WGU Introduction-to-Cryptography D830 Practice Questions

Shared by Vazquez on 02-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

(What type of encryption uses different keys to encrypt and decrypt the message?)

Options:

A- Symmetric
B- Private key
C- Secure
D- Asymmetric

P2P exams

Answer:

D

Explanation:

Asymmetric encryption (also called public key cryptography) uses a pair of mathematically related keys: a public key and a private key. One key is used to encrypt, and the other is used to decrypt, which is the defining ''different keys'' property asked in the question. In the common confidentiality use case, a sender encrypts a message using the recipient's public key, and only the recipient can decrypt it using their private key. This solves the key distribution problem inherent in symmetric encryption, where both parties must securely share the same secret key in advance. Asymmetric systems also enable digital signatures: the private key signs (creates a signature) and the public key verifies it, providing authenticity and integrity. Symmetric encryption, by contrast, uses the same shared key for both encryption and decryption (even though internal round keys may exist, it is still one shared secret). ''Private key'' alone is not a full encryption type, and ''secure'' is a generic description rather than a cryptographic category. Therefore, the correct answer is D. Asymmetric.

P2P exams

Question 2

Question Type: MultipleChoice

(Which attack maps hashed values to their original input data?)

Options:

A- Dictionary
B- Rainbow table
C- Birthday
D- Brute-force

Answer:

B

Explanation:

A rainbow table attack uses large, precomputed tables that link hash outputs back to likely original inputs (typically passwords). Instead of storing every passwordhash pair directly (which would be huge), rainbow tables store chains created by alternating hash operations with reduction functions, allowing attackers to reconstruct candidate plaintexts that produce a given hash. This makes cracking fast, if the target hashes are unsalted and use a known, fast hash function. Salt defeats rainbow tables because the attacker would need separate tables for each salt value, which becomes infeasible when salts are unique and sufficiently large. A dictionary attack is related but typically computes hashes on the fly from a wordlist rather than using precomputed chain structures. A birthday attack targets collisions, not mapping to original data. Brute-force tries all candidates without precomputation. Because the question explicitly describes mapping hashed values back to original data via a precomputed approach, the correct choice is Rainbow table.

Question 3

Question Type: MultipleChoice

(What is lattice-based cryptography?)

Options:

A- A technique for encoding messages using lattice points
B- A blockchain option from clone
C- A cryptographic scheme based on geometric lattices
D- A type of encryption algorithm using modular arithmetic

Answer:

C

Explanation:

Lattice-based cryptography refers to cryptographic constructions whose security is based on the computational hardness of problems on mathematical lattices (regular grids of points in high-dimensional space). Examples of hard lattice problems include the Shortest Vector Problem (SVP) and Closest Vector Problem (CVP), and practical schemes often use related problems like Learning With Errors (LWE) or Ring-LWE. These problems are believed to remain hard even for quantum computers, making lattice-based cryptography a major candidate family for post-quantum cryptography. Lattice schemes can support encryption, digital signatures, and key exchange, often with strong security reductions (worst-case to average-case) and efficient implementations. The word ''lattice'' here is not about simple point encoding; it's about relying on geometric/algebraic structures and noise-based hardness assumptions. It is also unrelated to blockchain ''options.'' While many lattice schemes do involve modular arithmetic internally, what defines the category is the underlying lattice hardness assumptions, not modular arithmetic alone. Therefore, the correct definition is a cryptographic scheme based on geometric lattices.

Question 4

Question Type: MultipleChoice

(Why is lightweight cryptography important in modern information security?)

Options:

A- To complicate data protection measures
B- To ensure secure communication on high-speed networks
C- To limit the use of encryption tools in organizations
D- To address the security needs of Internet of Things (IoT) devices and mobile applications

Answer:

D

Explanation:

Lightweight cryptography is important because many modern systems operate in constrained environments---IoT sensors, embedded controllers, wearables, and mobile devices---where CPU, memory, storage, bandwidth, and battery power are limited. Traditional ''heavy'' cryptographic suites may be too slow, too energy-intensive, or too large in code footprint for these platforms, leading to insecure workarounds or disabling security entirely. Lightweight cryptographic primitives and profiles are designed to deliver strong security properties (confidentiality and

integrity, often via AEAD) while fitting within tight resource budgets and real-time constraints. This is essential as IoT and mobile ecosystems expand, increasing the attack surface and the consequences of compromised devices (botnets, surveillance, physical safety risks). Lightweight cryptography is not meant to ''limit encryption tools'' or complicate protection; it enables practical, deployable security where otherwise implementations might be weak or absent. High-speed network communication can benefit from efficient crypto too, but the defining modern driver is constrained-device security. Therefore, the correct reason is addressing the security needs of IoT devices and mobile applications.

Question 5

Question Type: MultipleChoice

(Why did the National Institute of Standards and Technology (NIST) choose Ascon for lightweight cryptography?)

Options:

A- To authenticate users during data transmission
B- To ensure compatibility with legacy systems
C- To provide a secure and efficient encryption solution for resource-constrained devices
D- To encrypt data at rest

Answer:

C

Explanation:

NIST's lightweight cryptography effort targets environments like IoT and embedded systems where CPU, memory, energy, and bandwidth are constrained, yet strong security is still required. Ascon is an authenticated encryption with associated data (AEAD) family designed to be efficient in both hardware and software with small footprint, making it well-suited for constrained devices. NIST selected Ascon because it offers a strong security design with good performance and implementability under tight resource budgets, while providing modern protections (confidentiality + integrity) through AEAD. That aligns with option C: secure and efficient encryption for resource-constrained devices. The selection was not primarily about authenticating users (that is typically handled by protocols and identity systems, not an AEAD primitive). It was also not mainly about legacy compatibility; lightweight cryptography aims at new and constrained deployments rather than preserving outdated stacks. And while Ascon can certainly be used to protect data at rest, that is only one application; the core reason for the choice is its suitability for constrained environments and robust, efficient authenticated encryption.

Question 6

Question Type: MultipleChoice

(What is the RC4 encryption key size when utilizing WPA with Temporal Key Integrity Protocol (TKIP)?)

Options:

A- 40 bits
B- 56 bits
C- 128 bits
D- 256 bits

Answer:

C

Explanation:

WPA with TKIP was designed as an interim improvement over WEP while still using the RC4 stream cipher for compatibility with legacy hardware. TKIP addresses WEP's major weaknesses by introducing per-packet key mixing, a message integrity mechanism (''Michael''), and replay protection. In TKIP, the encryption key used with RC4 is 128 bits. Practically, TKIP derives a per-packet RC4 key from a 128-bit temporal key (TK), the transmitter's MAC address, and a sequence counter (TKIP Sequence Counter, TSC) to avoid the simple IV reuse patterns that made WEP easy to break. Even with these improvements, TKIP has known weaknesses and is deprecated in favor of WPA2/WPA3 using AES-based CCMP/GCMP. But strictly for the question asked, TKIP's RC4 keying material is based on a 128-bit key size, not 40/56-bit legacy sizes and not 256-bit.

Question 7

Question Type: MultipleChoice

(Which additional input element can be used to implement integrity in combination with symmetric ciphers?)

Options:

A- Initialization vector
B- Encoding algorithm
C- Nonce value
D- Hash function

Answer:

D

Explanation:

Symmetric encryption alone typically provides confidentiality, but it does not automatically provide integrity. Many encryption modes (especially older ones like CBC without authentication) are malleable, meaning an attacker may be able to modify ciphertext and cause predictable changes in plaintext after decryption. To add integrity, systems commonly combine symmetric encryption with a cryptographic hash-based integrity mechanism, such as a hash function used in an HMAC (Hash-based Message Authentication Code) or a dedicated authenticated-encryption mode like GCM that internally uses authentication tags. Among the given options, a hash function is the fundamental additional element that enables integrity checks: it allows construction of a MAC (e.g., HMAC-SHA-256) that the receiver verifies to detect any tampering. An initialization vector and a nonce value are used to ensure uniqueness and randomness properties for encryption but do not, by themselves, guarantee integrity. An encoding algorithm changes representation, not security. Therefore, the correct additional input element for implementing integrity alongside symmetric encryption is a hash function, typically as part of an HMAC or similar MAC construction.

Question 8

Question Type: MultipleChoice

(What describes a true random number generator?)

Options:

A- Fast and deterministic, and the same input produces the same results
B- Slow and nondeterministic, and the same input produces different results
C- Unique integer determined through factorization of integers
D- Integer increased by one to match requests and responses

Answer:

B

Explanation:

A true random number generator (TRNG) draws randomness from physical phenomena that are inherently unpredictable and not algorithmically reproducible. Because of this, it is nondeterministic: you cannot feed it the same ''input'' and expect the same output stream. TRNGs are often slower than PRNGs because they depend on collecting entropy from hardware sources and may require conditioning to remove bias. This aligns with option B: slow and nondeterministic, producing different results even under similar or repeated conditions. Option A describes a deterministic PRNG, where identical seeds yield identical sequences. Option C is unrelated; factorization is a hard math problem used in cryptography (e.g., RSA security assumptions), not a randomness generator definition. Option D describes a counter, which is deterministic and not random. In secure systems, TRNG output may seed a cryptographically secure PRNG to provide both unpredictability and high throughput; but the defining characteristic of a TRNG is nondeterminism from physical entropy. Therefore, option B is correct.

Question 9

Question Type: MultipleChoice

(Which cipher uses shifting letters of the alphabet for encryption?)

Options:

A- SHA-1
B- Vigenre
C- Bifid
D- Caesar

Answer:

D

Explanation:

The Caesar cipher is the classic substitution cipher that encrypts by shifting letters of the alphabet by a fixed number of positions (e.g., shift by 3: AD, BE, etc.). It is a monoalphabetic

cipher because a single shift value is applied uniformly across the entire message, making it simple and vulnerable to frequency analysis and brute force (only 25 meaningful shifts in the Latin alphabet). Vigenre also involves shifting, but it uses a repeating keyword to vary the shift per character (polyalphabetic), whereas the question's phrasing typically points to the fundamental ''shift cipher,'' which is Caesar. SHA-1 is a cryptographic hash function, not a cipher. Bifid is a fractionation cipher combining Polybius square coordinates and transposition, not a direct shifting method. Therefore, the cipher that uses shifting letters of the alphabet for encryption is the Caesar cipher.

Question 10

Question Type: MultipleChoice

(Which number generator has different results given the same input data?)

Options:

A- Prime
B- Sequence
C- Pseudorandom
D- True random

Answer:

D

Explanation:

A true random number generator (TRNG) produces outputs derived from nondeterministic physical processes (e.g., thermal noise, oscillator jitter, radioactive decay, or other hardware entropy sources). Because the underlying phenomenon is not algorithmically determined by an input seed in the same way as a PRNG, repeated ''inputs'' (or identical conditions from a software perspective) do not yield the same sequence; the outputs vary unpredictably. By contrast, a pseudorandom number generator (PRNG) is deterministic: given the same seed and internal state, it produces the same output sequence, which is useful for repeatability but means security depends on seed secrecy and proper seeding. ''Prime'' is not a generator type, and ''sequence'' is too generic and does not imply nondeterminism. In cryptographic systems, TRNGs (or hardware entropy sources) are often used to seed cryptographically secure PRNGs (CSPRNGs), combining high-quality entropy with efficient generation. Therefore, the generator that can produce different results for the ''same input data'' is a true random number generator.

Question 11

Question Type: MultipleChoice

(What is a key benefit of using a cryptography framework?)

Options:

A- It guarantees complete security against all attacks.
B- It removes the need for employee training in security.
C- It is solely focused on regulatory compliance.
D- It provides a structured approach to implementing encryption practices.

Answer:

D

Explanation:

A cryptography framework provides a consistent, repeatable way to select, deploy, and manage cryptographic controls across an organization. Its key benefit is structure: it defines approved algorithms and key sizes, acceptable modes of operation, key management rules (generation, storage, rotation, revocation, backup), certificate handling, and secure protocol configurations (e.g., TLS settings). This reduces ad hoc implementations that often lead to vulnerabilities such as weak ciphers, key reuse, improper randomness, or missing integrity protections. A framework also clarifies roles and processes---who can access keys, how secrets are audited, and how exceptions are handled---improving governance and operational reliability. Importantly, it does not guarantee perfect security; no framework can eliminate all risk, and secure outcomes still depend on correct implementation, monitoring, and maintenance. It also does not eliminate the need for training; human error is a major source of crypto misconfiguration. While frameworks help with compliance, they are not solely about regulation; they are about sound security engineering and lifecycle management. Therefore, the primary benefit is providing a structured approach to implementing encryption practices.

Question 12

Question Type: MultipleChoice

(Which certificate encoding process is binary-based?)

Options:

A- Public Key Infrastructure (PKI)
B- Distinguished Encoding Rules (DER)
C- Rivest--Shamir--Adleman (RSA)
D- Privacy Enhanced Mail (PEM)

Answer:

B

Explanation:

DER (Distinguished Encoding Rules) is a binary encoding format used to represent ASN.1 structures in a canonical, unambiguous way. X.509 certificates are defined using ASN.1, and DER provides a strict subset of BER (Basic Encoding Rules) that guarantees a single, unique encoding for any given data structure. That ''unique encoding'' property is important for cryptographic operations such as hashing and digital signatures, because different encodings of the same abstract data could otherwise produce different hashes and break signature verification. In contrast, PEM is not a binary encoding; it is essentially a Base64-encoded text wrapper around DER data, bounded by header/footer lines (e.g., ''BEGIN CERTIFICATE''). PKI is an overall framework for certificate issuance, trust, and lifecycle management---not an encoding. RSA is an asymmetric algorithm used for encryption/signing, not a certificate encoding format. Therefore, the binary-based certificate encoding process among the options is DER.

Question 13

Question Type: MultipleChoice

(What is used to randomize the initial value when generating Initialization Vectors (IVs)?)

Options:

A- Key
B- Plaintext
C- Algorithm
D- Nonce

Answer:

D

Explanation:

An IV (Initialization Vector) is a value used to ensure that encrypting identical plaintext under the same key produces different ciphertexts, preventing pattern leakage. In many secure designs, the IV must be unique (and often unpredictable) per encryption operation. A common way to ensure uniqueness is to incorporate a nonce---a ''number used once.'' A nonce can be random, pseudo-random, or a counter-based value depending on the mode and security requirements. For example, CTR mode uses a nonce combined with a counter to produce unique input blocks; GCM uses a nonce/IV to ensure unique authentication and encryption behavior. The encryption key should remain stable across many operations and should not be used as the ''randomizer'' for IV generation; mixing key material into IV creation in an ad hoc way can create reuse or correlation issues. Plaintext and algorithm do not provide the needed uniqueness property. The nonce concept is specifically about ensuring one-time uniqueness of the starting value so that IV reuse does not repeat keystream blocks (stream modes) or reveal plaintext equality (CBC/CTR). Therefore, the correct choice is Nonce.

P2P exams

To Get Premium Files for Introduction-to-Cryptography Visit

https://www.p2pexams.com/products/introduction-to-cryptography

For More Free Questions Visit

https://www.p2pexams.com/wgu/pdf/introduction-to-cryptography

