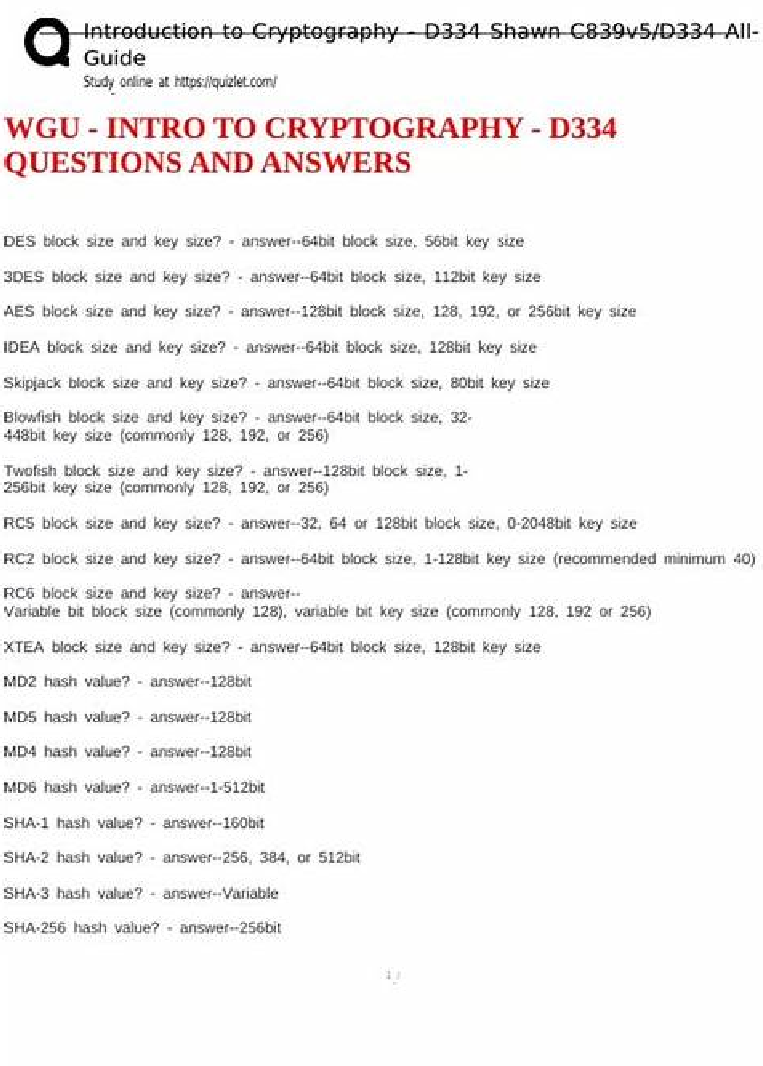
Free PDF 2026 WGU Reliable Introduction-to-Cryptography: WGU Introduction to Cryptography HNO1 Best Vce



~~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

PracticeDump has one of the most comprehensive and top-notch WGU Introduction-to-Cryptography Exam Questions. We eliminated the filler and simplified the WGU Introduction to Cryptography HNO1 exam preparation process so you can ace the WGU certification exam on your first try. Our WGU Introduction-to-Cryptography Questions include real-world examples to help you learn the fundamentals of the subject not only for the WGU exam but also for your future job.

Passing the Introduction-to-Cryptography exam rests squarely on the knowledge of exam questions and exam skills. Our Introduction-to-Cryptography training quiz has bountiful content that can fulfill your aims at the same time. We know high efficient Introduction-to-Cryptography practice materials play crucial roles in your review. Our experts also collect with the newest contents of Introduction-to-Cryptography Study Guide and have been researching where the exam trend is heading and what it really want to examine you.

>> Introduction-to-Cryptography Best Vce <<

2026 Useful Introduction-to-Cryptography – 100% Free Best Vce | WGU Introduction to Cryptography HNO1 Discount Code

Free update for 365 days for Introduction-to-Cryptography study guide materials is available. That is to say, in the following year,

WGU Introduction to Cryptography HNO1 Sample Questions (Q34-Q39):

NEW QUESTION # 34
(How often are transactions added to a blockchain?)

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

Answer: B

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 # 35
(What describes a true random number generator?)

- A. Unique integer determined through factorization of integers
- B. Slow and nondeterministic, and the same input produces different results
- C. Integer increased by one to match requests and responses
- D. Fast and deterministic, and the same input produces the same results

Answer: B

Explanation:
A true random number generator (TRNG) draws randomness from physical phenomena that are inherently unpredictable and not algorithmically reproducible. Because of this, it is nondeterministic:
you cannot feed it the same "input" and expect the same output stream. TRNGs are often slower than PRNGs because they depend on collecting entropy from hardware sources and may require conditioning to remove bias. This aligns with option B: slow and nondeterministic, producing different results even under similar or repeated conditions. Option A describes a deterministic PRNG, where identical seeds yield identical sequences. Option C is unrelated; factorization is a hard math problem used in cryptography (e.g., RSA security assumptions), not a randomness generator definition. Option D describes a counter, which is deterministic and not random. In secure systems, TRNG output may seed a cryptographically secure PRNG to provide both unpredictability and high throughput; but the defining characteristic of a TRNG is nondeterminism from physical entropy. Therefore, option B is correct.

NEW QUESTION # 36
(How does Electronic Codebook (ECB) mode encryption function?)

- A. Encrypts each block with the same key, where each block is independent of the others
- B. Converts from block to stream, then uses a counter value and a nonce to encrypt the data
- C. Uses an IV to encrypt the first block, then uses the result to encrypt the next block
- D. Uses a self-synchronizing stream on the blocks, where the IV is encrypted and XORed with the data stream

Answer: A

Explanation:

ECB is the simplest block cipher mode: each plaintext block is encrypted independently using the same key and the block cipher primitive. There is no IV and no chaining, so identical plaintext blocks produce identical ciphertext blocks. This property leaks patterns and structure in the plaintext, which is why ECB is generally considered insecure for most real-world data beyond tiny, random-looking inputs. For example, images encrypted with ECB often reveal outlines because repeated pixel blocks map to repeated ciphertext blocks. Option A describes CTR mode, option C describes CBC mode, and option B resembles feedback-based modes. ECB's independence also means it can be parallelized, but the pattern leakage is a severe weakness. Modern practice prefers authenticated encryption modes (like GCM) or, at minimum, modes with IVs and chaining (like CBC with proper padding and MAC).
Therefore, the correct statement is that ECB encrypts each block with the same key and each block is independent of the others.

NEW QUESTION # 37
(Which attack may take the longest amount of time to achieve success?)

- A. Birthday
- B. Brute-force
- C. Dictionary
- D. Rainbow table

Answer: B

Explanation:
A brute-force attack exhaustively tries every possible key or password candidate until the correct one is found. Because it explores the full search space (or a very large portion of it), brute force is often the slowest method, especially when strong keys, long passwords, rate limits, and slow password hashing (bcrypt/Argon2) are used. By contrast, a dictionary attack reduces work by trying only common or likely passwords, often succeeding quickly against weak human-chosen secrets. Rainbow table attacks shift work into precomputation; once a table exists, lookup can be faster than brute-force-though salt and modern hashing defeat them. Birthday attacks are about finding collisions, not necessarily recovering a specific secret, and their expected work is about 2