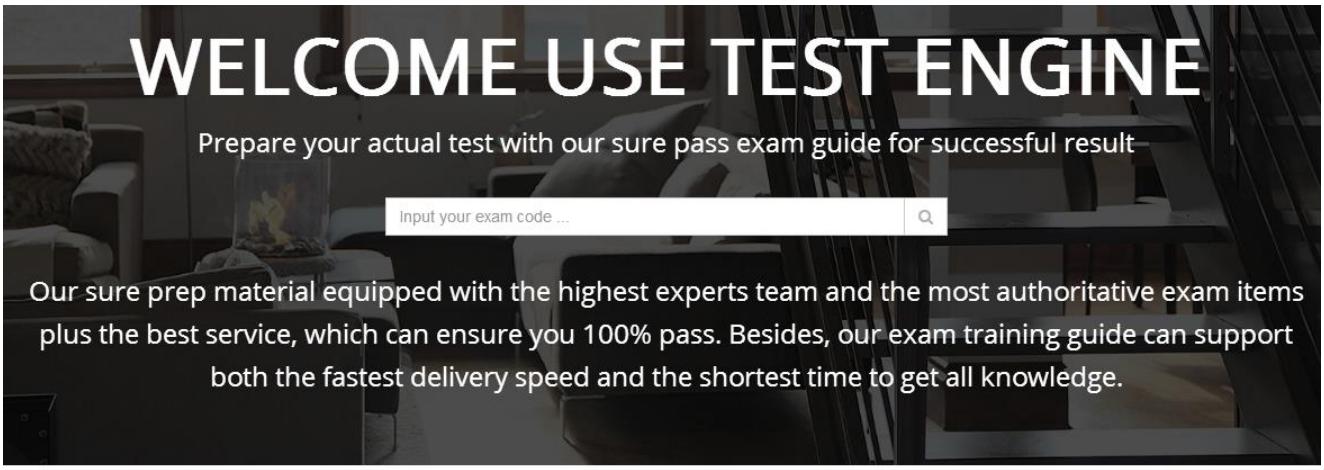
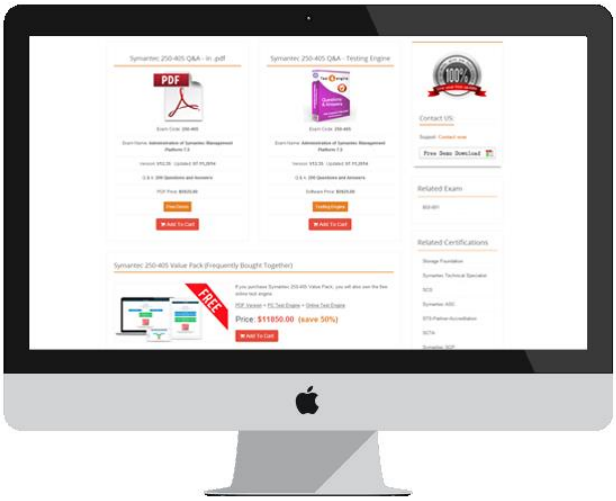
Prep4sureGuide

Prep4sureGuide





Quality and Value

Prep4sureGuide Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

Tested and Approved

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

Easy to Pass

If you prepare for the exams using our Prep4sureGuide testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

Try Before Buy

Prep4sureGuide offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

HAPPY CUSTOMERS	DOWNLOADS	TEAM MEMBERS	SHARES
32694	62152	32694	56692

http://www.prep4sureguide.com

Prepare your actual test with our sure pass exam guide for successful result

Exam : **Introduction-to-Cryptography**

Title : WGU Introduction to Cryptography HNO1

Vendor : WGU

Version : DEMO

NO.1 (What is a key benefit of using a cryptography framework?)
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.

NO.2 (A security analyst is using 3DES for data encryption. Which 3DES key size is valid?)
A. 128-bit
B. 2,048-bit
C. 56-bit
D. 112-bit
Answer: D
Explanation:
3DES (Triple DES) applies the DES block cipher three times to increase effective security, and its commonly cited valid key sizes correspond to how many independent DES keys are used. Two-key 3DES uses two 56- bit DES keys (K1 and K2) in an EDE sequence (Encrypt with K1, Decrypt with K2, Encrypt with K1), yielding 112 bits of keying material (ignoring parity bits). Three-key 3DES uses three independent 56-bit keys for a total of 168 bits of keying material, but that option is not listed here. A 56-bit key corresponds to single DES, not 3DES. 128-bit is associated with AES, not 3DES. 2,048-bit is typical for RSA keys, not symmetric ciphers. Therefore, among the choices provided, 112-bit is a valid 3DES key size. While 3DES is now deprecated for many uses due to its 64-bit block size and performance limitations, understanding its keying options remains important for legacy system assessment.

NO.3 (Which type of encryption is Advanced Encryption Standard (AES) considered to be?)
A. Hybrid encryption
B. Quantum encryption
C. Asymmetric encryption

D. Symmetric encryption

Answer: D

Explanation:

AES is a symmetric-key block cipher, meaning the same shared secret key is used for both encryption and decryption. It operates on fixed-size 128-bit blocks and supports key sizes of 128, 192, and 256 bits. Being symmetric, AES is efficient and well-suited for encrypting large volumes of data-files, disk encryption, VPN payloads, and bulk traffic in protocols like TLS once a session key is established. AES is not "hybrid" by itself; hybrid encryption refers to combining asymmetric cryptography (for key exchange or key wrapping) with symmetric cryptography (for bulk data encryption), and AES often plays the symmetric part of that hybrid design. It is not "quantum encryption," which is a separate, loosely used term sometimes referring to quantum key distribution or quantum-resistant algorithms. AES is also not asymmetric; it does not use public
/private key pairs. Therefore, AES is correctly classified as symmetric encryption, matching option D.

NO.4 (What describes a true random number generator?)

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.

NO.5 (What is a component of a one-time password (OTP) that is needed to guess future iterations of passwords?)

A. Function

B. Initialization vector

C. Encryption algorithm

D. Seed

Answer: D

Explanation:

OTP systems (such as HOTP and TOTP) generate a sequence of passwords using a shared secret and a moving factor (counter or time). The critical secret that underpins the ability to compute past or

future OTP values is the seed (also called the shared secret key). In HOTP, the seed is used with an HMAC function and an incrementing counter; in TOTP, the seed is used with HMAC and a time-step value. If an attacker obtains the seed and knows the algorithm and moving factor, they can compute future OTPs. The "function" and
"encryption algorithm" are typically standardized and public; security relies on keeping the seed secret. An initialization vector is not a standard OTP component in HOTP/TOTP generation.
Therefore, the component needed to predict future OTP values is the seed. Protecting the seed is essential: it should be stored securely (e.
g., hardware token secure storage) and transmitted only through controlled provisioning processes. If compromised, OTP becomes predictable and no longer serves as a strong second factor.

NO.6 (An organization wants to digitally sign its software to guarantee the integrity of its source code. Which key should the customer use to decrypt the digest of the source code?)

A. Customer's private key

B. Organization's public key

C. Organization's private key

D. Customer's public key

Answer: B

Explanation:
When software is digitally signed, the organization computes a cryptographic hash (digest) of the software (or its manifest) and then signs that digest using the organization's private key. Verification works in the opposite direction: the customer (verifier) uses the organization's public key to validate the signature and recover
/confirm the signed digest, then independently hashes the received software and compares the result. If the digests match and the signature validates under the public key, the customer has strong assurance that the software has not been altered since it was signed and that it was signed by the holder of the corresponding private key. The customer never needs the organization's private key-sharing it would destroy security and enable forgery. Likewise, the customer's own keys are irrelevant to verifying the publisher's signature. The organization's public key is typically delivered inside a certificate chain (code signing certificate) so the verifier can also validate publisher identity and trust. Therefore, the customer uses the organization's public key for signature verification (often described as "decrypting" the signed digest).

NO.7 (Which symmetric encryption technique uses a 256-bit key size and a 128-bit block size?)

A. 3DES

B. DES

C. IDEA

D. AES

Answer: D

Explanation:
AES (Advanced Encryption Standard) is a symmetric block cipher standardized to operate on a fixed 128-bit block size and supports key sizes of 128, 192, and 256 bits. When the key size is 256 bits, the cipher is commonly referred to as AES-256, but the block size remains 128 bits regardless of key length. This combination (256-bit key, 128-bit block) matches the question precisely. By comparison, DES uses a 64-bit block size with a 56-bit effective key. 3DES also uses a 64-bit block size and

effectively applies DES three times, yielding an effective key length typically cited as 112 bits (two-key 3DES) or 168 bits (three-key
3DES), depending on how keys are configured. IDEA uses a 64-bit block size with a 128-bit key. Therefore, the only listed algorithm that supports a 256-bit key while maintaining a 128-bit block size is AES. This is one reason AES is widely adopted for modern symmetric encryption: strong key sizes with efficient implementation and broad standardization.

NO.8 (What makes the RC4 cipher unique compared to RC5 and RC6?)
A. Stream
B. Asymmetric
C. Symmetric
D. Block
Answer: A
Explanation:
RC4 is unique among the RC family listed because it is a stream cipher. It generates a pseudorandom keystream and encrypts data by XORing that keystream with plaintext bytes (and decryption is the same XOR operation). This differs from RC5 and RC6, which are block ciphers: they encrypt fixed-size blocks of data through multiple rounds of operations (such as modular addition, XOR, and rotations) using a secret key. The stream-cipher design means RC4 historically fit protocols where data arrives continuously (e.g., early wireless and web encryption) and where simple, fast software implementation was desired. However, stream ciphers demand careful handling of nonces/IVs to avoid keystream reuse; reuse can catastrophically leak plaintext relationships. RC4 also has well-documented statistical biases in its keystream, leading to practical attacks in protocols like WEP and later concerns in TLS, which is why RC4 has been deprecated in modern security standards. Still, from a classification standpoint, "stream" is the distinguishing characteristic versus RC5/RC6 being block ciphers.

NO.9 (An administrator has configured a Virtual Private Network (VPN) connection utilizing IPsec transport mode with Encapsulating Security Payload (ESP) between a server in the corporate office and a client computer in the remote office. In which situation can the packet content be inspected?)
A. On devices at headquarters and offsite before being sent and after being received
B. In the headquarters' and offsite location's networks after the data has been sent
C. Only in the offsite location's network while data is in transit
D. Only in the headquarters' network while data is in transit
Answer: A
Explanation:
With IPsec ESP in transport mode, the payload of the original IP packet (typically the transport-layer segment and higher) is encrypted and integrity-protected between the two endpoints-here, the corporate server and the remote client. Because encryption is applied by the sending endpoint and removed only by the receiving endpoint, intermediate routers, switches, and monitoring devices in either network cannot view the protected payload while it is in transit. They may see outer IP headers and certain metadata needed for routing, but not the encrypted content protected by ESP. As a result, the packet's contents are inspectable only at the endpoints: before encryption on the sender (plaintext exists in memory/stack before IPsec processing) and after decryption on the receiver (plaintext is restored for the application). This is true whether the traffic traverses internal

networks or the Internet; the cryptographic boundary is between the endpoints participating in the IPsec SA. Therefore, inspection of the actual content is possible only on the devices at headquarters and offsite, before sending and after receiving, not by in-transit networks.

NO.10 (What is an example of a block cipher mode of operation?)

A. Secure Hash Algorithm 256 (SHA-256)

B. Digital Signature Algorithm (DSA)

C. Rivest-Shamir-Adleman (RSA)

D. Electronic Codebook (ECB)

Answer: D

Explanation:

A block cipher mode of operation defines how a block cipher (such as AES) is applied to data longer than a single block, and how blocks are linked (or not linked) to provide certain security properties. ECB (Electronic Codebook) is one of the canonical block cipher modes: it encrypts each plaintext block independently using the same key. While ECB is generally discouraged because it leaks patterns (identical plaintext blocks produce identical ciphertext blocks), it is still a valid and historically important mode of operation and is often used as a teaching example of what not to do for structured data. In contrast, SHA-256 is a hash function (one- way digest) and not a mode for block ciphers. DSA is a digital signature algorithm and provides authenticity /integrity, not encryption mode behavior. RSA is an asymmetric cryptosystem, not a block cipher mode.

Therefore, among the options, ECB is the correct example of a block cipher mode of operation.