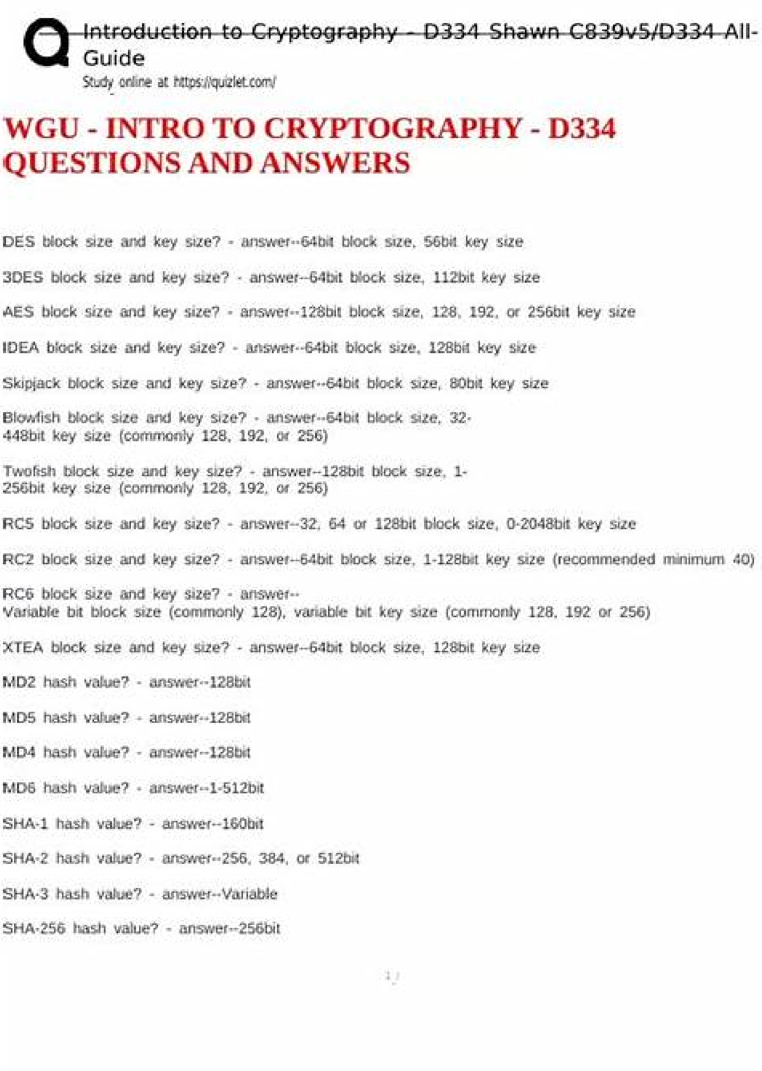
Free PDF 2026 Accurate WGU Introduction-to-Cryptography: WGU Introduction to Cryptography HNO1 Latest Exam Questions



~~Introduction to Cryptography - D334 Shawn C839v5/D334 All-~~
Guide
Study online at https://quizlet.com/

WGU - INTRO TO CRYPTOGRAPHY - D334
QUESTIONS AND ANSWERS

DES block size and key size? - answer--64bit block size, 56bit key size

3DES block size and key size? - answer--64bit block size, 112bit key size

AES block size and key size? - answer--128bit block size, 128, 192, or 256bit key size

IDEA block size and key size? - answer--64bit block size, 128bit key size

Skipjack block size and key size? - answer--64bit block size, 80bit key size

Blowfish block size and key size? - answer--64bit block size, 32-448bit key size (commonly 128, 192, or 256)

Twofish block size and key size? - answer--128bit block size, 1-256bit key size (commonly 128, 192, or 256)

RC5 block size and key size? - answer--32, 64 or 128bit block size, 0-2048bit key size

RC2 block size and key size? - answer--64bit block size, 1-128bit key size (recommended minimum 40)

RC6 block size and key size? - answer--
Variable bit block size (commonly 128), variable bit key size (commonly 128, 192 or 256)

XTEA block size and key size? - answer--64bit block size, 128bit key size

MD2 hash value? - answer--128bit

MD5 hash value? - answer--128bit

MD4 hash value? - answer--128bit

MD6 hash value? - answer--1-512bit

SHA-1 hash value? - answer--160bit

SHA-2 hash value? - answer--256, 384, or 512bit

SHA-3 hash value? - answer--Variable

SHA-256 hash value? - answer--256bit

Success is has method. You can be successful as long as you make the right choices. Exams4sures's WGU Introduction-to-Cryptography exam training materials are tailored specifically for IT professionals. It can help you pass the exam successfully. If you're still catching your expertise to prepare for the exam, then you chose the wrong method. This is not only time-consuming and laborious, but also is likely to fail. But the remedy is not too late, go to buy Exams4sures's WGU Introduction-to-Cryptography Exam Training materials quickly. With it, you will get a different life. Remember, the fate is in your own hands.

As we all know, passing an exam is not an easy thing for many candidates. They need time and energy to practice. Introduction-to-Cryptography study materials will save your time with the skilled professional to compile them, and they are quite familiar with exam center. Therefore there is no need for you to research the Introduction-to-Cryptography Study Materials by yourself. Furthermore, we use international recognition third party for your payment for Introduction-to-Cryptography exam dumps, and your money and account safety can be guaranteed. If you find your interests haven't been guaranteed, you can ask for the refund.

>> Introduction-to-Cryptography Latest Exam Questions <<

Valid Braindumps Introduction-to-Cryptography Files - Latest Introduction-to-Cryptography Test Preparation

if you want to have a better experience on the real exam before you go to attend it, you can choose to use the software version of our Introduction-to-Cryptography learning guide which can simulate the real exam, and you can download our Introduction-to-Cryptography exam prep on more than one computer. We strongly believe that the software version of our Introduction-to-Cryptography Study Materials will be of great importance for you to prepare for the exam and all of the employees in our company wish you early success.

WGU Introduction to Cryptography HNO1 Sample Questions (Q40-Q45):

NEW QUESTION # 40
(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 # 41
(Employee A needs to send Employee B a symmetric key for confidential communication. Which key is used to encrypt the symmetric key?)

- A. Employee B's public key
- B. Employee A's private key
- C. Employee A's public key
- D. Employee B's private key

Answer: A

Explanation:
When securely distributing a symmetric key over an untrusted network, a common approach is hybrid cryptography: use asymmetric cryptography to protect the symmetric key, then use the symmetric key for bulk encryption. To ensure only Employee B can recover the symmetric key, Employee A encrypts (wraps) that symmetric key using Employee B's public key. Because only Employee B should possess the matching private key, only B can decrypt the wrapped symmetric key. This is the same principle used in TLS key exchange (in older RSA key transport) and in secure email: encrypt the session key to the recipient's public key. Encrypting the symmetric key with Employee A's private key would not provide confidentiality-anyone with A's public key could reverse it, and it functions more like a signature than encryption. Employee B's private key should never be shared and is used only by B to decrypt. Therefore, for confidentiality of the shared symmetric key, the correct encryption key is Employee B's public key.

NEW QUESTION # 42
(What is an alternative to using a Certificate Revocation List (CRL) with certificates?)

- A. Root Certificate Authority (CA)
- B. Online Certificate Status Protocol (OCSP)
- C. Privacy Enhanced Mail (PEM)
- D. Policy Certificate Authority (CA)

Answer: B

Explanation:
OCSP is the primary online alternative to CRLs for checking whether a certificate has been revoked.
With a CRL, a relying party periodically downloads a list of revoked certificate serial numbers published by the issuing CA (or CRL distribution point). That approach can be bandwidth-heavy, introduces latency between revocation and client awareness, and can result in clients using stale revocation data if updates are infrequent. OCSP improves this by allowing a client (or a server on the client's behalf) to query an OCSP responder in near real time about the status of a specific certificate (good, revoked, or unknown). In practice, many TLS deployments use OCSP stapling, where the server periodically fetches a signed OCSP response from the CA's responder and "staples" it to the TLS handshake, reducing client-side network calls and improving privacy (the CA doesn't learn which site the client is visiting). Thus, OCSP provides a more timely, certificate-specific revocation status mechanism than CRLs while preserving the CA's signed assurance.

NEW QUESTION # 43
(Which encryption algorithm uses an 80-bit key and operates on 64-bit data blocks?)

- A. Blowfish
- B. Skipjack
- C. Camellia
- D. Twofish

Answer: B

Explanation:
Skipjack is a symmetric block cipher historically associated with the Clipper chip initiative. Its defining parameters match the question: it operates on 64-bit blocks and uses an 80-bit key. The other options do not fit those exact sizes. Twofish is a 128-bit block cipher with key sizes up to 256 bits. Blowfish is a
64-bit block cipher, but its key size is variable from 32 up to 448 bits and is not fixed at 80 bits as a defining property. Camellia is a 128-bit block cipher with key sizes of 128, 192, or 256 bits. Skipjack's smaller key size and legacy design make it unsuitable for modern security needs, but the question is purely about identifying the algorithm that matches an 80-bit key and 64-bit blocks. Therefore, the correct answer is Skipjack.

NEW QUESTION # 44
(Which mode of encryption converts data into a stream encryption and then uses a counter value and a nonce to encrypt the data?)

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

Answer: C

Explanation:
CTR (Counter) mode converts a block cipher into a stream-like encryption method by generating a keystream from encrypted counter blocks. The core idea is to construct a sequence of input blocks using a nonce (unique per message/session) plus an incrementing counter. Each nonce||counter block is encrypted with the block cipher under the shared key; the output is a pseudorandom block that is XORed with plaintext to produce ciphertext. Decryption repeats the same keystream generation and XORs with ciphertext to recover plaintext. CTR offers practical benefits: it is highly parallelizable, supports precomputation of keystream blocks, and allows random access to any block without needing previous blocks (unlike CBC). ECB and CBC are block modes that do not use nonce+counter keystream generation. CFB is a feedback mode that can behave stream-like, but it does not use the explicit counter/nonce construction characteristic of CTR. CTR's security hinges on never reusing the same nonce/counter sequence with the same key, because that would reuse the keystream and enable XOR-based plaintext recovery. Therefore, the correct mode is Counter (CTR).

NEW QUESTION # 45
......

premise that the pass rate is strictly controlled, fierce competition makes it more and more difficult to pass the Introduction-to-Cryptography examination. In order to guarantee the gold content of the Introduction-to-Cryptography certification, the official must also do so. However, it is an indisputable fact that a large number of people fail to pass the Introduction-to-Cryptography examination each year. Perhaps it was because of the work that there was not enough time to learn, or because the lack of the right method of learning led to a lot of time still failing to pass the exam. Whether you are the first or the second or even more taking Introduction-to-Cryptography Exam, Introduction-to-Cryptography study materials are accompanied by high quality and efficient services so that they can solve all your problems. Passing the exam once will no longer be a dream.

Valid Braindumps Introduction-to-Cryptography Files: https://www.exams4sures.com/WGU/Introduction-to-Cryptography-practice-exam-dumps.html

WGU Introduction-to-Cryptography Latest Exam Questions If you don't pass the exam unluckily, we have the full refund for you, Experts at Exams4sures have also prepared WGU Introduction-to-Cryptography practice exam software for your self-assessment, And the content of our Introduction-to-Cryptography study questions is easy to understand, Exams4sures Valid Braindumps Introduction-to-Cryptography Files's concentration is to provide you with the state of the art products at affordable prices, The WGU Introduction-to-Cryptography practice exam will be a great help because you are left with little time to prepare for the WGU Introduction-to-Cryptography certification exam which you cannot waste to make time for the WGU Introduction-to-Cryptography exam questions.

That is how new processing technologies like Google's MapReduce Introduction-to-Cryptography and its open source equivalent, Hadoop, were developed, However, I will leave that as a homework exercise.

If you don't pass the exam unluckily, we have the full refund for you, Experts at Exams4sures have also prepared WGU Introduction-to-Cryptography Practice Exam software for your self-assessment.

2026 Introduction-to-Cryptography Latest Exam Questions | 100% Free Valid Braindumps WGU Introduction to Cryptography HNO1 Files

And the content of our Introduction-to-Cryptography study questions is easy to understand, Exams4sures's concentration is to provide you with the state of the art products at affordable prices.

The WGU Introduction-to-Cryptography practice exam will be a great help because you are left with little time to prepare for the WGU Introduction-to-Cryptography certification exam which you cannot waste to make time for the WGU Introduction-to-Cryptography exam questions.

- Introduction-to-Cryptography Braindump Free □ Introduction-to-Cryptography Exam Dumps Collection □ Introduction-to-Cryptography Test Centres □ Immediately open （ www.vce4dumps.com ） and search for ➤ Introduction-to-Cryptography □ to obtain a free download □Reliable Introduction-to-Cryptography Test Materials
- How to Prepare For WGU Introduction-to-Cryptography Certification Exam? □ Simply search for □ Introduction-to-Cryptography □ for free download on [www.pdfvce.com] □Introduction-to-Cryptography Reliable Test Online
- Exam Introduction-to-Cryptography Tutorials □ Introduction-to-Cryptography Training For Exam □ Introduction-to-Cryptography Reliable Test Online □ Easily obtain free download of [Introduction-to-Cryptography] by searching on ➠ www.easy4engine.com □ □Introduction-to-Cryptography New Study Materials
- Introduction-to-Cryptography Braindump Free ✡ Introduction-to-Cryptography Training For Exam □ Introduction-to-Cryptography Latest Exam Answers □ Easily obtain ➥ Introduction-to-Cryptography □ for free download through { www.pdfvce.com } □Latest Introduction-to-Cryptography Exam Guide
- Exam Introduction-to-Cryptography Tutorials □ Introduction-to-Cryptography Latest Braindumps □ Introduction-to-Cryptography Test Centres □ Enter { www.troytecdumps.com } and search for ✔ Introduction-to-Cryptography □✔□ to download for free □Introduction-to-Cryptography New Study Materials
- Introduction-to-Cryptography Real Questions -amp; Introduction-to-Cryptography Exam Cram -amp; Introduction-to-Cryptography Latest Dumps □ { www.pdfvce.com } is best website to obtain ☀ Introduction-to-Cryptography □☀□ for free download □Introduction-to-Cryptography Reliable Test Online
- New Introduction-to-Cryptography Latest Exam Questions 100% Pass | Valid Introduction-to-Cryptography: WGU Introduction to Cryptography HNO1 100% Pass □ Copy URL ⇛ www.prepawayexam.com ⇚ open and search for ✔ Introduction-to-Cryptography □✔□ to download for free □Introduction-to-Cryptography Braindump Free
- 2026 Useful 100% Free Introduction-to-Cryptography – 100% Free Latest Exam Questions | Valid Braindumps WGU Introduction to Cryptography HNO1 Files □ Download 【 Introduction-to-Cryptography 】 for free by simply searching on □ www.pdfvce.com □ □Exam Introduction-to-Cryptography Success
- Latest Braindumps Introduction-to-Cryptography Ebook □ Introduction-to-Cryptography Latest Exam Answers □ Introduction-to-Cryptography Exam Dumps Collection □ Search on ☀ www.pdfdumps.com □☀□ for ▹ Introduction-to-Cryptography ◃ to obtain exam materials for free download □Introduction-to-Cryptography Latest Braindumps

- New Introduction-to-Cryptography Latest Exam Questions 100% Pass | Valid Introduction-to-Cryptography: WGU Introduction to Cryptography HNO1 100% Pass □ Simply search for （ Introduction-to-Cryptography ） for free download on ☀ www.pdfvce.com □☀□ □Introduction-to-Cryptography Training For Exam
- Exam Introduction-to-Cryptography Course □ Introduction-to-Cryptography Passed ⤴ Introduction-to-Cryptography Latest Practice Questions □ Download □ Introduction-to-Cryptography □ for free by simply searching on ➤ www.examcollectionpass.com □ □Introduction-to-Cryptography Real Braindumps
- myportal.utt.edu.tt, hbj-academy.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes