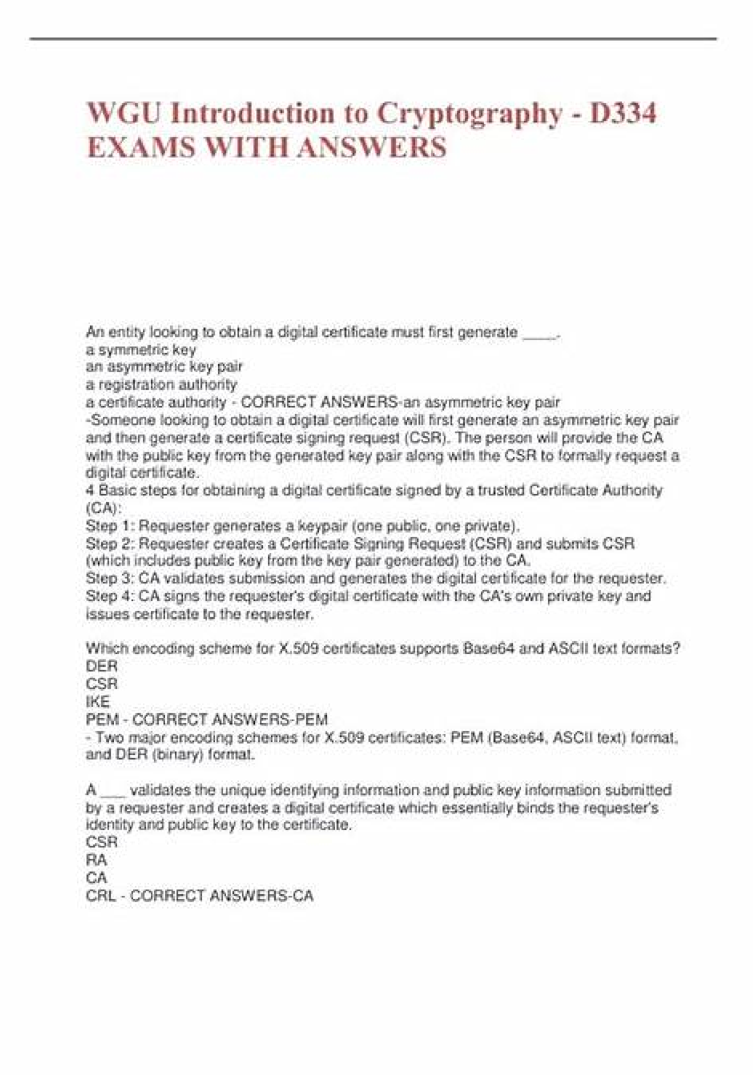
Here's the Easiest and Quick Way to Pass WGU Introduction-to-Cryptography Exam



WGU Introduction to Cryptography - D334
EXAMS WITH ANSWERS

An entity looking to obtain a digital certificate must first generate ____.
a symmetric key
an asymmetric key pair
a registration authority
a certificate authority - CORRECT ANSWERS-an asymmetric key pair
-Someone looking to obtain a digital certificate will first generate an asymmetric key pair and then generate a certificate signing request (CSR). The person will provide the CA with the public key from the generated key pair along with the CSR to formally request a digital certificate.
4 Basic steps for obtaining a digital certificate signed by a trusted Certificate Authority (CA):
Step 1: Requester generates a keypair (one public, one private).
Step 2: Requester creates a Certificate Signing Request (CSR) and submits CSR (which includes public key from the key pair generated) to the CA.
Step 3: CA validates submission and generates the digital certificate for the requester.
Step 4: CA signs the requester's digital certificate with the CA's own private key and issues certificate to the requester.

Which encoding scheme for X.509 certificates supports Base64 and ASCII text formats?
DER
CSR
IKE
PEM - CORRECT ANSWERS-PEM
- Two major encoding schemes for X.509 certificates: PEM (Base64, ASCII text) format, and DER (binary) format.

A ___ validates the unique identifying information and public key information submitted by a requester and creates a digital certificate which essentially binds the requester's identity and public key to the certificate.
CSR
RA
CA
CRL - CORRECT ANSWERS-CA

ITexamReview provides WGU Introduction-to-Cryptography desktop-based practice software for you to test your knowledge and abilities. The Introduction-to-Cryptography desktop-based practice software has an easy-to-use interface. You will become accustomed to and familiar with the free demo for WGU Introduction-to-Cryptography Exam Questions. Exam self-evaluation techniques in our Introduction-to-Cryptography desktop-based software include randomized questions and timed tests. These tools assist you in assessing your ability and identifying areas for improvement to pass the WGU certification exam.

Just install the WGU Introduction to Cryptography HNO1 (Introduction-to-Cryptography) PDF dumps file on your desktop computer, laptop, tab, or even on your smartphone and start WGU Introduction to Cryptography HNO1 (Introduction-to-Cryptography) exam preparation anytime and anywhere. Whereas the other two WGU Introduction to Cryptography HNO1 (Introduction-to-Cryptography) exam questions formats are concerned both are the easy-to-use and compatible Mock Introduction-to-Cryptography Exam that will give you a real-time environment for quick WGU Exams preparation. Now choose the right WGU Introduction-to-Cryptography exam questions format and start this career advancement journey.

>> Latest Test Introduction-to-Cryptography Discount <<

Training Introduction-to-Cryptography Material & Introduction-to-Cryptography Authentic Exam Hub

The Introduction-to-Cryptography desktop-based practice exam is compatible with Windows-based computers and only requires an internet connection for the first-time license validation. The web-based Introduction-to-Cryptography practice test is accessible on any browser without needing to install any separate software. Finally, the Introduction-to-Cryptography Dumps PDF is easily portable and can be used on smart devices or printed out. We constantly update the Introduction-to-Cryptography pdf file to ensure customers receive the latest version of WGU Introduction-to-Cryptography questions, based on the actual WGU Introduction to Cryptography HNO1 (Introduction-to-Cryptography) exam content.

WGU Introduction to Cryptography HNO1 Sample Questions (Q58-Q63):

NEW QUESTION # 58
(How does adding salt to a password improve security?)

- A. Salt prevents users from reusing the same password.
- B. Salt creates a different hash if two people use the same password.
- C. Salt ensures two people do not have the same password.
- D. Salt enforces the complexity rules for passwords.

Answer: B

Explanation:
A salt is a unique, random value stored alongside a password hash and combined with the password during hashing. Its main security benefit is that it ensures identical passwords do not produce identical hashes across different accounts or systems. If two users choose the same password, their stored hashes will differ because their salts differ, which directly prevents attackers from spotting shared passwords by comparing hashes. Salts also defeat precomputation attacks such as rainbow tables, because an attacker would need to regenerate tables for each possible salt value-a task that becomes infeasible when salts are large and unique per password. Salt does not enforce password complexity rules (that's a policy/validation function), does not guarantee users choose different passwords, and does not prevent password reuse across sites. The correct statement is that salt makes the resulting hash different even for the same password, improving resistance to offline cracking at scale and eliminating the "same hash = same password" shortcut attackers rely on.

NEW QUESTION # 59
(How often are transactions added to a blockchain?)

- A. Approximately every 1 hour
- B. Approximately every 30 minutes
- C. Approximately every 10 minutes
- D. Approximately every 24 hours

Answer: C

Explanation:
For Bitcoin, transactions are confirmed by inclusion in blocks, and the network targets an average block interval of about 10 minutes. That means transactions are "added" to the Bitcoin blockchain approximately every 10 minutes in the sense that a new block containing a batch of transactions is appended at that cadence. The 10-minute target is achieved by a difficulty adjustment mechanism that recalibrates mining difficulty roughly every 2016 blocks, aiming to keep the average interval stable despite changes in total network hash power. It is important to note that this is an average: blocks can be found faster or slower in the short term due to the probabilistic nature of proof-of-work mining.
Other blockchains have different block times (seconds to minutes), but the question's options and typical curriculum context align with Bitcoin's 10-minute design. Therefore, the correct choice is approximately every 10 minutes.

NEW QUESTION # 60
(Which type of exploit involves looking for different inputs that generate the same hash?)

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

Answer: A

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