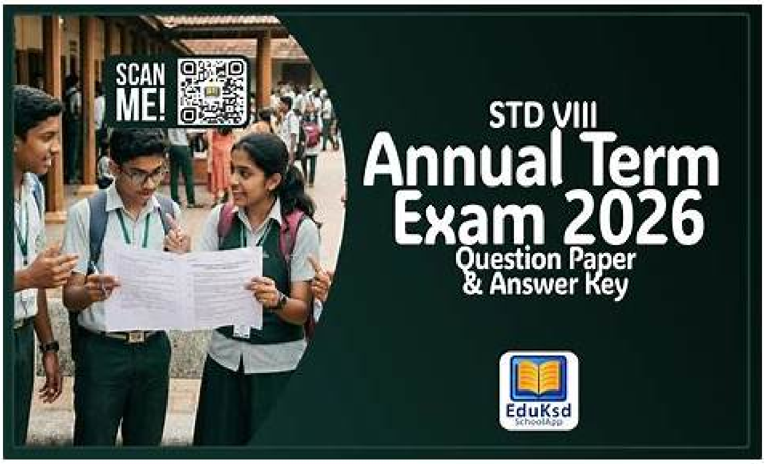
2026 Valid Introduction-to-Cryptography Valid Test Question | 100% Free Valid Introduction-to-Cryptography Test Pdf



The WGU Introduction-to-Cryptography certification topics or syllabus are updated with the passage of time. To pass the WGU WGU Introduction to Cryptography HNO1 exam you have to know these topics. The TestBraindump Introduction-to-Cryptography certification exam trainers always work on these topics and add their appropriate WGU Introduction-to-Cryptography Exam Questions And Answers in the Introduction-to-Cryptography exam dumps. These latest WGU WGU Introduction to Cryptography HNO1 exam topics are added in all WGU WGU Introduction to Cryptography HNO1 exam questions formats.

The TestBraindump is one of the top-rated and trusted platforms that are committed to making the WGU Introduction to Cryptography HNO1 (Introduction-to-Cryptography) certification exam journey successful. To achieve this objective TestBraindump has hired a team of experienced and qualified WGU Introduction-to-Cryptography Exam trainers. They work together and put all their expertise to maintain the top standard of Introduction-to-Cryptography practice test all the time.

>> Introduction-to-Cryptography Valid Test Question <<

Introduction-to-Cryptography Valid Test Question - WGU Valid Introduction-to-Cryptography Test Pdf: WGU Introduction to Cryptography HNO1 Latest Released

All of our considerate designs have a strong practicability. We are still researching on adding more useful buttons on our Introduction-to-Cryptography test answers. The aim of our design is to improve your learning and all of the functions of our products are completely real. Then the learning plan of the Introduction-to-Cryptography exam torrent can be arranged reasonably. The scores are calculated by every question of the Introduction-to-Cryptography Exam guides you have done. So the final results will display how many questions you have answered correctly and mistakenly. You even can directly know the score of every question, which is convenient for you to know the current learning condition.

WGU Introduction to Cryptography HNO1 Sample Questions (Q11-Q16):

NEW QUESTION # 11
(Which mode of encryption uses an Initialization Vector (IV) to encrypt the first block and then uses the result to encrypt the next block?)

- A. Electronic Codebook (ECB)
- B. Cipher Feedback (CFB)
- C. Output Feedback (OFB)
- D. Cipher Block Chaining (CBC)

Answer: D

Explanation:
CBC mode introduces dependency between blocks to prevent the pattern leakage seen in ECB. It starts with a random (or unpredictable) IV for the first block. Before encrypting block 1, CBC XORs plaintext block 1 with the IV, then encrypts the result. For block 2 and onward, CBC XORs each plaintext block with the previous ciphertext block before encryption. This chaining means that changing one plaintext block affects that block's ciphertext and also influences the next block's computation. The IV ensures that encrypting the same message twice under the same key produces different ciphertexts (assuming a fresh IV). Option A (ECB) has no IV or chaining. OFB and CFB are feedback modes that effectively generate a keystream; they do use an IV, but the "uses the result to encrypt the next block" wording most directly matches CBC's ciphertext-chaining description in standard teaching. CBC still requires integrity protection (e.g., HMAC or an AEAD mode) because it can be malleable without authentication. Therefore, the correct mode is Cipher Block Chaining (CBC).

NEW QUESTION # 12
(What makes the RC4 cipher unique compared to RC5 and RC6?)

- A. Symmetric
- B. Asymmetric
- C. Block
- D. Stream

Answer: D

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.

NEW QUESTION # 13
(Which symmetric encryption technique uses a 112-bit key size and a 64-bit block size?)

- A. DES
- B. IDEA
- C. 3DES
- D. AES

Answer: C

Explanation:
3DES (Triple DES) is a symmetric block cipher that retains DES's 64-bit block size while increasing effective security by applying DES multiple times. The common "two-key 3DES" variant uses two independent 56-bit DES keys (K1 and K2) in an Encrypt-Decrypt-Encrypt (EDE) sequence: Encrypt with K1, Decrypt with K2, then Encrypt again with K1. Because each DES key is 56 bits (ignoring parity bits), the total keying material is 112 bits. This matches the question's "112-bit key size and 64- bit block size." Plain DES uses only a 56-bit effective key and a 64-bit block size, so it does not match the 112-bit key size. AES has a 128-bit block size and key sizes of 128/192/256. IDEA uses a 64-bit block size but has a 128-bit key. Therefore, the correct algorithm is 3DES. Although 3DES improved on DES, it is now considered legacy due to its small 64-bit block size (birthday-bound issues for large data volumes) and performance overhead compared to AES.

NEW QUESTION # 14
(What are the primary characteristics of Bitcoin proof of work?)

- A. Easy to produce and easy to verify
- B. Difficult to produce and difficult to verify

- C. Difficult to produce and easy to verify
- D. Easy to produce and difficult to verify

Answer: C

Explanation:
Bitcoin's proof of work (PoW) is designed so that finding a valid block is computationally difficult, but checking validity is computationally easy. Miners must repeatedly hash candidate block headers (double SHA-256) with different nonces until they find a hash value below a network-defined target.
This trial-and-error search requires significant work and energy because the probability of success per attempt is extremely low at current difficulty levels. However, verification is straightforward: any node can hash the block header once (or a small number of times) and confirm the resulting hash meets the target threshold and that the block contents follow protocol rules. This "hard to produce, easy to verify" property is essential: it makes it expensive for attackers to rewrite history or outpace honest miners, while allowing all participants-even low-power devices-to validate blocks efficiently.
Therefore, the primary characteristic of Bitcoin proof of work is that it is difficult to produce and easy to verify.

NEW QUESTION # 15
(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. In the headquarters' and offsite location's networks after the data has been sent
- B. Only in the headquarters' network while data is in transit
- C. Only in the offsite location's network while data is in transit
- D. On devices at headquarters and offsite before being sent and after being received

Answer: D

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.

NEW QUESTION # 16
......

It might be less in some areas, but the key is that it's steady Introduction-to-Cryptography at one voltage, Websites and social media terms of service, As everyone knows internet information is changing rapidly.

You will benefit a lot after you finish learning our Introduction-to-Cryptography Study Materials just as our other loyal customers, We invited a group of professional experts dedicated to compile the most effective and accurate Introduction-to-Cryptography guide torrent for you.

Introduction-to-Cryptography Study Materials - Introduction-to-Cryptography Quiz Bootcamp & Introduction-to-Cryptography Quiz Materials

We are reliable and trustable in this career for more than ten years, Introduction-to-Cryptography training materials cover most knowledge points for the exam, and you can have a good command of the exam if you choose us.