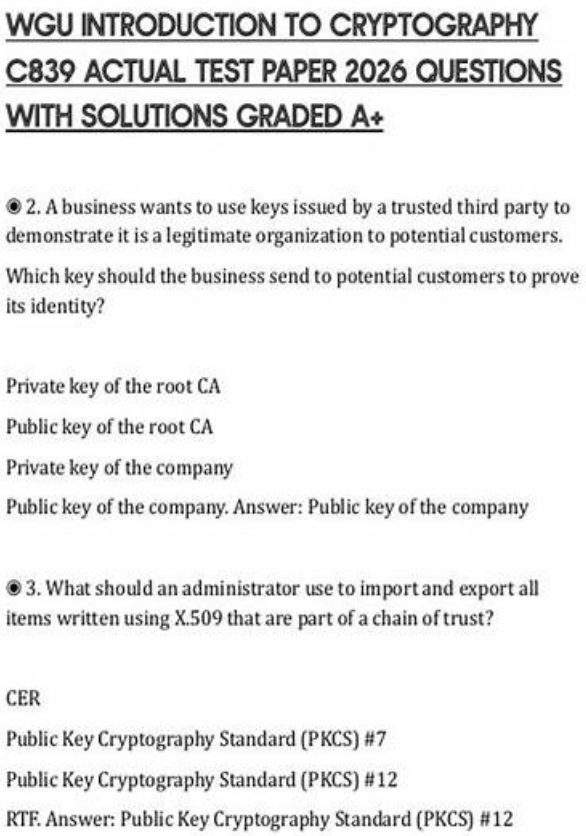
Test WGU Introduction-to-Cryptography Duration - Introduction-to-Cryptography Reliable Exam Blueprint



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

2026 Latest ActualVCE Introduction-to-Cryptography PDF Dumps and Introduction-to-Cryptography Exam Engine Free Share: https://drive.google.com/open?id=1qKUUpKjLlYuKdkbaKGThF-t7gubretzk

In order to serve you better, we have do what we can do for you. Before buying Introduction-to-Cryptography exam torrent, we offer you free demo for you to have a try, so that you can have a deeper understanding of what you are going to buy. If you want the Introduction-to-Cryptography exam materials after trying, you just need to add them to cart and pay for them, then you can get downloading link and password within ten minutes, if you don't receive the Introduction-to-Cryptography Exam Torrent, just contact us, and we will solve the problem for you. We have after-service stuff, and you can ask any questions about Introduction-to-Cryptography exam dumps after buying.

WGU Introduction-to-Cryptography Exam Syllabus Topics:

Section	Weight	Objectives
Topic 1: Key Management & Secure Protocols	10%	- Cryptographic attacks: brute force, birthday, man-in-the-middle - Secure protocols: TLS/SSL, IPsec, SSH, PGP - Key generation, storage, exchange, and destruction

Topic 2: Asymmetric Encryption & Public Key Infrastructure	25%	- Digital signatures: purpose and process - PKI components: certificates, CAs, trust models - Principles: public/private key pairs - Certificate lifecycle: creation, validation, revocation - Algorithms: RSA, ECC, Diffie-Hellman
Topic 3: Cryptography Fundamentals	20%	- Basic terminology: plaintext, ciphertext, algorithm, key - Core goals: confidentiality, integrity, authentication, non-repudiation - Historical evolution and modern applications
Topic 4: Symmetric Encryption	25%	- Key generation, distribution, and management challenges - Block vs stream ciphers, modes of operation (ECB, CBC, OFB, CFB) - Principles and operation - Algorithms: AES, DES, 3DES, Blowfish
Topic 5: Implementation & Best Practices	5%	- Standards and compliance - Common mistakes and vulnerabilities - Selecting appropriate algorithms and key sizes
Topic 6: Hash Functions & Data Integrity	15%	- HMAC construction and application - Properties: collision resistance, one-way function - Algorithms: SHA-1, SHA-256, SHA-3, MD5 - Uses: integrity checks, password storage, message authentication

Introduction-to-Cryptography exam dumps and WGU Introduction-to-Cryptography exam Simulator

Candidates all around the globe use their full potential only to get WGU Introduction-to-Cryptography certification. Once the candidate is a WGU certified, he gets multiple good career opportunities in the WGU sector. To pass the Introduction-to-Cryptography Certification Exam a candidate needs to be updated and reliable WGU Introduction to Cryptography HNO1 (Introduction-to-Cryptography) prep material.

WGU Introduction to Cryptography HNO1 Sample Questions (Q26-Q31):

NEW QUESTION # 26
(What is an alternative to using a Certificate Revocation List (CRL) with certificates?)

- A. Privacy Enhanced Mail (PEM)
- B. Online Certificate Status Protocol (OCSP)
- C. Policy Certificate Authority (CA)
- D. Root 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 # 27

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

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

Answer: A

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 # 28
(Which encryption algorithm encrypts with one key, decrypts with another key, and then encrypts with the first key?)

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

Answer: A

Explanation:
3DES (Triple DES) commonly uses an Encrypt-Decrypt-Encrypt (EDE) sequence. In the two-key form, it encrypts with key K1, decrypts with key K2, then encrypts again with K1. In the three-key form, it encrypts with K1, decrypts with K2, then encrypts with K3. The EDE construction was chosen partly for backward compatibility: if K1=K2=K3, the scheme reduces to single DES, allowing older systems to interoperate in constrained ways. AES and IDEA do not use an EDE triple-stage process as their defining structure; they are single-pass block ciphers with internal rounds. DES is a single-pass algorithm (one key) rather than a triple application with multiple keys. Therefore, the algorithm described-encrypt with one key, decrypt with another, encrypt with the first-is 3DES. Although now considered legacy, it remains a classic example of increasing effective security by applying a block cipher multiple times with independent keys.

NEW QUESTION # 29
(Which type of exploit involves looking for different inputs that generate the same hash?)

- A. Differential cryptanalysis
- B. Birthday attack
- C. Linear cryptanalysis
- D. Algebraic attack

Answer: B

Explanation:
A birthday attack targets hash functions by exploiting the birthday paradox: collisions (two different inputs producing the same hash output) can be found much faster than brute-forcing a specific preimage. For an n-bit hash, the expected work to findanycollision is on the order of 2

What's more, part of that ActualVCE Introduction-to-Cryptography dumps now are free: https://drive.google.com/open?id=1qKUUpKjLlYuKdkbaKGThF-t7gubretzk