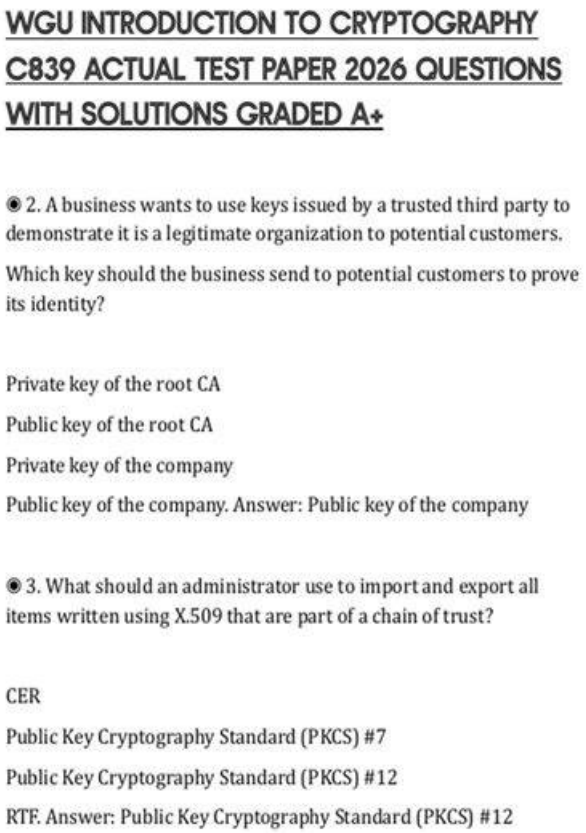
Actual WGU Introduction-to-Cryptography PDF Question For Quick Success



WGU INTRODUCTION TO CRYPTOGRAPHY
C839 ACTUAL TEST PAPER 2026 QUESTIONS
WITH SOLUTIONS GRADED A+

◉ 2. A business wants to use keys issued by a trusted third party to demonstrate it is a legitimate organization to potential customers.

Which key should the business send to potential customers to prove its identity?

Private key of the root CA

Public key of the root CA

Private key of the company

Public key of the company. Answer: Public key of the company

◉ 3. What should an administrator use to import and export all items written using X.509 that are part of a chain of trust?

CER

Public Key Cryptography Standard (PKCS) #7

Public Key Cryptography Standard (PKCS) #12

RTF. Answer: Public Key Cryptography Standard (PKCS) #12

DOWNLOAD the newest BootcampPDF Introduction-to-Cryptography PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1yMLBYZvYLqHqcYcQ9mvAwbUDlui6Smc7

Our website platform has no viruses and you can download Introduction-to-Cryptography test guide at ease. If you encounter difficulties in installation or use of Introduction-to-Cryptography exam torrent, we will provide you with remote assistance from a dedicated expert to help you and provide 365 days of free updates that you do not have to worry about what you missed. Whether you are a worker or student, you will save much time to do something whatever you want. It only needs 5-10 minutes after you pay for our Introduction-to-Cryptography learn torrent that you can learn it to prepare for your exam. Actually, if you can guarantee that your effective learning time with Introduction-to-Cryptography test preps are up to 20-30 hours, you can pass the exam.

WGU Introduction-to-Cryptography Exam Syllabus Topics:

Section	Objectives
Topic 1: Cryptography Fundamentals	- Symmetric vs Asymmetric Encryption - History and Evolution of Cryptography - Cryptographic Terminology
Topic 2: Hashing and Digital Signatures	- Message Authentication Codes (MAC) - Hash Functions (MD5, SHA-1, SHA-256) - Digital Signature Standards

Topic 3: Asymmetric Cryptography	- Diffie-Hellman Key Exchange - Elliptic Curve Cryptography (ECC) - Public Key Infrastructure (PKI) - RSA Algorithm
Topic 4: Applied Cryptography	- SSL/TLS Protocols - Cryptographic Best Practices - VPN Security - PGP and Email Encryption
Topic 5: Cryptanalysis and Attacks	- Brute Force and Dictionary Attacks - Common Attack Vectors - Social Engineering Prevention
Topic 6: Symmetric Cryptography	- Key Management - Stream Ciphers - Block Ciphers (AES, DES, 3DES) - Initialization Vectors (IV)

Exam WGU Introduction-to-Cryptography Cram Review | Reliable Introduction-to-Cryptography Test Cost

Our Introduction-to-Cryptography guide torrent provides 3 versions and they include PDF version, PC version, APP online version. Each version boosts their strength and using method. For example, the PC version of WGU Introduction to Cryptography HNO1 test torrent is suitable for the computers with the Window system. It can stimulate the real exam operation environment, stimulate the exam and undertake the time-limited exam. The download and installation has no limits for the amount of the computers and the users. The PDF version of Introduction-to-Cryptography study torrent is convenient to download and print our Introduction-to-Cryptography guide torrent and is suitable for browsing learning. If you use the PDF version you can print our WGU Introduction to Cryptography HNO1 test torrent on the papers and it is convenient for you to take notes. You can learn our Introduction-to-Cryptography study torrent at any time and place. You may choose the most convenient version to learn according to your practical situation.

WGU Introduction to Cryptography HNO1 Sample Questions (Q51-Q56):

NEW QUESTION # 51
(What does nonrepudiation aim to achieve in the context of cryptography?)

- A. Preventing unauthorized access to sensitive data
- B. Ensuring the confidentiality of encrypted messages
- C. Verifying the identity of the sender in secure communication
- D. Holding parties accountable for their actions and transactions

Answer: D

Explanation:
Nonrepudiation aims to prevent a party from later denying having performed an action, such as sending a message, approving a transaction, or signing a document. In cryptographic systems, nonrepudiation is typically supported by digital signatures, audit logs, and trusted time-stamping: if a message is signed with a private key and verified with the corresponding public key (often bound to an identity via a certificate), the signer can be held accountable for that signed content. This creates evidence that can be used for dispute resolution, compliance, and legal or contractual enforcement. Nonrepudiation is distinct from confidentiality (keeping data secret) and from access control (preventing unauthorized use). While authentication (verifying identity) is related and often a prerequisite, the defining goal is accountability-ensuring that actions can be attributed to entities in a way that is difficult to dispute later. Effective nonrepudiation also depends on secure private key management, certificate validation, and procedures that show the key was under the signer's control at the time. Therefore, the correct answer is holding parties accountable for their actions and transactions.

NEW QUESTION # 52
(Which cryptographic technique is used to ensure data integrity?)

- A. Authentication
- B. Steganography
- C. Non-repudiation
- D. Digital signatures

Answer: D

Explanation:
Data integrity means ensuring that information has not been modified without authorization. Digital signatures are a core cryptographic technique that provides integrity by binding a message (typically its hash) to the signer's private key. The signer creates a signature over the message digest; the verifier checks it with the signer's public key and recomputes the digest. Any change to the message alters the digest and causes verification to fail, revealing tampering. Digital signatures also support authenticity (verifying the signer) and can contribute to nonrepudiation under proper key-management and policy controls, but integrity is a primary guarantee they deliver. "Authentication" is broader and can be achieved by other means, but it is not as directly tied to integrity as signatures in this option set. "Non-repudiation" is an outcome/goal rather than a standalone integrity technique. "Steganography" hides the existence of data and does not inherently protect integrity. Therefore, among these options, digital signatures are the best cryptographic technique for ensuring data integrity.

NEW QUESTION # 53
(What is a component of a one-time password (OTP) that is needed to guess future iterations of passwords?)

- A. Encryption algorithm
- B. Initialization vector
- C. Seed
- D. Function

Answer: C

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.

NEW QUESTION # 54
(Which encryption mode is known for supporting parallel processing?)

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

Answer: A

Explanation:
ECB (Electronic Codebook) mode encrypts each block independently with the same key, which makes it naturally amenable to parallel processing: multiple blocks can be encrypted or decrypted simultaneously because there is no chaining dependency between blocks. This is in contrast to CBC encryption, where each plaintext block is XORed with the previous ciphertext block, creating a dependency that prevents straightforward parallelization of encryption (though CBC decryption can be parallelized because ciphertext blocks are already known). Feedback modes like CFB and OFB generate keystream material sequentially, where each step depends on the previous state, limiting parallelism. While ECB's parallelism is an implementation advantage, it is widely discouraged for most real data because it leaks patterns-identical plaintext blocks produce identical ciphertext blocks. Modern systems prefer parallel-friendly and secure modes such as CTR or GCM, but among the listed options, the mode most known for parallel processing is ECB due to block independence. Therefore, the correct answer is Electronic Codebook (ECB).

NEW QUESTION # 55
(What is the length (in bits) of a SHA-1 hash output?)

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

Answer: C

Explanation:
SHA-1 (Secure Hash Algorithm 1) produces a fixed-size output of 160 bits (20 bytes). Hash output size matters in cryptography because it influences collision resistance and the effort required for various attacks. For an ideal n-bit hash, finding a collision by generic means is expected around 2