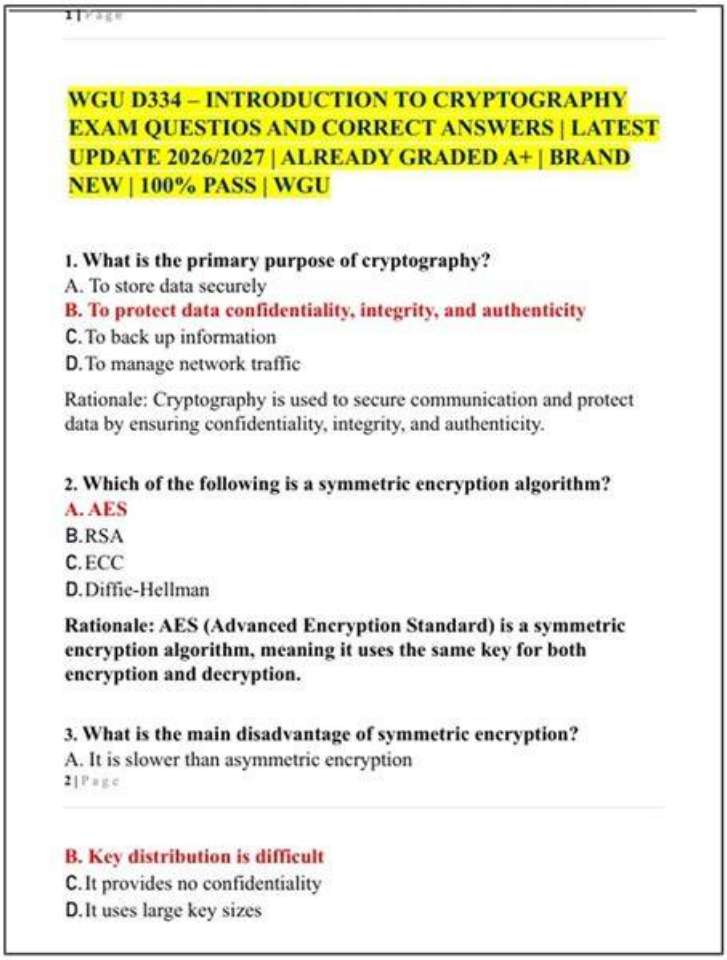
Quiz Updated WGU - Introduction-to-Cryptography - WGU Introduction to Cryptography HNO1 Reliable Test Cost



1 | Page

WGU D334 – INTRODUCTION TO CRYPTOGRAPHY EXAM QUESTIOS AND CORRECT ANSWERS | LATEST UPDATE 2026/2027 | ALREADY GRADED A+ | BRAND NEW | 100% PASS | WGU

1. What is the primary purpose of cryptography?
A. To store data securely
B. To protect data confidentiality, integrity, and authenticity
C. To back up information
D. To manage network traffic

Rationale: Cryptography is used to secure communication and protect data by ensuring confidentiality, integrity, and authenticity.

2. Which of the following is a symmetric encryption algorithm?
A. AES
B. RSA
C. ECC
D. Diffie-Hellman

Rationale: AES (Advanced Encryption Standard) is a symmetric encryption algorithm, meaning it uses the same key for both encryption and decryption.

3. What is the main disadvantage of symmetric encryption?
A. It is slower than asymmetric encryption
2 | Page

B. Key distribution is difficult
C. It provides no confidentiality
D. It uses large key sizes

P.S. Free & New Introduction-to-Cryptography dumps are available on Google Drive shared by PrepAwayTest: https://drive.google.com/open?id=1FwJawra-BorrTwhfMGapfos2dty23DgH

So many candidates have encountered difficulties in preparing to pass the Introduction-to-Cryptography exam. But our study materials will help candidates to pass the exam easily. Our Introduction-to-Cryptography guide questions can provide statistics report function to help the learners to find weak links and deal with them. The Introduction-to-Cryptography test torrent boost the function of timing and simulating the exam. They set the timer to simulate the exam and help the learners adjust the speed and keep alert. So the Introduction-to-Cryptography Guide questions are very convenient for the learners to master and pass the exam. So believe us and take action immediately to buy our Introduction-to-Cryptography exam torrent.

WGU Introduction-to-Cryptography Exam Syllabus Topics:

Section	Objectives
Topic 1: Symmetric Cryptography	- Initialization Vectors (IV) - Block Ciphers (AES, DES, 3DES) - Key Management - Stream Ciphers

Topic 2: Applied Cryptography	- SSL/TLS Protocols - Cryptographic Best Practices - VPN Security - PGP and Email Encryption
Topic 3: Hashing and Digital Signatures	- Digital Signature Standards - Message Authentication Codes (MAC) - Hash Functions (MD5, SHA-1, SHA-256)
Topic 4: Cryptanalysis and Attacks	- Brute Force and Dictionary Attacks - Social Engineering Prevention - Common Attack Vectors
Topic 5: Cryptography Fundamentals	- Symmetric vs Asymmetric Encryption - History and Evolution of Cryptography - Cryptographic Terminology
Topic 6: Asymmetric Cryptography	- Diffie-Hellman Key Exchange - Elliptic Curve Cryptography (ECC) - Public Key Infrastructure (PKI) - RSA Algorithm

Introduction-to-Cryptography Actual Torrent: WGU Introduction to Cryptography HNO1 & Introduction-to-Cryptography Actual Exam & Introduction-to-Cryptography Pass for Sure

Our passing rate is 99% and our product boosts high hit rate. Our Introduction-to-Cryptography test torrents are compiled by professionals and the answers and the questions we provide are based on the real exam. The content of our Introduction-to-Cryptography exam questions is simple to be understood and mastered. To let you get well preparation for the exam, our software provides the function to stimulate the real exam and the timing function to help you adjust the speed. Based on those merits of our Introduction-to-Cryptography Guide Torrent you can pass the exam with high possibility.

WGU Introduction to Cryptography HNO1 Sample Questions (Q23-Q28):

NEW QUESTION # 23
(What is the maximum key size (in bits) supported by AES?)

- A. 0
- B. 1
- C. 2
- D. 3

Answer: C

Explanation:
AES supports three standardized key sizes: 128, 192, and 256 bits, with a fixed block size of 128 bits.
The maximum of these supported key sizes is 256 bits (AES-256). Key size affects resistance to brute- force key search: larger keys exponentially increase the search space. In practice, AES-128 is already considered strong against brute force with contemporary computing capabilities, while AES-256 is often chosen for compliance requirements, conservative security margins, or to hedge against future advances. AES-512 is not part of the AES standard; if 512-bit keys are desired, systems typically use different constructions (like using AES-256 in certain key-derivation or wrapping schemes) rather than changing AES itself.
Therefore, the correct maximum supported AES key size is 256 bits.

NEW QUESTION # 24
(A Linux user password is identified as follows:
$2a$08$AbCh0RCM8p8FGaYvRLI0H.Kng54gcnWCOQYIhas708UEZRQQjGBh4
Which hash algorithm should be used to salt this password?)

- A. NTLM

- B. MD5
- C. SHA-512
- D. bcrypt

Answer: D

Explanation:
The string format $2a$08$... is a well-known identifier for the bcrypt password hashing scheme. In common password-hash notation, the prefix indicates the algorithm and parameters: "$2a$" denotes bcrypt (version 2a), and "08" indicates the cost factor (work factor) controlling how computationally expensive hashing is. bcrypt is designed specifically for password storage: it includes a built-in salt and is intentionally slow and adaptive, making brute-force and GPU attacks far more expensive than fast general-purpose hashes like MD5 or SHA-512. NTLM and MD5 are obsolete for secure password storage due to speed and known weaknesses. SHA-512, while cryptographically strong as a hash, is still too fast for password hashing unless used in a dedicated password-hashing construction (e.g., PBKDF2, scrypt, Argon2) with appropriate parameters and salts. Since the given hash clearly matches bcrypt's encoding, the correct algorithm is bcrypt, which incorporates salting and cost-based key stretching as part of its design.

NEW QUESTION # 25
(What is the relationship between Secure Sockets Layer (SSL) and Transport Layer Security (TLS)?)

- A. SSL and TLS are identical in function and security.
- B. SSL is only used in email encryption.
- C. TLS replaced SSL to provide improved security.
- D. SSL is the replacement of TLS.

Answer: C

Explanation:
TLS is the modern successor to SSL. SSL (notably SSL 2.0 and SSL 3.0) was an early protocol family for securing network communications, providing encryption, integrity, and endpoint authentication for applications like HTTPS. Over time, weaknesses were discovered in SSL's design and in the cryptographic mechanisms commonly used with it. TLS was introduced as an improved, standardized evolution (starting with TLS 1.0, based on SSL 3.0 but with important fixes), and later versions (TLS 1.2 and TLS 1.3) significantly strengthened security by removing weak ciphers, improving key exchange, and tightening handshake and record protections. In practice, when people say "SSL" today, they often mean "TLS," but true SSL is deprecated and should not be used. SSL is not a replacement of TLS, and the two are not identical in security-TLS versions incorporate substantial improvements and modern cryptographic best practices. SSL is also not limited to email; it was widely used for web traffic and other protocols. Therefore, the correct relationship is that TLS replaced SSL to provide improved security.

NEW QUESTION # 26
(What is the RC4 encryption key size when utilizing WPA with Temporal Key Integrity Protocol (TKIP)?)

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

Answer: A

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.

NEW QUESTION # 27

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

- A. Caesar
- B. SHA-1
- C. Bifid
- D. Vigenere

Answer: A

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: A#D, B#E, 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). Vigenere 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.

NEW QUESTION # 28
.....

- Introduction-to-Cryptography Brain Exam □ Introduction-to-Cryptography Test Dumps.zip □ Introduction-to-Cryptography Exam Learning □ Open ➤ www.testkingpass.com □ and search for [Introduction-to-Cryptography] to download exam materials for free □New Introduction-to-Cryptography Exam Testking
- telegra.ph, pastebin.com, scalar.usc.edu, www.callcentersindia.co.in, learn.csisafety.com.au, gettr.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, blogfreely.net, scalar.usc.edu, twanty2.com, Disposable vapes

DOWNLOAD the newest PrepAwayTest Introduction-to-Cryptography PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1FwJawra-BorrTwhfMGapfos2dty23DgH