WGU.Introduction-to-Cryptography.v2026-08-28.q53

Exam Code:	Introduction-to-Cryptography
Exam Name:	WGU Introduction to Cryptography HNO1
Certification Provider:	WGU
Free Question Number:	53
Version:	v2026-08-28
# of views:	126
# of Questions views:	530
https://www.exam-tests.com/Introduction-to-Cryptography-exam/WGU.Introduction-to-Cryptography.v2026-08-28.q53.html	

NEW QUESTION: 1
(How are limits managed for the number of bitcoins that can be created and stored in a blockchain?)
A. Rewards for mining reduce over time
B. The total number of participants has been set
C. A maximum has been established per country
D. Each person has a maximum number
Answer: (SHOW ANSWER)
Bitcoin's supply is controlled by protocol rules enforced by consensus: new bitcoins enter circulation through the block subsidy awarded to miners for producing valid blocks. This subsidy is programmed to halve at fixed intervals (every 210,000 blocks), which steadily reduces the rate of new coin creation over time and asymptotically approaches a capped total supply (commonly cited as 21 million BTC). This mechanism is often called the halving schedule and is the primary way limits are managed. The number of participants is not fixed; anyone can run a node or mine. There is no per-country cap and no per-person maximum enforced by the protocol-addresses and ownership are not limited that way. The supply cap emerges from the decreasing issuance schedule combined with consensus validation rules that reject blocks creating coins beyond what the schedule allows. Therefore, the correct answer is that limits are managed because rewards for mining reduce over time.

NEW QUESTION: 2
(What makes the RC4 cipher unique compared to RC5 and RC6?)
A. Stream
B. Asymmetric
C. Symmetric

D. Block

Answer: A (LEAVE A REPLY)

RC4 is unique among the RC family listed because it is a stream cipher. It generates a pseudorandom keystream and encrypts data by XORing that keystream with plaintext bytes (and decryption is the same XOR operation). This differs from RC5 and RC6, which are block ciphers: they encrypt fixed-size blocks of data through multiple rounds of operations (such as modular addition, XOR, and rotations) using a secret key. The stream-cipher design means RC4 historically fit protocols where data arrives continuously (e.g., early wireless and web encryption) and where simple, fast software implementation was desired. However, stream ciphers demand careful handling of nonces/IVs to avoid keystream reuse; reuse can catastrophically leak plaintext relationships. RC4 also has well-documented statistical biases in its keystream, leading to practical attacks in protocols like WEP and later concerns in TLS, which is why RC4 has been deprecated in modern security standards. Still, from a classification standpoint, "stream" is the distinguishing characteristic versus RC5/RC6 being block ciphers.

NEW QUESTION: 3

(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. Root Certificate Authority (CA)

D. Policy Certificate Authority (CA)

Answer: B (LEAVE A REPLY)

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: 4

(How are limits managed for the number of bitcoins that can be created and stored in a blockchain?)

A. Rewards for mining reduce over time

B. The total number of participants has been set
C. A maximum has been established per country
D. Each person has a maximum number
Answer: A (LEAVE A REPLY)
Bitcoin's supply is controlled by protocol rules enforced by consensus: new bitcoins enter circulation through the block subsidy awarded to miners for producing valid blocks. This subsidy is programmed to halve at fixed intervals (every 210,000 blocks), which steadily reduces the rate of new coin creation over time and asymptotically approaches a capped total supply (commonly cited as 21 million BTC).
This mechanism is often called the halving schedule and is the primary way limits are managed. The number of participants is not fixed; anyone can run a node or mine. There is no per-country cap and no per-person maximum enforced by the protocol-addresses and ownership are not limited that way. The supply cap emerges from the decreasing issuance schedule combined with consensus validation rules that reject blocks creating coins beyond what the schedule allows. Therefore, the correct answer is that limits are managed because rewards for mining reduce over time.

NEW QUESTION: 5
(A Linux user password is identified as follows:
$2a$08$AbCh0RCM8p8FGaYvRLI0H.Kng54gcnWCOQYIhas708UEZRQQjGBh4
Which hash algorithm should be used to salt this password?)
A. NTLM
B. SHA-512
C. MD5
D. bcrypt
Answer: (SHOW ANSWER)
The string format $2a$08$... is a well-known identifier for the bcrypt password hashing scheme. In common password-hash notation, the prefix indicates the algorithm and parameters: "$2a$" denotes bcrypt (version
2a), and "08" indicates the cost factor (work factor) controlling how computationally expensive hashing is.
bcrypt is designed specifically for password storage: it includes a built-in salt and is intentionally slow and adaptive, making brute-force and GPU attacks far more expensive than fast general-purpose hashes like MD5 or SHA-512. NTLM and MD5 are obsolete for secure password storage due to speed and known weaknesses.
SHA-512, while cryptographically strong as a hash, is still too fast for password hashing unless used in a dedicated password-hashing construction (e.g., PBKDF2, scrypt, Argon2) with appropriate parameters and salts. Since the given hash clearly matches bcrypt's encoding, the correct algorithm is bcrypt, which incorporates salting and cost-based key stretching as part of its design.

NEW QUESTION: 6
(What is an example of a block cipher mode of operation?)
A. Secure Hash Algorithm 256 (SHA-256)
B. Digital Signature Algorithm (DSA)
C. Rivest-Shamir-Adleman (RSA)
D. Electronic Codebook (ECB)
Answer: D (LEAVE A REPLY)
A block cipher mode of operation defines how a block cipher (such as AES) is applied to data longer than a single block, and how blocks are linked (or not linked) to provide certain security properties. ECB (Electronic Codebook) is one of the canonical block cipher modes: it encrypts each plaintext block independently using the same key. While ECB is generally discouraged because it leaks patterns (identical plaintext blocks produce identical ciphertext blocks), it is still a valid and historically important mode of operation and is often used as a teaching example of what not to do for structured data. In contrast, SHA-256 is a hash function (one- way digest) and not a mode for block ciphers. DSA is a digital signature algorithm and provides authenticity
/integrity, not encryption mode behavior. RSA is an asymmetric cryptosystem, not a block cipher mode.
Therefore, among the options, ECB is the correct example of a block cipher mode of operation.

NEW QUESTION: 7
(What does nonrepudiation aim to achieve in the context of cryptography?)
A. Verifying the identity of the sender in secure communication
B. Holding parties accountable for their actions and transactions
C. Ensuring the confidentiality of encrypted messages
D. Preventing unauthorized access to sensitive data
Answer: B (LEAVE A REPLY)
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: 8
(What is an attribute of RC4 when used with WEP?)
A. 40-bit key
B. 128-bit key
C. 256-bit key
D. 512-bit key
Answer: A (LEAVE A REPLY)
In classic WEP deployments, RC4 was used with what is commonly called "40-bit WEP" (also labeled
"64-bit WEP" because it combines a 40-bit secret key with a 24-bit IV to form a 64-bit RC4 seed). The key attribute emphasized in many foundational descriptions of WEP is this 40-bit shared secret length, which was originally chosen due to export restrictions and legacy constraints. Although "104-bit WEP" (sometimes called "128-bit WEP," again counting the 24-bit IV) also existed, the option set here points to the historically standard and widely referenced attribute: a 40-bit key when RC4 is used in WEP.
Importantly, WEP's security failure is not only about key size; the 24-bit IV is too small and repeats frequently, and WEP's key scheduling vulnerabilities combined with IV reuse allow attackers to recover the secret key with enough captured frames. Still, among the given options, the correct attribute is the 40-bit key.

NEW QUESTION: 9
(Which of the following best describes lightweight cryptography?)
A. Cryptography that focuses solely on increasing encryption strength
B. Cryptographic methods that are only applicable in military settings
C. A method of encryption that is outdated and rarely used
D. Cryptographic algorithms designed for resource-constrained environments
Answer: (SHOW ANSWER)
Lightweight cryptography refers to cryptographic primitives and profiles engineered for environments where computational resources are constrained-limited CPU, memory, power, bandwidth, and code size-while still requiring robust security. Typical targets include IoT sensors, embedded controllers, smart cards, RFID, wearables, and many mobile or edge deployments. The design goals emphasize efficiency (low energy consumption, small silicon area for hardware, small firmware footprint) and practical performance under constraints, often while providing modern security properties like authenticated encryption (confidentiality + integrity) and secure hashing. Lightweight cryptography is not simply "stronger encryption"; it balances security with implementability in constrained systems. It is also not restricted to military settings and is not inherently outdated-many lightweight designs are modern and motivated by the rapid growth of IoT

and pervasive computing. Because constrained devices are common entry points for attackers, having secure primitives that fit those devices is a critical part of contemporary security architecture. Therefore, the best description is cryptographic algorithms designed for resource-constrained environments.

NEW QUESTION: 10
(What is a focus of the ISO/IEC 27001 standard?)
A. Development of new encryption algorithms
B. Risk management and continuous improvement of information security
C. Enforcement of criminal penalties for data breaches
D. Exclusively addressing network security
Answer: B (LEAVE A REPLY)
ISO/IEC 27001 is an international standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). Its focus is not inventing cryptographic algorithms, but managing information security through a structured governance approach: identifying assets, assessing risks, selecting and implementing controls, measuring effectiveness, and continuously improving.
The standard emphasizes a risk-based methodology-controls are chosen based on organizational context and threat landscape, and the ISMS is refined over time through audits, management reviews, and corrective actions. While cryptography can be part of the control set (e.g., encryption policies, key management, secure communications), ISO/IEC 27001 addresses a broad range of security domains beyond crypto, including physical security, access control, incident management, supplier relationships, and business continuity. It also does not enforce criminal penalties; it is a certification/management standard. And it is not limited to network security. Therefore, the correct focus is risk management and continuous improvement of information security.

NEW QUESTION: 11
(How does adding salt to a password improve security?)
A. Salt creates a different hash if two people use the same password.
B. Salt enforces the complexity rules for passwords.
C. Salt ensures two people do not have the same password.
D. Salt prevents users from reusing the same password.
Answer: A (LEAVE A REPLY)
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: 12
(Which cipher uses shifting letters of the alphabet for encryption?)
A. SHA-1
B. Vigenere
C. Bifid
D. Caesar
Answer: (SHOW ANSWER)
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: 13
(How can auditing enhance an organization ' s cryptographic practices?)
A. It identifies weaknesses in current practices.
B. It guarantees that no security incidents will occur.
C. It eliminates the need for regular policy updates.
D. It ensures all employees are trained in cryptography.
Answer: (SHOW ANSWER)
Auditing improves cryptographic practice by systematically evaluating whether cryptographic controls are correctly selected, implemented, configured, and maintained. Through audits, an organization can discover weak algorithms (e.g., deprecated hashes), improper key lengths, unsafe modes (e.g., unauthenticated CBC), missing integrity controls, poor certificate validation, and operational problems such as key reuse, weak randomness sources, inadequate rotation, or overly permissive access to key material. Audits also assess compliance with internal policy and external standards, ensuring crypto is used consistently across systems and that exceptions are documented and risk-

managed. Importantly, auditing does not guarantee that incidents will never happen; it reduces risk by finding gaps before attackers do. It also does not eliminate the need for updates-audits often reveal that policies must evolve as threats and best practices change. Employee training can be recommended as an outcome of auditing, but audits do not automatically ensure training. Thus, the most accurate benefit is that auditing identifies weaknesses and drives corrective action, strengthening cryptographic posture over time.

NEW QUESTION: 14
(Which wireless security standard uses an authentication server with 802.1X and EAP?)
A. WPA-PSK
B. WEP
C. WPA-Enterprise
D. TKIP
Answer: C (LEAVE A REPLY)
802.1X is a port-based network access control framework that enables centralized authentication using an authentication server (commonly RADIUS). EAP (Extensible Authentication Protocol) runs within
802.1X to support many credential types (password-based methods like PEAP, certificate-based methods like EAP-TLS, and others). WPA-Enterprise is the wireless security mode that explicitly uses
802.1X + EAP with an authentication server to perform per-user/per-device authentication and to derive dynamic session keys. By contrast, WPA-PSK uses a pre-shared key without an external authentication server; all users share the same PSK, which is weaker for enterprise identity management. WEP is an older mechanism using static keys and does not provide modern 802.1X/EAP enterprise authentication in the WPA-Enterprise sense. TKIP is an encryption/integrity protocol used under WPA, not the full authentication "standard" involving an authentication server. Therefore, the correct choice is WPA-Enterprise.

NEW QUESTION: 15
(An administrator has configured a Virtual Private Network (VPN) connection utilizing IPsec transport mode with Encapsulating Security Payload (ESP) between a server in the corporate office and a client computer in the remote office. In which situation can the packet content be inspected?)
A. On devices at headquarters and offsite before being sent and after being received
B. In the headquarters' and offsite location's networks after the data has been sent
C. Only in the offsite location's network while data is in transit
D. Only in the headquarters' network while data is in transit
Answer: A (LEAVE A REPLY)
With IPsec ESP in transport mode, the payload of the original IP packet (typically the transport-layer segment and higher) is encrypted and integrity-protected between the two

endpoints-here, the corporate server and the remote client. Because encryption is applied by the sending endpoint and removed only by the receiving endpoint, intermediate routers, switches, and monitoring devices in either network cannot view the protected payload while it is in transit. They may see outer IP headers and certain metadata needed for routing, but not the encrypted content protected by ESP. As a result, the packet's contents are inspectable only at the endpoints: before encryption on the sender (plaintext exists in memory/stack before IPsec processing) and after decryption on the receiver (plaintext is restored for the application). This is true whether the traffic traverses internal networks or the Internet; the cryptographic boundary is between the endpoints participating in the IPsec SA. Therefore, inspection of the actual content is possible only on the devices at headquarters and offsite, before sending and after receiving, not by in-transit networks.

NEW QUESTION: 16
(Why should a forensic investigator create a hash of a victim's hard drive and of the bitstream copy of the hard drive?)
A. To identify if someone opened the drive
B. To certify the information on the drive is correct
C. To establish who created the files on the drives
D. To verify that the drives are identical
Answer: D (LEAVE A REPLY)
In digital forensics, investigators must preserve evidence integrity and demonstrate an unbroken chain of custody. Creating a cryptographic hash (such as SHA-256) of the original drive and then hashing the forensic bitstream image provides a strong mathematical assurance that the copy is an exact, bit-for-bit replica. Because secure hash functions are designed so that any tiny change in data produces a dramatically different digest, matching hashes indicate the image contains identical data to the source at the time of acquisition. This is critical in legal and investigative contexts: analysis is performed on the copy, not the original, to avoid altering evidence. If the hashes match, the investigator can testify that the evidence examined is identical to what was collected, supporting admissibility and credibility.
Hashing does not prove who created files, nor does it directly show whether someone "opened the drive"; it specifically validates the integrity and equivalence of the captured image. Therefore, hashing both artifacts is done to verify that the original and the bitstream copy are identical.

NEW QUESTION: 17
(A company wants to use certificates issued by a root CA to demonstrate to customers that it is a legitimate company being hosted by a cloud provider. Who needs to trust the root CA public key?)
A. The cloud provider and the seller
B. The buyer and the Federal Trade Commission
C. The seller and the buyer
D. The Federal Trade Commission and the cloud provider
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18
(Which type of exploit involves looking for different inputs that generate the same hash?)
A. Birthday attack
B. Linear cryptanalysis
C. Algebraic attack
D. Differential cryptanalysis
Answer: A (LEAVE A REPLY)
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^(n/2), not 2^n.
The attack is relevant because many security constructions rely on collision resistance-digital signatures, certificate fingerprints, integrity checks, and some commitment schemes. If an attacker can generate two different documents with the same hash, they may trick a signer into signing one version while later presenting the other as "signed," depending on the protocol. Linear cryptanalysis and differential cryptanalysis are primarily techniques against block ciphers, analyzing relationships between plaintext/ciphertext differences or linear approximations across rounds. Algebraic attacks treat the cipher as a system of equations. The description "looking for different inputs that generate the same hash" is the hallmark of collision-finding, and the classic framing for that is the birthday attack.

NEW QUESTION: 19
(Which mechanism implemented in WPA-Enterprise guards against bit-flipping exploits?)
A. Advanced Encryption Standard (AES)
B. Pre-shared key (PSK)
C. Message Integrity Check (MIC)

D. Global encryption key

Answer: C (LEAVE A REPLY)

Bit-flipping exploits target encryption modes or protocols that do not provide strong integrity, allowing attackers to modify ciphertext so that predictable changes occur in plaintext after decryption. To defend against this, protocols add an integrity mechanism that detects tampering. In WPA (including enterprise deployments), TKIP introduced a Message Integrity Check (MIC) called "Michael." The MIC is computed over the frame contents (with additional fields) and verified by the receiver; if an attacker flips bits in transit, the MIC verification fails, and the frame is rejected. While AES (used by WPA2's CCMP) also provides integrity via authenticated encryption, the option presented that directly names the tamper-detection mechanism associated with guarding against bit-flipping is MIC. A pre- shared key is an authentication/keying method (and not enterprise-mode anyway), and a "global encryption key" would be the opposite of what you want-global/static keys worsen security.

Therefore, the intended mechanism that mitigates bit-flipping by detecting unauthorized modifications is the Message Integrity Check.

NEW QUESTION: 20

(What is the RC4 encryption key size when utilizing WPA with Temporal Key Integrity Protocol (TKIP)?)

A. 40 bits

B. 56 bits

C. 128 bits

D. 256 bits

Answer: C (LEAVE A REPLY)

WPA with TKIP was designed as an interim improvement over WEP while still using the RC4 stream cipher for compatibility with legacy hardware. TKIP addresses WEP's major weaknesses by introducing per-packet key mixing, a message integrity mechanism ("Michael"), and replay protection.

In TKIP, the encryption key used with RC4 is 128 bits. Practically, TKIP derives a per-packet RC4 key from a 128-bit temporal key (TK), the transmitter's MAC address, and a sequence counter (TKIP Sequence Counter, TSC) to avoid the simple IV reuse patterns that made WEP easy to break. Even with these improvements, TKIP has known weaknesses and is deprecated in favor of WPA2/WPA3 using AES-based CCMP/GCMP. But strictly for the question asked, TKIP's RC4 keying material is based on a 128-bit key size, not 40/56-bit legacy sizes and not 256-bit.

NEW QUESTION: 21

(How does a cryptographic policy contribute to incident response?)

A. By providing guidelines for secure data recovery and communication

B. By limiting the use of encryption tools during incidents

C. By slowing down the incident resolution process
D. By increasing the likelihood of data breaches
Answer: A (LEAVE A REPLY)
A cryptographic policy defines how encryption, keys, certificates, and integrity mechanisms are used and managed across an organization. During incident response, that policy becomes a playbook for making safe, consistent decisions under pressure. It can specify how to rotate or revoke compromised keys, how to validate and reissue certificates, how to preserve evidence integrity with hashing, and how to securely communicate sensitive incident details (e.g., using approved encrypted channels). It can also define backup encryption requirements and key escrow or recovery procedures, enabling secure data recovery without exposing protected data. Policies typically outline roles and responsibilities (who can access keys, who can approve rekeying), logging requirements, and escalation steps-reducing confusion and preventing ad hoc crypto changes that might worsen exposure. The goal is not to limit encryption; it is to ensure cryptography is used correctly to contain and remediate incidents. Therefore, providing guidelines for secure recovery and communication is the correct contribution of cryptographic policy to incident response.

NEW QUESTION: 22
(What are the roles of keys when using digital signatures?)
A. A private key is used for both signing and signature validation.
B. A private key is used for signing, and a public key is used for signature validation.
C. A public key is used for both signing and signature validation.
D. A public key is used for signing, and a private key is used for signature validation.
Answer: B (LEAVE A REPLY)
Digital signatures provide integrity, authenticity, and typically non-repudiation by using an asymmetric key pair. The signer uses the private key to create a signature over a message (usually over a hash
/digest of the message). Because the private key is kept secret, only the legitimate signer should be able to produce a valid signature. Anyone who has the corresponding public key can then validate the signature: they verify that the signature matches the message digest under the public key and that the signed data has not been altered. This is why the public key can be widely distributed (often inside an X.
509 certificate) while the private key must be protected by the signer. If a public key were used to sign, anyone could forge signatures; if a private key were required for validation, only the signer could validate, defeating the purpose of public verifiability. Therefore, the correct key roles are private key for signing and public key for signature validation.

NEW QUESTION: 23
(Which attack may take the longest amount of time to achieve success?)
A. Birthday

B. Rainbow table
C. Dictionary
D. Brute-force
Answer: D (LEAVE A REPLY)
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^(n/2) for an n-bit hash, which can be less than brute-force key search in many contexts. Therefore, among the listed options, brute-force generally takes the longest to succeed because it makes the fewest assumptions and does the most total work.

NEW QUESTION: 24
(What is the Enigma machine known for in the history of cryptography?)
A. A type of cryptographic algorithm
B. A device used for secure communication during World War II
C. A method for decrypting messages
D. A software program for encrypting emails
Answer: B (LEAVE A REPLY)
The Enigma machine is historically known as an electro-mechanical cipher device used primarily by Nazi Germany to secure military and diplomatic communications during World War II. It implemented a polyalphabetic substitution through a system of rotors, a reflector, and a plugboard, producing a large number of possible daily key settings. Operators would configure rotor order, ring settings, initial positions, and plugboard swaps, then type messages to generate ciphertext. Enigma's operational security depended heavily on correct procedures and secrecy of keys; weaknesses in procedures and design properties, combined with brilliant cryptanalysis and engineering efforts by Allied codebreakers (notably at Bletchley Park), enabled large-scale decryption of Enigma-encrypted traffic. In cryptography history, Enigma represents the transition from manual ciphers to machine-assisted encryption and demonstrates how both mathematics and operational practices determine real-world security. It is not simply an "algorithm" in the modern software sense, and it is not a decryption method or email encryption tool. Therefore, the correct description is that it was a device used for secure communication during WWII.

NEW QUESTION: 25
(Which symmetric encryption technique uses a 112-bit key size and a 64-bit block size?)

A. AES
B. 3DES
C. DES
D. IDEA
Answer: B (LEAVE A REPLY)
3DES (Triple DES) is a symmetric block cipher that retains DES's 64-bit block size while increasing effective security by applying DES multiple times. The common "two-key 3DES" variant uses two independent 56-bit DES keys (K1 and K2) in an Encrypt-Decrypt-Encrypt (EDE) sequence: Encrypt with K1, Decrypt with K2, then Encrypt again with K1. Because each DES key is 56 bits (ignoring parity bits), the total keying material is 112 bits. This matches the question's "112-bit key size and 64-bit block size." Plain DES uses only a 56-bit effective key and a 64-bit block size, so it does not match the 112-bit key size. AES has a 128-bit block size and key sizes of 128/192/256. IDEA uses a 64-bit block size but has a 128-bit key.
Therefore, the correct algorithm is 3DES. Although 3DES improved on DES, it is now considered legacy due to its small 64-bit block size (birthday-bound issues for large data volumes) and performance overhead compared to AES.

NEW QUESTION: 26
(What type of encryption uses different keys to encrypt and decrypt the message?)
A. Symmetric
B. Private key
C. Secure
D. Asymmetric
Answer: (SHOW ANSWER)
Asymmetric encryption (also called public key cryptography) uses a pair of mathematically related keys: a public key and a private key. One key is used to encrypt, and the other is used to decrypt, which is the defining "different keys" property asked in the question. In the common confidentiality use case, a sender encrypts a message using the recipient's public key, and only the recipient can decrypt it using their private key. This solves the key distribution problem inherent in symmetric encryption, where both parties must securely share the same secret key in advance. Asymmetric systems also enable digital signatures: the private key signs (creates a signature) and the public key verifies it, providing authenticity and integrity. Symmetric encryption, by contrast, uses the same shared key for both encryption and decryption (even though internal round keys may exist, it is still one shared secret). "Private key" alone is not a full encryption type, and
"secure" is a generic description rather than a cryptographic category. Therefore, the correct answer is D.
Asymmetric.

NEW QUESTION: 27

(What are the primary characteristics of Bitcoin proof of work?)
A. Difficult to produce and difficult to verify
B. Difficult to produce and easy to verify
C. Easy to produce and easy to verify
D. Easy to produce and difficult to verify
Answer: B (LEAVE A REPLY)
Bitcoin's proof of work (PoW) is designed so that finding a valid block is computationally difficult, but checking validity is computationally easy. Miners must repeatedly hash candidate block headers (double SHA-256) with different nonces until they find a hash value below a network-defined target.
This trial-and-error search requires significant work and energy because the probability of success per attempt is extremely low at current difficulty levels. However, verification is straightforward: any node can hash the block header once (or a small number of times) and confirm the resulting hash meets the target threshold and that the block contents follow protocol rules. This "hard to produce, easy to verify" property is essential: it makes it expensive for attackers to rewrite history or outpace honest miners, while allowing all participants-even low-power devices-to validate blocks efficiently.
Therefore, the primary characteristic of Bitcoin proof of work is that it is difficult to produce and easy to verify.

NEW QUESTION: 28
(What describes a true random number generator?)
A. Fast and deterministic, and the same input produces the same results
B. Slow and nondeterministic, and the same input produces different results
C. Unique integer determined through factorization of integers
D. Integer increased by one to match requests and responses
Answer: B (LEAVE A REPLY)
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: 29
(What is a key benefit of using a cryptography framework?)
A. It guarantees complete security against all attacks.
B. It removes the need for employee training in security.
C. It is solely focused on regulatory compliance.
D. It provides a structured approach to implementing encryption practices.
Answer: (SHOW ANSWER)
A cryptography framework provides a consistent, repeatable way to select, deploy, and manage cryptographic controls across an organization. Its key benefit is structure: it defines approved algorithms and key sizes, acceptable modes of operation, key management rules (generation, storage, rotation, revocation, backup), certificate handling, and secure protocol configurations (e.g., TLS settings). This reduces ad hoc implementations that often lead to vulnerabilities such as weak ciphers, key reuse, improper randomness, or missing integrity protections. A framework also clarifies roles and processes-who can access keys, how secrets are audited, and how exceptions are handled-improving governance and operational reliability.
Importantly, it does not guarantee perfect security; no framework can eliminate all risk, and secure outcomes still depend on correct implementation, monitoring, and maintenance. It also does not eliminate the need for training; human error is a major source of crypto misconfiguration. While frameworks help with compliance, they are not solely about regulation; they are about sound security engineering and lifecycle management.
Therefore, the primary benefit is providing a structured approach to implementing encryption practices.

NEW QUESTION: 30
(Which mechanism can be applied to protect the integrity of plaintext when using AES?)
A. RC4
B. Message Authentication Code (MAC)
C. RSA
D. Kerberos key sharing
Answer: B (LEAVE A REPLY)
AES by itself is a symmetric block cipher that provides confidentiality, but not guaranteed integrity unless used in an authenticated mode. To protect integrity of the plaintext (ensuring it has not been altered), a Message Authentication Code (MAC) can be applied. In the classic Encrypt-then-MAC pattern, the sender encrypts the plaintext with AES and then computes a MAC (often HMAC-SHA-256 or CMAC-AES) over the ciphertext (and relevant headers). The receiver verifies the MAC before attempting decryption, preventing tampering and many padding-oracle style vulnerabilities.
Alternatively, AES can be used in an AEAD mode like AES-GCM, which produces an authentication tag serving a similar purpose, but among the listed options the general

integrity mechanism is "MAC." RC4 is an unrelated stream cipher and does not provide integrity. RSA is asymmetric and not the standard integrity add-on for AES-encrypted bulk data. Kerberos is an authentication protocol and key distribution system, not a message integrity primitive. Therefore, to protect plaintext integrity when using AES, the correct mechanism is a Message Authentication Code.

NEW QUESTION: 31
(What is the correlation between the number of rounds and the key length used in the AES algorithm?)
A. The number of rounds decreases as the key length increases.
B. The number of rounds increases as the key length increases.
C. The key length is the same regardless of the number of rounds.
D. The number of rounds is the same regardless of the key length.
Answer: B (LEAVE A REPLY)
In AES, the number of rounds is explicitly tied to the key length. AES-128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds. The purpose of additional rounds is to increase diffusion and confusion, strengthening resistance against cryptanalysis as the key schedule and state transformations iterate more times. Although key length primarily affects brute-force resistance, AES's designers and standardization parameters link longer keys with more rounds to maintain security margins across variants, especially considering differences in the key schedule structure. Thus, as key length increases from 128 to 192 to 256 bits, the number of rounds increases correspondingly from 10 to 12 to 14. This relationship is fixed by the AES specification and does not vary dynamically at runtime.
Therefore, the correct correlation is that the number of rounds increases as the key length increases.

NEW QUESTION: 32
(Which cryptographic operation uses a single key?)
A. Hashing

B. Asymmetric
C. Padding
D. Symmetric
Answer: D (LEAVE A REPLY)
Symmetric cryptography uses a single shared secret key for both encryption and decryption. This contrasts with asymmetric cryptography, which uses a key pair (public/private). Symmetric algorithms (like AES, ChaCha20) are efficient and well-suited for bulk data encryption, but they require a secure method for key distribution because both parties must possess the same secret. Hashing is not a keyed operation by default (though HMAC is keyed); it maps arbitrary data to a fixed-size digest and is primarily used for integrity checking, fingerprints, and password hashing constructions. Padding is a data formatting technique (e.g., PKCS#7) used to align plaintext to a block size; it is not a cryptographic "operation" that uses a key.
Therefore, the cryptographic operation characterized by using one key shared between parties is symmetric encryption. In real systems, symmetric encryption is frequently combined with asymmetric methods for key exchange and with MACs/AEAD for integrity, producing the standard hybrid approach used in protocols like TLS and IPsec.

NEW QUESTION: 33
(Why is lightweight cryptography important in modern information security?)
A. To complicate data protection measures
B. To ensure secure communication on high-speed networks
C. To limit the use of encryption tools in organizations
D. To address the security needs of Internet of Things (IoT) devices and mobile applications
Answer: D (LEAVE A REPLY)
Lightweight cryptography is important because many modern systems operate in constrained environments- IoT sensors, embedded controllers, wearables, and mobile devices-where CPU, memory, storage, bandwidth, and battery power are limited. Traditional "heavy" cryptographic suites may be too slow, too energy-intensive, or too large in code footprint for these platforms, leading to insecure workarounds or disabling security entirely. Lightweight cryptographic primitives and profiles are designed to deliver strong security properties (confidentiality and integrity, often via AEAD) while fitting within tight resource budgets and real-time constraints. This is essential as IoT and mobile ecosystems expand, increasing the attack surface and the consequences of compromised devices (botnets, surveillance, physical safety risks). Lightweight cryptography is not meant to "limit encryption tools" or complicate protection; it enables practical, deployable security where otherwise implementations might be weak or absent. High-speed network communication can benefit from efficient crypto too, but the defining modern driver is constrained-device security. Therefore, the correct reason is addressing the security needs of IoT devices and mobile applications.

NEW QUESTION: 34
(Which cryptographic technique is used to ensure data integrity?)
A. Authentication
B. Non-repudiation
C. Digital signatures
D. Steganography
Answer: (SHOW ANSWER)
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: 35
(What is the value of 51 mod 11?)
A. 04
B. 05
C. 07
D. 11
Answer: C (LEAVE A REPLY)
The value 51 mod 11 is the remainder after dividing 51 by 11. Modular arithmetic is widely used in cryptography to keep computations within a finite set of residues, such as in RSA where values are taken modulo n, or in Diffie-Hellman where exponents and group elements are reduced modulo a prime. To compute 51 mod 11, find the largest multiple of 11 less than or equal to 51. Multiples of 11 are 11, 22, 33, 44, 55. The closest without exceeding 51 is 44. Subtracting gives 51 # 44 = 7, so the remainder is 7. Therefore, 51 mod 11 = 7, matching option "07." This remainder is always in the range
0 through 10 because the modulus is 11. Such residue computations underpin the "wraparound" behavior that makes modular exponentiation and inverse computations well-defined in cryptographic groups.

NEW QUESTION: 36

(What is lattice-based cryptography?)
A. A technique for encoding messages using lattice points
B. A blockchain option from clone
C. A cryptographic scheme based on geometric lattices
D. A type of encryption algorithm using modular arithmetic
Answer: C (LEAVE A REPLY)
Lattice-based cryptography refers to cryptographic constructions whose security is based on the computational hardness of problems on mathematical lattices (regular grids of points in high-dimensional space). Examples of hard lattice problems include the Shortest Vector Problem (SVP) and Closest Vector Problem (CVP), and practical schemes often use related problems like Learning With Errors (LWE) or Ring- LWE. These problems are believed to remain hard even for quantum computers, making lattice-based cryptography a major candidate family for post-quantum cryptography. Lattice schemes can support encryption, digital signatures, and key exchange, often with strong security reductions (worst-case to average- case) and efficient implementations. The word "lattice" here is not about simple point encoding; it's about relying on geometric/algebraic structures and noise-based hardness assumptions. It is also unrelated to blockchain "options." While many lattice schemes do involve modular arithmetic internally, what defines the category is the underlying lattice hardness assumptions, not modular arithmetic alone. Therefore, the correct definition is a cryptographic scheme based on geometric lattices.

NEW QUESTION: 37
(Which cryptographic operation uses a single key?)
A. Hashing
B. Asymmetric
C. Padding
D. Symmetric
Answer: D (LEAVE A REPLY)
Symmetric cryptography uses a single shared secret key for both encryption and decryption. This contrasts with asymmetric cryptography, which uses a key pair (public/private). Symmetric algorithms (like AES, ChaCha20) are efficient and well-suited for bulk data encryption, but they require a secure method for key distribution because both parties must possess the same secret. Hashing is not a keyed operation by default (though HMAC is keyed); it maps arbitrary data to a fixed-size digest and is primarily used for integrity checking, fingerprints, and password hashing constructions. Padding is a data formatting technique (e.g., PKCS#7) used to align plaintext to a block size; it is not a cryptographic "operation" that uses a key. Therefore, the cryptographic operation characterized by using one key shared between parties is symmetric encryption. In real systems, symmetric encryption is frequently combined with asymmetric methods for key exchange and with MACs/AEAD for integrity, producing the standard hybrid approach used in protocols like TLS and IPsec.

NEW QUESTION: 38
(What is the relationship between Secure Sockets Layer (SSL) and Transport Layer Security (TLS)?)
A. SSL is the replacement of TLS.
B. SSL and TLS are identical in function and security.
C. SSL is only used in email encryption.
D. TLS replaced SSL to provide improved security.
Answer: (SHOW ANSWER)
TLS is the modern successor to SSL. SSL (notably SSL 2.0 and SSL 3.0) was an early protocol family for securing network communications, providing encryption, integrity, and endpoint authentication for applications like HTTPS. Over time, weaknesses were discovered in SSL's design and in the cryptographic mechanisms commonly used with it. TLS was introduced as an improved, standardized evolution (starting with TLS 1.0, based on SSL 3.0 but with important fixes), and later versions (TLS 1.2 and TLS 1.3) significantly strengthened security by removing weak ciphers, improving key exchange, and tightening handshake and record protections. In practice, when people say "SSL" today, they often mean "TLS," but true SSL is deprecated and should not be used. SSL is not a replacement of TLS, and the two are not identical in security-TLS versions incorporate substantial improvements and modern cryptographic best practices. SSL is also not limited to email; it was widely used for web traffic and other protocols. Therefore, the correct relationship is that TLS replaced SSL to provide improved security.

NEW QUESTION: 39
(What is the maximum key size (in bits) supported by AES?)
A. 128
B. 192
C. 256
D. 512
Answer: C (LEAVE A REPLY)
AES supports three standardized key sizes: 128, 192, and 256 bits, with a fixed block size of 128 bits. The maximum of these supported key sizes is 256 bits (AES-256). Key size affects resistance to brute-force key search: larger keys exponentially increase the search space. In practice, AES-128 is already considered strong against brute force with contemporary computing capabilities, while AES-256 is often chosen for compliance requirements, conservative security margins, or to hedge against future advances. AES-512 is not part of the AES standard; if 512-bit keys are desired, systems typically use different constructions (like using AES-256 in certain key-derivation or wrapping schemes) rather than changing AES itself. Therefore, the correct maximum supported AES key size is 256 bits.

NEW QUESTION: 40
(Which default port must be allowed by firewalls for the key exchange of the IPsec handshaking process to be successful?)
A. TCP 443
B. UDP 443
C. TCP 500
D. UDP 500
Answer: (SHOW ANSWER)
IPsec's initial key exchange is commonly performed using IKE (Internet Key Exchange), which negotiates Security Associations (SAs), authenticates peers, and establishes shared keys for ESP/AH protection. The traditional and default transport for IKEv1 and IKEv2 is UDP port 500. During negotiation, peers exchange proposals (crypto suites), perform Diffie-Hellman to derive key material, and authenticate using pre-shared keys, certificates, or EAP methods. If a firewall blocks UDP 500, the IKE negotiation cannot begin, preventing IPsec tunnels from forming. In many real deployments, NAT traversal is also used; in that case, traffic typically shifts to UDP 4500 (NAT-T) after detection of NAT, but UDP 500 is still required for the initial exchange and NAT detection in many configurations. TCP 500 is not standard for IKE. Port 443 is associated with HTTPS/TLS and some SSL VPNs, not IPsec IKE. Therefore, among the options provided, the firewall must allow UDP 500 for IPsec key exchange to succeed.

NEW QUESTION: 41
(A company wants to use certificates issued by a root CA to demonstrate to customers that it is a legitimate company being hosted by a cloud provider. Who needs to trust the root CA public key?)
A. The seller and the buyer
B. The cloud provider and the seller
C. The Federal Trade Commission and the cloud provider
D. The buyer and the Federal Trade Commission
Answer: A (LEAVE A REPLY)
In a public key infrastructure, trust in a certificate ultimately depends on the relying party's trust anchor set-typically the root CA certificates preinstalled in a customer's browser/OS trust store. For customers to accept the company's certificate as legitimate, the buyer (customer) must trust the root CA public key (or an intermediate chained to it) so they can validate the certificate chain and signatures. The seller (the company) also must trust and rely on the root CA public key to build and present a valid chain and to make operational decisions based on that CA's issuance and revocation mechanisms; practically, the seller selects a CA whose root is widely trusted by customers. The cloud provider's trust is not what makes the certificate valid to customers; the provider may terminate TLS or pass traffic through, but customer validation is based on the chain to a trusted root. Government

agencies like the FTC are not part of the cryptographic trust path for TLS certificate validation.
Therefore, among the given options, the correct pairing is the seller and the buyer, reflecting both the issuer selection/usage by the company and the relying-party validation by customers.

NEW QUESTION: 42
(How does a Caesar cipher operate in the encryption of messages?)
A. Encrypting messages using complex mathematical algorithms
B. Substitution of letters with their numerical equivalents
C. Reversing the order of letters in a message
D. Shifting each letter in the alphabet by a fixed number
Answer: D (LEAVE A REPLY)
A Caesar cipher is a classic monoalphabetic substitution cipher where each plaintext letter is replaced by a letter a fixed number of positions away in the alphabet. For example, with a shift of 3, A becomes D, B becomes E, and so on, wrapping around at the end (X#A, Y#B, Z#C). This "fixed shift" is the entire key: both sender and receiver must know the shift value to encrypt and decrypt. Decryption simply shifts letters back by the same amount. The Caesar cipher illustrates foundational cryptographic ideas: key-based transformation, reversible mapping, and the importance of key space size. Because the key space is tiny (only 25 meaningful shifts in the Latin alphabet), it is easily broken by brute force. It is also vulnerable to frequency analysis because letter frequency patterns in the ciphertext resemble those of the plaintext, just relabeled. While historically important for introducing substitution concepts, it provides no meaningful security by modern standards. The defining operation is the fixed positional shift, which directly matches option D.

NEW QUESTION: 43
(What describes how Counter (CTR) mode encryption functions?)
A. Converts the block cipher into a stream cipher, then uses a counter value and a nonce to encrypt the data
B. Uses a self-synchronizing stream cipher where the IV is encrypted and XORed with the data stream one bit at a time
C. Encrypts each block with the same key, where each block is independent of the others
D. Uses an IV to encrypt the first block, then uses the result of the encryption to encrypt the next block
Answer: (SHOW ANSWER)
CTR mode turns a block cipher (like AES) into a stream-like construction by generating a keystream from successive encryptions of a changing input block. Specifically, CTR forms input blocks using a nonce (unique per message) combined with an increasing counter. Each nonce||counter block is encrypted with the block cipher under the shared key, producing a pseudorandom output block. That output is then XORed with plaintext to yield

ciphertext (and XORed with ciphertext to recover plaintext). This design enables parallelization (blocks can be generated independently), efficient random access decryption, and avoids chaining dependencies seen in modes like CBC. Option B describes CFB-like behavior; option C describes ECB; option D describes CBC. CTR's security critically depends on never reusing the same nonce/counter sequence with the same key, because reuse would repeat keystream blocks and expose plaintext relationships. Therefore, the correct description is that CTR converts the block cipher into a stream cipher using a counter value and a nonce.

NEW QUESTION: 44
(A security analyst is using 3DES for data encryption. Which 3DES key size is valid?)
A. 128-bit
B. 2,048-bit
C. 56-bit
D. 112-bit
Answer: D (LEAVE A REPLY)
3DES (Triple DES) applies the DES block cipher three times to increase effective security, and its commonly cited valid key sizes correspond to how many independent DES keys are used. Two-key
3DES uses two 56-bit DES keys (K1 and K2) in an EDE sequence (Encrypt with K1, Decrypt with K2, Encrypt with K1), yielding 112 bits of keying material (ignoring parity bits). Three-key 3DES uses three independent 56-bit keys for a total of 168 bits of keying material, but that option is not listed here.
A 56-bit key corresponds to single DES, not 3DES. 128-bit is associated with AES, not 3DES. 2,048-bit is typical for RSA keys, not symmetric ciphers. Therefore, among the choices provided, 112-bit is a valid 3DES key size. While 3DES is now deprecated for many uses due to its 64-bit block size and performance limitations, understanding its keying options remains important for legacy system assessment.

NEW QUESTION: 45
(Which of the following is an example of a software encryption solution for disk storage?)
A. Virtual Private Network (VPN)
B. Hardware Security Module (HSM)
C. BitLocker and FileVault
D. USB encryption hardware
Answer: C (LEAVE A REPLY)
Disk/storage encryption protects data at rest by encrypting the contents of a drive so it remains unreadable without the correct authentication and keys. BitLocker (commonly on Windows) and FileVault (commonly on macOS) are well-known software-based full-disk encryption solutions integrated into their operating systems.

They encrypt sectors on disk and typically tie key protection to user credentials and, where available, hardware features such as a TPM or secure enclave to reduce key extraction risk. A VPN encrypts network traffic in transit, not disk storage. An HSM is specialized hardware used to generate, store, and protect cryptographic keys and perform crypto operations; it is not a disk encryption product itself. USB encryption hardware refers to hardware-encrypted removable media, not a software solution for a system disk. Therefore, the correct example of a software encryption solution for disk storage is BitLocker and FileVault.

NEW QUESTION: 46
(A security analyst is using 3DES for data encryption. Which 3DES key size is valid?)
A. 128-bit
B. 2,048-bit
C. 56-bit
D. 112-bit
Answer: (SHOW ANSWER)
3DES (Triple DES) applies the DES block cipher three times to increase effective security, and its commonly cited valid key sizes correspond to how many independent DES keys are used. Two-key 3DES uses two 56- bit DES keys (K1 and K2) in an EDE sequence (Encrypt with K1, Decrypt with K2, Encrypt with K1), yielding 112 bits of keying material (ignoring parity bits). Three-key 3DES uses three independent 56-bit keys for a total of 168 bits of keying material, but that option is not listed here. A 56-bit key corresponds to single DES, not 3DES. 128-bit is associated with AES, not 3DES. 2,048-bit is typical for RSA keys, not symmetric ciphers. Therefore, among the choices provided, 112-bit is a valid 3DES key size. While 3DES is now deprecated for many uses due to its 64-bit block size and performance limitations, understanding its keying options remains important for legacy system assessment.

NEW QUESTION: 47
(Which encryption algorithm uses an 80-bit key and operates on 64-bit data blocks?)

A. Twofish
B. Blowfish
C. Camellia
D. Skipjack
Answer: D (LEAVE A REPLY)
Skipjack is a symmetric block cipher historically associated with the Clipper chip initiative. Its defining parameters match the question: it operates on 64-bit blocks and uses an 80-bit key. The other options do not fit those exact sizes. Twofish is a 128-bit block cipher with key sizes up to 256 bits. Blowfish is a
64-bit block cipher, but its key size is variable from 32 up to 448 bits and is not fixed at 80 bits as a defining property. Camellia is a 128-bit block cipher with key sizes of 128, 192, or 256 bits. Skipjack's smaller key size and legacy design make it unsuitable for modern security needs, but the question is purely about identifying the algorithm that matches an 80-bit key and 64-bit blocks. Therefore, the correct answer is Skipjack.

NEW QUESTION: 48
(Which number of bits gets encrypted each time encryption is applied during stream encryption?)
A. 1
B. 40
C. 192
D. 256
Answer: A (LEAVE A REPLY)
In the classical definition, a stream cipher encrypts data in very small units-often described as one bit at a time-by combining plaintext with a keystream (commonly via XOR). While many practical stream ciphers operate on bytes or words for efficiency, the conceptual distinction compared to block ciphers is that stream encryption processes data as a continuous stream rather than fixed-size blocks. This is why the standard teaching answer is "1 bit" per application of the keystream. Block ciphers, by contrast, encrypt blocks like 64 bits (DES/3DES) or 128 bits (AES) in each invocation of the block primitive. Options like 40, 192, and 256 are not typical stream cipher "per-step" processing sizes; 40 and 256 are often associated with key sizes, and
192 could be a key size for AES, not an encryption granularity. The essential security requirement for stream ciphers is that the keystream must be unpredictable and never reused with the same key/nonce combination; otherwise XOR properties allow attackers to recover relationships between plaintexts. Thus, the best answer is
1.

NEW QUESTION: 49
(Why should an asymmetric private key be used to encrypt the digest of an application?)

A. An asymmetric private key uses the same key to encrypt and decrypt large amounts of media, one bit at a time.
B. An asymmetric private key signs files by signing (encrypting) the hash of a file so integrity and authenticity can be verified with the corresponding public key.
C. An asymmetric private key encrypts and decrypts data in blocks of characters at a time with a complex algorithm.
D. An asymmetric private key encrypts a small amount of information, which is decrypted with the corresponding private key.
Answer: (SHOW ANSWER)
Digital signing of software typically works by hashing the application (or its manifest) and then using the publisher's private key to create a digital signature over that digest. The private key is used because it is secret and uniquely controlled by the publisher; only the publisher should be able to produce a valid signature.
Verifiers (customers) use the publisher's public key to validate the signature and confirm that the digest matches the software they received. This yields two key properties: integrity (the software hasn't been altered; any modification changes the digest and breaks verification) and authenticity (the signature proves it came from the private-key holder).
Option A incorrectly describes symmetric stream encryption. Option C incorrectly generalizes private-key behavior as "block encryption." Option D is wrong because verification uses the public key, not a private key; also, "encrypting with private key" in this context is better understood as signing, not confidentiality encryption. Therefore, the correct rationale is that the asymmetric private key is used to sign the file's digest so the corresponding public key can verify integrity and authenticity.

NEW QUESTION: 50
(Which regulation requires organizations to implement strong encryption measures to protect credit card data?)
A. California Consumer Privacy Act (CCPA)
B. Payment Card Industry Data Security Standard (PCI DSS)
C. Health Insurance Portability and Accountability Act (HIPAA)
D. General Data Protection Regulation (GDPR)
Answer: B (LEAVE A REPLY)
For protecting credit card data, the primary compliance framework is PCI DSS (Payment Card Industry Data Security Standard). PCI DSS is an industry standard created by major card brands and administered through the PCI Security Standards Council. It sets requirements for organizations that store, process, or transmit cardholder data, including controls around network security, access control, monitoring, and cryptography.
PCI DSS explicitly addresses encryption and protection of cardholder data (for example, protecting stored cardholder data and encrypting transmission over open, public networks, and using strong cryptography and secure protocols). CCPA and GDPR are privacy regulations focused on personal data rights and governance, and while they may

encourage security measures, they are not specifically the card-industry security standard for payment data. HIPAA applies to protected health information, not payment card data. Therefore, the correct answer is PCI DSS.

NEW QUESTION: 51
(How often are transactions added to a blockchain?)
A. Approximately every 10 minutes
B. Approximately every 30 minutes
C. Approximately every 1 hour
D. Approximately every 24 hours
Answer: A (LEAVE A REPLY)
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: 52
(Which attack may take the longest amount of time to achieve success?)
A. Birthday
B. Rainbow table
C. Dictionary
D. Brute-force
Answer: D (LEAVE A REPLY)
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^(n/2) for an n-bit hash, which can be less than brute-force key search in many contexts. Therefore, among the

listed options, brute-force generally takes the longest to succeed because it makes the fewest assumptions and does the most total work.

NEW QUESTION: 53
(What is used to randomize the initial value when generating Initialization Vectors (IVs)?)
A. Key
B. Plaintext
C. Algorithm
D. Nonce
Answer: D (LEAVE A REPLY)
An IV (Initialization Vector) is a value used to ensure that encrypting identical plaintext under the same key produces different ciphertexts, preventing pattern leakage. In many secure designs, the IV must be unique (and often unpredictable) per encryption operation. A common way to ensure uniqueness is to incorporate a nonce-a "number used once." A nonce can be random, pseudo-random, or a counter-based value depending on the mode and security requirements. For example, CTR mode uses a nonce combined with a counter to produce unique input blocks; GCM uses a nonce/IV to ensure unique authentication and encryption behavior. The encryption key should remain stable across many operations and should not be used as the "randomizer" for IV generation; mixing key material into IV creation in an ad hoc way can create reuse or correlation issues. Plaintext and algorithm do not provide the needed uniqueness property. The nonce concept is specifically about ensuring one-time uniqueness of the starting value so that IV reuse does not repeat keystream blocks (stream modes) or reveal plaintext equality (CBC/CTR). Therefore, the correct choice is Nonce.