Department of Computer Science

Computer Security

Exam 1

October 6, 2025

Review – Answers Discussions

Prepared with tender loving care by Paul Krzyzanowski

100 POINTS – 25 QUESTIONS – 4 POINTS EACH – For each statement, select the *most* appropriate answer.

1. What defines the *Trusted Computing Base (TCB)*?
   a. A tamperproof CPU and system chassis.
   b. User-written applications that are security-critical.
   c. Firewalls and intrusion detection systems.
   d. All the hardware, software, and firmware involved in enforcing security policies

d: All the hardware, software, and firmware involved in enforcing security policies

The TCB includes all components that enforce the system's security policy.

Incorrect answers:

a. Physical protections like a secure chassis don't enforce policy.

b. User-written applications are outside the TCB unless they enforce security.

c. Firewalls and intrusion detection systems are external, not part of the TCB.

2. Which of the following best describes an *exploit*?
   a. A tool that takes advantage of a vulnerability.
   b. A flaw in the software's code.
   c. The successful theft of confidential data.
   d. A denial-of-service attack.

a: A tool that takes advantage of a vulnerability

An exploit is the method or code that uses a flaw to achieve unauthorized behavior.

Incorrect answers:

b. A flaw is a vulnerability, not an exploit.

c. Data theft is a result of exploitation, not the exploit itself.

d. A denial-of-service attack is a separate attack type, not the definition of an exploit.

3. Which is true about *Advanced Persistent Threats (APTs)*?
   a. They are usually opportunistic.
   b. They refer to operations run by criminal gangs.
   c. They are state-backed, skilled, and long-term.
   d. They leverage insiders to get around security defenses.

c: They are state-backed, skilled, and long-term

APTs are well-funded, organized campaigns that operate persistently, often by or for nation-states.

Incorrect answers:

a. Opportunistic attacks are random and short-term, not APTs.

b. Criminal gangs may run operations but lack the persistence that defines APTs.

d. Insider help can occur, but it doesn't define the term APT.

4. The *Common Vulnerabilities and Exposures* (CVE) system is used to:
   a. Rank the severity of vulnerabilities on a 0–10 scale.
   b. Assign identifiers to publicly known security flaws.
   c. Provide patches to fix vulnerabilities.
   d. Detect intrusions in real time.

b: Assign identifiers to publicly known security flaws

CVE assigns standardized identifiers so vulnerabilities can be tracked consistently.

Incorrect answers:

a. CVSS ranks severity, not CVE.

c. CVE documents flaws but doesn't provide fixes.

d. CVE is not an intrusion-detection system.

5. Which situation illustrates the danger of conflating a *policy* with its *mechanism*?
   a. Assuming that a strong password requirement means the system enforces complexity rules.
   b. Setting up two-factor authentication for user logins.
   c. Having multiple firewalls from different vendors.
   d. Logging user activity for compliance reasons.

a: Assuming that a strong password requirement means the system enforces complexity rules

A policy is what should happen; the mechanism is how it's enforced. Assuming one implies the other is an error.

Incorrect answers:

b. Two-factor authentication is a specific mechanism, not conflation.

c. Using multiple firewalls shows layered defense, not policy confusion.

d. Logging supports policy enforcement but isn't an example of conflating them.

6. Which property guarantees that ciphertext reveals *no information whatsoever* about the plaintext, even to an adversary with unlimited computing power?
   a. Perfect secrecy.
   b. Diffusion.
   c. Forward secrecy.
   d. Confusion.

a: Perfect secrecy

Perfect secrecy means the ciphertext gives no information about the plaintext; the key is required to learn anything.

Incorrect answers:

b. Diffusion hides statistical structure but doesn't make ciphertext information-free.

c. Forward secrecy protects past sessions if long-term keys are lost; it's unrelated to individual ciphertexts.

d. Confusion hides the relationship between key and ciphertext but doesn't ensure total secrecy.

7. Shannon identified two key properties that strong ciphers should have: confusion and diffusion. Which of the following best describes *diffusion*?
   a. Making the relationship between the key and ciphertext complex and nonlinear.
   b. Hiding the encryption algorithm from potential attackers.
   c. Ensuring the key is randomly generated.
   d. Spreading the influence of each plaintext bit across many ciphertext bits.

d: Spreading the influence of each plaintext bit across many ciphertext bits

Diffusion ensures small plaintext changes affect many ciphertext bits, destroying recognizable patterns.

Incorrect answers:

a. That defines confusion, not diffusion.

b. Hiding the algorithm is "security through obscurity," not diffusion.

c. Random key generation is unrelated to diffusion.

8. The Vigenère cipher was considered unbreakable for centuries because it is a polyalphabetic cipher. However, it can be broken if an attacker can determine the key length. Why is knowing the *key length* so helpful?
   a. The ciphertext can be split into streams based on key length, and each stream becomes a simple Caesar cipher.
   b. Once you know the key length, you can use brute force to try all possible keys.
   c. The key length reveals the encryption algorithm being used.
   d. Knowing the key length allows you to reverse the encryption directly.

a: The ciphertext can be split into streams based on key length, and each stream becomes a simple Caesar cipher

Knowing the key length allows each position in the key to be analyzed separately using frequency analysis.

Incorrect answers:

b. Brute-forcing the key is not the efficient attack here.

c. Key length doesn't identify the encryption algorithm.

d. Knowing key length doesn't directly reverse the encryption.

9. How does *CTR (Counter) mode* make a block cipher like AES behave like a stream cipher?
   a. CTR mode splits the plaintext into individual bits instead of blocks.
   b. CTR mode uses a different key for each byte of plaintext.
   c. CTR mode encrypts a sequence of numbers to generate a keystream, which is then XORed with the plaintext.
   d. CTR mode removes the need for any encryption key.

c: CTR mode encrypts a sequence of numbers to generate a keystream, which is then XORed with the plaintext

Encrypting counters produces a keystream that's XORed with plaintext, turning a block cipher into a stream cipher.

Incorrect answers:

a. CTR still operates on blocks, not individual bits.

b. CTR uses one key for all blocks, not a new key per byte.

d. It still requires an encryption key.

10. What makes *polyalphabetic substitution ciphers* (like Vigenère) stronger than monoalphabetic substitution ciphers?
    a. They add transposition to substitution.
    b. Different character positions use different substitution alphabets.
    c. They require the key to be as long as the message.
    d. They use larger key sizes.

b: Different character positions use different substitution alphabets

Multiple alphabets obscure single-letter frequency patterns.

Incorrect answers:

a. That describes transposition, not substitution.

c. Only the one-time pad uses a key as long as the message.

d. Larger keys alone don't hide statistical patterns.

11. What problem do *block cipher modes* solve?
    a. They add multiple iterations per block for greater diffusion.
    b. They enable secure encryption of messages longer than one block.
    c. They replace the need for round keys.
    d. They generate initialization vectors automatically.

b: They enable secure encryption of messages longer than one block

Modes combine cipher outputs across blocks so long messages can be encrypted securely.

Incorrect answers:

a. They don't add internal rounds.

c. They don't replace round keys.

d. Not all modes automatically create initialization vectors.

12. A cryptographic hash function should be *collision-resistant*. What does this property mean?
    a. The hash output should be difficult to compress.
    b. The hash should produce different outputs for similar inputs.
    c. It should be hard to find two different inputs that produce the same hash output.
    d. The function should run without errors on all possible inputs.

c: It should be hard to find two different inputs that produce the same hash output

Collision resistance prevents attackers from substituting two messages with the same hash.

Incorrect answers:

a. Difficulty of compression is irrelevant.

b. Producing different outputs for similar inputs is the avalanche effect, not collision resistance.

d. Error-free execution isn't a cryptographic property.

13. In *hybrid cryptosystems*, what is the usual role of public key cryptography?
    a. Encrypt bulk data.
    b. Establish a shared session key.
    c. Provide message integrity.
    d. Add multiple layers of encryption for greater security.

b: Establish a shared session key

Public key algorithms set up or exchange a session key used later by faster symmetric encryption.

Incorrect answers:

a. Public key encryption is too slow for bulk data.

c. Message integrity comes from MACs or signatures.

d. Layering encryption isn't its main purpose.

14. What is *forward secrecy*?
    a. The ability to reuse a session key from previous communications to avoid re-establishing it.
    b. A guarantee that no quantum computer will break keys.
    c. Protection of past sessions if long-term keys are later compromised.
    d. A method of compressing ciphertext.

c: Protection of past sessions if long-term keys are later compromised.

Forward secrecy ensures old communications remain secure even if long-term keys are stolen later.

Incorrect answers:

a. Reusing session keys breaks forward secrecy.

b. It doesn't guarantee quantum-proof security.

d. It has nothing to do with compression.

15. What can Alice do if she obtains Bob's X.509 *certificate*?
    a. Validate a digital signature created by Bob.
    b. Impersonate Bob by creating digital signatures with his key.
    c. Decrypt messages that were encrypted for Bob.
    d. Authenticate as Bob to services that trust his certificate.

a: Validate a digital signature created by Bob.

A certificate gives Bob's public key so Alice can verify his signed messages.

Incorrect answers:

b. Only Bob's private key can create his signatures.

c. Bob's private key is needed to decrypt his encrypted mail.

d. A certificate alone doesn't let Alice impersonate Bob.

16. Why do *quantum computers* pose a threat to RSA and elliptic curve cryptography?
    a. Quantum computers can break any encryption instantly.
    b. Quantum computers generate random numbers that defeat all cryptography.
    c. Shor's algorithm can efficiently factor large numbers and solve discrete logarithms.
    d. Quantum computers make brute force attacks one million times faster.

c: Shor's algorithm can efficiently factor large numbers and solve discrete logarithms

Shor's algorithm breaks the mathematical problems that secure RSA and ECC.

Incorrect answers:

a. Quantum computers can't instantly break all encryption.

b. Random number generation isn't relevant.

d. Grover's algorithm only speeds brute force quadratically.

17. In a hybrid cryptosystem, why are *session keys* critical for forward secrecy?
    a. Session keys are stored permanently.
    b. Each session key is independent, so long-term key compromise does not expose past traffic.
    c. Session keys prevent hash collisions.
    d. Session keys are larger than long-term keys.

b: Each session key is independent, so long-term key compromise does not expose past traffic

Unique, temporary session keys isolate each conversation's confidentiality.

Incorrect answers:

a. Session keys are short-lived, not permanent.

c. Hash collisions are unrelated.

d. Key size isn't the reason; independence is.

18. Which feature distinguishes a *trapdoor function* from a regular one-way function?
    a. It becomes invertible if you know a secret.
    b. It is probabilistic instead of deterministic.
    c. It has no collisions.
    d. It can only be computed with elliptic curves.

a: It becomes invertible if you know a secret

A trapdoor allows someone with special information (like a private key) to invert the function easily.

Incorrect answers:

b. Being probabilistic isn't the difference.

c. Trapdoor functions can still have collisions.

d. They don't require elliptic curves.

19. What is the role of a *trusted third party* in symmetric key protocols?
    a. To authenticate users and share their long-term symmetric keys with authorized parties.
    b. To encrypt all communication between users.
    c. To generate and distribute session keys to communicating parties.
    d. To maintain a database of all symmetric keys currently in use.

c: To generate and distribute session keys to communicating parties

A trusted server issues temporary session keys for secure exchanges.

Incorrect answers:

a. It doesn't share users' long-term keys with others.

b. It doesn't handle all encryption itself.

d. It doesn't store every symmetric key permanently.

20. What is the role of *nonces* in the Needham–Schroeder protocol?
    a. They add randomness to encrypted tickets.
    b. They allow a session key to be shared across multiple sessions.
    c. They ensure clocks are synchronized.
    d. They are intended to show that messages are fresh and not replays.

d: They are intended to show that messages are fresh and not replays

Nonces prove message freshness and defend against replay attacks.

Incorrect answers:

a. Tickets provide credentials, not randomness.

b. Nonces don't allow reuse of session keys.

c. The protocol doesn't rely on synchronized clocks.

21. What problem does the *Challenge Handshake Authentication Protocol (CHAP)* solve compared to PAP?
    a. It prevents passwords from being sent directly over the network.
    b. It eliminates the need for a trusted third party.
    c. It ensures forward secrecy of session keys.
    d. It requires hardware tokens for stronger authentication.

a: It prevents passwords from being sent directly over the network

CHAP uses challenge–response authentication so passwords never travel in plaintext.

Incorrect answers:

b. It still requires a trusted authenticator.

c. CHAP doesn't provide forward secrecy.

d. It doesn't require hardware tokens.

22. Why does Kerberos split the trusted third party into an Authentication Server (AS) and a Ticket Granting Server (TGS)?
    a. To reduce encryption overhead by using shorter keys.
    b. To allow the use of both symmetric and public key cryptography.
    c. To eliminate the need for tickets.
    d. To separate password-based login from service ticket requests, limiting password exposure.

d: To separate password-based login from service ticket requests, limiting password exposure

This separation minimizes how often a user's password is used or transmitted.

Incorrect answers:

a. The split doesn't reduce encryption overhead.

b. Kerberos uses only symmetric cryptography.

c. Tickets are essential to Kerberos, not removed.

23. What is the key idea behind *HOTP (HMAC-based One-Time Password)*?
    a. It uses a secret key and the current time to generate codes.
    b. It relies on random challenges from the server.
    c. It generates codes by chaining hashes of a password.
    d. It uses a secret key and a counter to generate codes.

d: It uses a secret key and a counter to generate codes

Each increment of a counter with the secret key produces a new one-time code.

Incorrect answers:

a. That describes TOTP, which uses time, not a counter.

b. HOTP doesn't use server-issued random challenges.

c. It doesn't chain password hashes.

24. Why are *salt values* critical in password storage?
    a. They make it easier for legitimate users to remember passwords.
    b. They make rainbow tables ineffective.
    c. They ensure passwords meet minimum complexity requirements.
    d. They ensure that dictionary attacks cannot succeed.

b: They make rainbow tables ineffective

Salts ensure each password hash is unique, defeating precomputed tables.

Incorrect answers:

a. Salts don't help users remember passwords.

c. They don't enforce complexity.

d. Dictionary attacks are still possible but slower.

25. Why are *passkeys* considered more secure than traditional passwords?
    a. They are easier for users to memorize.
    b. They store credentials encrypted in the cloud for easy recovery.
    c. They rely on rainbow tables to verify authentication.
    d. They use unique public/private key pairs per service, eliminating reuse.

d: They use unique public/private key pairs per service, eliminating reuse

Each account has its own key pair, removing password reuse and reducing phishing risk.

Incorrect answers:

a. Passkeys don't rely on memorization.

b. They aren't simply encrypted cloud credentials.

c. Rainbow tables apply to password hashes, not key pairs.s

The end.