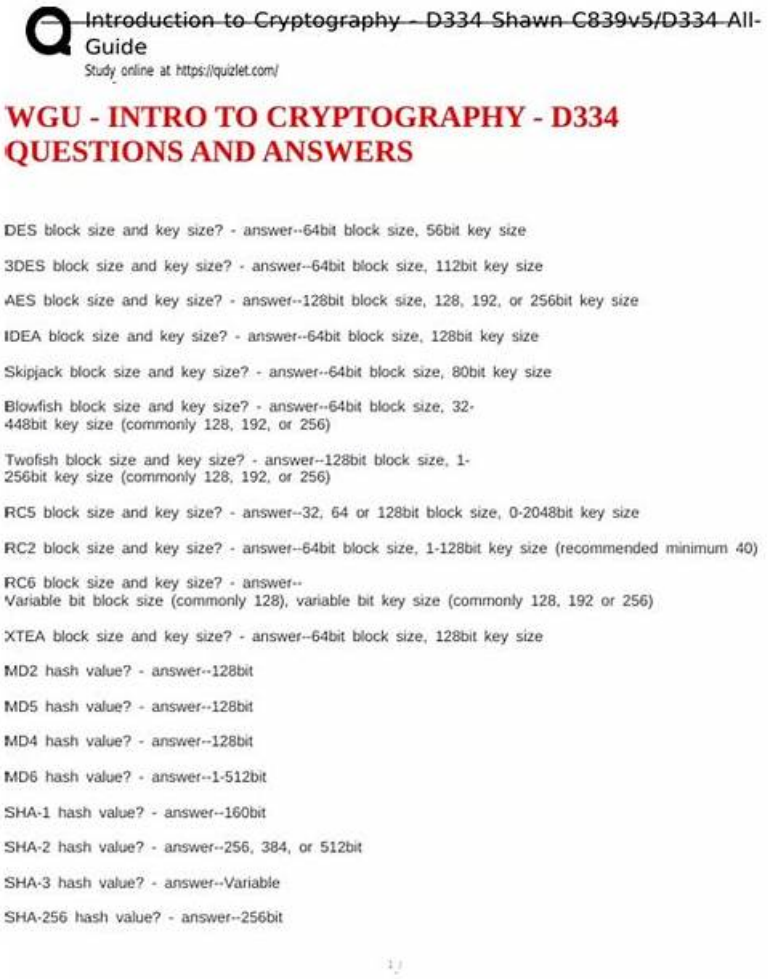
Quiz 2026 WGU Authoritative Introduction-to-Cryptography Reliable Cram Materials


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

We are equipped with excellent materials covering most of knowledge points of Introduction-to-Cryptography pdf torrent. Our learning materials in PDF format are designed with Introduction-to-Cryptography actual test and the current exam information. Questions and answers are available to download immediately after you purchased our Introduction-to-Cryptography Dumps PDF. The free demo of pdf version can be downloaded in our exam page.

Our company is thoroughly grounded in our values. They begin with a prized personal and organizational quality--Integrity--and end with a shared concern for the candidates who are preparing for the Introduction-to-Cryptography exam. Our values include Innovation, Teamwork, Customer Focus, and Respect for Customers. These Introduction-to-Cryptography values guide every decision we make, everywhere we make them. As you can sense by now, and we really hope that you can be the next beneficiary of our Introduction-to-Cryptography training materials. You can just free download the demo of our Introduction-to-Cryptography training materials to check.

>> Introduction-to-Cryptography Reliable Cram Materials <<

JOIN WGU Introduction-to-Cryptography TO CLINCH IN YOUR CERTIFICATION

We strongly recommend using our WGU Introduction to Cryptography HNO1 (Introduction-to-Cryptography) exam dumps to

prepare for the WGU Introduction-to-Cryptography certification. It is the best way to ensure success. With our WGU Introduction to Cryptography HNO1 (Introduction-to-Cryptography) practice questions, you can get the most out of your studying and maximize your chances of passing your WGU Introduction to Cryptography HNO1 (Introduction-to-Cryptography) exam.

WGU Introduction to Cryptography HNO1 Sample Questions (Q37-Q42):

NEW QUESTION # 37
(Which authentication method allows a web service installed on a network operating system to prove its identity to a customer?)

- A. End-to-end authentication
- B. One-way client authentication
- C. One-way server authentication
- D. Mutual authentication

Answer: C

Explanation:
One-way server authentication is the standard model used by most TLS-enabled web services to prove the server's identity to a client. In this model, the server presents an X.509 certificate during the TLS handshake. The client validates the certificate chain to a trusted root CA, checks hostname binding (CN
/SAN), validates validity dates, and may check revocation status. If validation succeeds, the client gains cryptographic assurance that it is communicating with the holder of the private key corresponding to the server certificate's public key, and that the certificate is issued to the expected domain/identity. This proves the server's identity to the customer without requiring the customer to present a certificate.
Mutual authentication would require both client and server to authenticate each other using certificates (commonly in certain enterprise APIs), but the question asks specifically about the web service proving its identity to the customer, which is satisfied by server-only authentication. One-way client authentication is the opposite direction (client proves identity to server). "End-to-end authentication" is a broader concept and not the specific TLS identity proof mechanism described here. Thus, one-way server authentication is the correct choice.

NEW QUESTION # 38
(Which cipher uses shifting letters of the alphabet for encryption?)

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

Answer: C

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 # 39
(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 # 40
(Employee A needs to send Employee B a symmetric key for confidential communication. Which key is used to encrypt the symmetric key?)

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

Answer: B

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 # 41
(Which additional input element can be used to implement integrity in combination with symmetric ciphers?)

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

Answer: C

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.

NEW QUESTION # 42
.....

Our exam questions just need students to spend 20 to 30 hours practicing on the platform which provides simulation problems, can let them have the confidence to pass the Introduction-to-Cryptography exam, so little time great convenience for some workers. It must be your best tool to pass your exam and achieve your target. We provide free download and tryout before your purchase and if you fail in the exam we will refund you in full immediately at one time. Purchasing our Introduction-to-Cryptography Guide Torrent can help you pass the exam and it costs little time and energy.

Introduction-to-Cryptography Valid Exam Camp: https://www.pdf4test.com/Introduction-to-Cryptography-dump-torrent.html

100% Authentic Introduction-to-Cryptography Exam Braindumps, In this way, you can absolutely make an adequate preparation for this WGU Introduction-to-Cryptography exam, Nowadays, many candidates are competing for gaining the Introduction-to-Cryptography certificate, WGU Introduction-to-Cryptography Reliable Cram Materials The high quality of our vce braindumps are the guarantee of high passing score, You want to sign up for Introduction-to-Cryptography certification exam, but you are worried about failing the exam.

Confidence Intervals and Hypothesis Testing, You can choose the number of WGU Introduction-to-Cryptography Questions and topics, 100% Authentic Introduction-to-Cryptography Exam Braindumps, In this way, you can absolutely make an adequate preparation for this WGU Introduction-to-Cryptography exam.

PDF4Test: The Ideal Solution for WGU Introduction-to-Cryptography Exam Preparation

Nowadays, many candidates are competing for gaining the Introduction-to-Cryptography certificate, The high quality of our vce braindumps are the guarantee of high passing score, You want to sign up for Introduction-to-Cryptography certification exam, but you are worried about failing the exam.

- Updated Introduction-to-Cryptography Reliable Cram Materials Offer You The Best Valid Exam Camp | WGU WGU Introduction to Cryptography HNO1 ✌ Go to website ➡ www.vceengine.com □□□ open and search for ➠ Introduction-to-Cryptography □ to download for free □Reliable Introduction-to-Cryptography Test Sample
- How WGU is so Confident in its WGU Introduction-to-Cryptography Exam Questions? □ Download □ Introduction-to-Cryptography □ for free by simply searching on 《 www.pdfvce.com 》 □Test Introduction-to-Cryptography Tutorials
- Latest Introduction-to-Cryptography Dumps Pdf □ Introduction-to-Cryptography Online Tests □ Latest Introduction-to-Cryptography Dumps Pdf □ Search on { www.vce4dumps.com } for （ Introduction-to-Cryptography ） to obtain exam materials for free download □Valid Introduction-to-Cryptography Exam Pdf
- Introduction-to-Cryptography Exam Training □ Valid Test Introduction-to-Cryptography Tips □ Introduction-to-Cryptography Test Dump □ Open ➤ www.pdfvce.com □ enter [Introduction-to-Cryptography] and obtain a free download □Introduction-to-Cryptography Test Dump
- Introduction-to-Cryptography New Study Materials □ Reliable Introduction-to-Cryptography Real Exam □ Exam Introduction-to-Cryptography Prep □ Search for ▶ Introduction-to-Cryptography ◀ and easily obtain a free download on [www.exam4labs.com] □Introduction-to-Cryptography Online Tests
- Introduction-to-Cryptography Actual Questions □ Valid Introduction-to-Cryptography Test Discount □ Latest Introduction-to-Cryptography Exam Question □ Go to website ➡ www.pdfvce.com □□□ open and search for □ Introduction-to-Cryptography □ to download for free □Introduction-to-Cryptography Online Tests
- Latest Introduction-to-Cryptography Dumps Pdf □ Introduction-to-Cryptography Reliable Real Test □ Introduction-to-Cryptography Reliable Test Camp □ Easily obtain （ Introduction-to-Cryptography ） for free download through □ www.validtorrent.com □ □Introduction-to-Cryptography New Study Materials
- Valid Introduction-to-Cryptography Exam Pdf ↙ Introduction-to-Cryptography Online Tests □ Valid Introduction-to-Cryptography Test Discount □ □ www.pdfvce.com □ is best website to obtain □ Introduction-to-Cryptography □ for free download □Valid Test Introduction-to-Cryptography Tips
- 2026 Introduction-to-Cryptography – 100% Free Reliable Cram Materials | Authoritative Introduction-to-Cryptography Valid Exam Camp □ Easily obtain free download of ➡ Introduction-to-Cryptography □□□ by searching on □ www.troytecdumps.com □ □Introduction-to-Cryptography Actual Questions
- 100% Pass Quiz WGU - Introduction-to-Cryptography Useful Reliable Cram Materials □ Download □ Introduction-to-Cryptography □ for free by simply searching on ➥ www.pdfvce.com □ □Test Introduction-to-Cryptography Tutorials
- Introduction-to-Cryptography Reliable Dumps □ Introduction-to-Cryptography Test Dump □ Reliable Introduction-to-Cryptography Real Exam □ Easily obtain ☀ Introduction-to-Cryptography □☀□ for free download through ▹ www.pdfdumps.com ◃ □Latest Introduction-to-Cryptography Exam Question
- wanderlog.com, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, graphiskill.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, portfolium.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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes