. **B** – Asymmetric uses public/private key pair.
4. **C** – Use asymmetric to exchange a symmetric session key, then encrypt data symmetrically.
5. **B** – Hashing is one-way mapping to fixed-size digest.
6. **C** – Slow, salted, memory-hard password hashing thwarts cracking.
7. **B** – Salts defeat precomputed/rainbow-table attacks.
8. **B** – Signatures prove integrity and origin (and support non-repudiation).
9. **B** – Certificates bind a public key to an identity via CA signature.
10. **B** – CA validates identities and signs certs to establish trust.
11. **D** – Good hashes are *not* reversible.
12. **B** – DEP/ASLR are OS mitigations; separate from cryptography.
13. **B** – HTTPS = HTTP over TLS for secure web traffic.
14. **B** – Asymmetric is ideal for initial small-secret/key distribution.
15. **B** – Verified signature → integrity/authentication, but no confidentiality.
16. **A** – gpg --gen-key creates a key pair.
17. **B** – Encrypt to recipient's public key.
18. **A** – sha256sum produces/verifies SHA-256 digests.
19. **B** – Detached signature is stored separately from the file.
20. **A** – gpg --verify sig file checks a detached signature.
21. **B** – Padlock = encrypted connection + valid cert (not "site is safe").
22. **B** – Subject/SAN must match the domain.
23. **B** – Expiry and hostname mismatch are classic certificate errors.
24. **B** – Shows server → intermediate(s) → trusted root path.
25. **C** – Don't proceed; verify URL/cert before trusting.