PassQueen
a.k.a dumpsqueen.com

EC-Council Certified Encryption Specialist (ECES)

ECCouncil 212-81

Version Demo

Total Demo Questions: 24

Total Premium Questions: 243

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to Cryptography	41
Topic 2, Symmetric Cryptography and Hashes	89
Topic 3, Number Theory and Asymmetric Cryptography	40
Topic 4, Applications of Cryptography	51
Topic 5, Cryptanalysis	22
Total	243

QUESTION NO: 1

The greatest weakness with symmetric algorithms is _____.

A. They are less secure than asymmetric

B. The problem of key exchange

C. The problem of generating keys

D. They are slower than asymmetric

ANSWER: B

Explanation:

The problem of key exchange is the greatest practical weakness of symmetric cryptography. A symmetric cipher uses one shared secret key, or keys that are readily derived from one another, to encrypt and decrypt information. Before protected communication can begin, every authorized party must obtain that secret key through a secure and authenticated process. Distributing the key over an untrusted network creates a bootstrapping problem: if an attacker intercepts the key, that attacker can decrypt the protected data and potentially impersonate a participant. The challenge expands substantially as the number of users or communicating pairs grows, because secure key establishment, rotation, revocation, storage, and access control must be managed for each required relationship. Symmetric ciphers such as AES are efficient and can provide very strong confidentiality when they are correctly implemented and when their keys remain secret. In real-world systems, asymmetric cryptography or authenticated key-agreement mechanisms are commonly used to establish a temporary symmetric session key, combining manageable key establishment with the performance of symmetric encryption. NIST describes key establishment as a process that securely provides cryptographic keying material to parties, while its AES standard specifies a symmetric block cipher. See NIST SP 800-56A Rev. 3 and FIPS 197: AES.

QUESTION NO: 2

Which of the following is a block cipher?

A. AES

B. DH

C. RC4

D. RSA

ANSWER: A

Explanation:

AES is a block cipher. It encrypts data in fixed-size blocks of 128 bits and supports key sizes of 128, 192, or 256 bits. AES was standardized by NIST as FIPS 197 and is the widely deployed symmetric encryption algorithm used to protect data at rest and in transit. Internally, AES performs a defined series of substitution, permutation, and key-addition transformations on each plaintext block, using the selected secret key to produce the ciphertext block. For messages longer than one block, AES is used with an approved mode of operation, such as GCM, CCM, or CBC; these modes specify how blocks are processed securely and, where applicable, how integrity or authentication is provided. The fact that AES operates on fixed-length input blocks is the defining feature that classifies it as a block cipher. NIST specifies the AES algorithm and explicitly identifies its 128-bit block size in FIPS 197. Additional implementation and mode-of-operation guidance is available in NIST's Block Cipher Techniques project documentation.

QUESTION NO: 3

Which of the following are characteristics of a cryptographically secure pseudorandom number generator (CSPRNG)? (Choose two)

A. Its output should be computationally unpredictable

B. It should be seeded from sufficient entropy

C. It must repeat the same sequence after every reboot

D. It is intended only for graphical simulations

E. Statistical randomness alone is sufficient

ANSWER: A B

Explanation:

Its output should be computationally unpredictable and **it should be seeded from sufficient entropy** are correct. A CSPRNG is intended for security-sensitive values such as cryptographic keys, nonces, and initialization values. An attacker who observes prior output should not feasibly predict later output or reconstruct the generator state. The generator also needs unpredictable seed material obtained from an adequate entropy source.

Statistical appearance alone is not enough for cryptographic use. A deterministic generator may produce values that appear random while remaining predictable if its state or seed can be recovered. NIST specifies deterministic random-bit generator constructions and entropy-source requirements in the SP 800-90 series. See NIST SP 800-90A Rev. 1 and NIST SP 800-90B.

QUESTION NO: 4

A _____ is a function that takes a variable-size input m and returns a fixed-size string.

A. Feistel

B. Asymmetric cipher

C. Symmetric cipher

D. Hash

ANSWER: D

Explanation:

Hash is correct because a hash function maps an input message of arbitrary or variable length, conventionally represented by *m*, to an output of a predetermined, fixed length called a hash value, message digest, or digest. For example, SHA-256 produces a 256-bit digest whether the input is a short password, a document, or a multi-gigabyte file. This fixed-length representation is fundamental to cryptographic integrity checking: parties can calculate and compare compact digests rather than compare entire messages. Cryptographic hash functions are also designed so that it is computationally infeasible to derive a suitable original input from a digest or to find distinct inputs with the same digest. ECES cryptography concepts therefore use “hash” to describe the variable-input, fixed-output function stated in the question. NIST’s Secure Hash Standard specifies approved hash algorithms and their fixed digest lengths, including SHA-224, SHA-256, SHA-384, and SHA-512. See NIST FIPS 180-4: Secure Hash Standard and RFC 6234: US Secure Hash Algorithms.

QUESTION NO: 5

John is responsible for VPNs at his company. He is using IPSec because it has two different modes. He can choose the mode appropriate for a given situation. What are the two modes of IPSec? (Choose two)

A. Encrypt mode

B. Transport mode

C. Tunnel mode

D. Decrypt mode

ANSWER: B C

Explanation:

IPsec supports **Transport mode** and **Tunnel mode**. In transport mode, IPsec protects the payload of the original IP packet while the original IP header remains in place. This is commonly used for direct host-to-host protection, where the communicating endpoints themselves implement IPsec. The receiving host can use the exposed IP header for normal routing while validating and decrypting the protected payload through the negotiated IPsec security association.

In tunnel mode, IPsec protects the entire original IP packet, including its original IP header, by encapsulating it inside a new IP packet with a new outer header. This mode is particularly appropriate for VPN deployments involving security gateways, such as site-to-site connections between separate networks, because internal addressing and the original packet contents are carried within the protected tunnel. IPsec architecture documentation specifies that the Encapsulating Security Payload and Authentication Header mechanisms can be applied using either transport or tunnel mode, depending on the security topology and traffic-protection requirements. See RFC 4301: Security Architecture for the Internet Protocol and the Cisco IPsec overview.

QUESTION NO: 6

Developed by Netscape and has been replaced by TLS. It was the preferred method used with secure websites.

A. OCSP

B. VPN

C. CRL

D. SSL

ANSWER: D

Explanation:

SSL is correct because Secure Sockets Layer was originally developed by Netscape to protect communications between web browsers and web servers. It provided core security services for secure websites: authentication of the server through digital certificates, confidentiality through encryption, and integrity protection to help detect modification of data in transit. SSL was widely deployed with HTTPS and therefore became the historic protocol associated with secure web browsing.

TLS was designed as SSL's standardized successor and is the protocol used by modern secure websites. Although people may still casually say that a site "uses SSL," secure implementations should use current versions of TLS rather than SSL. SSL 2.0 and SSL 3.0 have known security weaknesses and are deprecated; systems should disable them and negotiate TLS instead. This historical relationship—the Netscape origin of SSL and its replacement by TLS—directly identifies SSL as the protocol described. For protocol history and the relationship between SSL and TLS, see RFC 6101: The Secure Sockets Layer (SSL) Protocol Version 3.0. Current TLS protocol requirements and the deprecation of obsolete versions are specified in RFC 8996: Deprecating TLS 1.0 and TLS 1.1.

QUESTION NO: 7

Which of the following are appropriate uses for HMAC? (Choose two)

A. Verifying message integrity

B. Verifying that a message came from a holder of the shared secret key

C. Encrypting a message for confidentiality

D. Providing nonrepudiation to a third party

ANSWER: A B

Explanation:

Verifying message integrity and **verifying that a message came from a holder of the shared secret key** are appropriate uses for HMAC. HMAC combines a cryptographic hash function with a secret key. The sender calculates the HMAC over a message, and the receiver verifies it by performing the same calculation with the shared secret. A matching result provides message authentication and integrity assurance.

HMAC does not provide confidentiality because it does not encrypt the underlying message. It also does not provide nonrepudiation, since both communicating parties possess the same secret key and either could have generated the HMAC. NIST specifies HMAC in FIPS 198-1, The Keyed-Hash Message Authentication Code.

QUESTION NO: 8

Which of the following statements about public keys and private keys are true? (Choose two)

A. A public key may be distributed openly

B. A private key must be protected from disclosure

C. A public key must be kept secret from all users

D. Anyone with the public key can derive the private key

ANSWER: A B

Explanation:

A public key may be distributed openly and **a private key must be protected from disclosure** are true. Public-key cryptography uses mathematically related key pairs. The public key is intended for distribution and is used for operations such as signature verification or encrypting a secret for the key owner. The corresponding private key is retained by its owner and is used for operations such as signature generation or decryption.

Possession of a public key must not enable an attacker to derive the corresponding private key within feasible computational limits. In addition, public and private keys are not generally interchangeable for all operations; proper schemes and protocol rules determine their permitted use. NIST key-management guidance discusses the distinct roles and protection requirements of public and private keys in NIST SP 800-57 Part 1 Rev. 5.

QUESTION NO: 9

Which one of the following are characteristics of a hash function? (Choose two)

A. Requires a key

B. One-way

C. Fixed length output

D. Symmetric

E. Fast

ANSWER: B C

Explanation:

One-way and **Fixed length output** are core characteristics of a cryptographic hash function. A hash accepts an input message of arbitrary length and deterministically produces a message digest with a length defined by the selected algorithm. For example, SHA-256 always produces a 256-bit digest, regardless of whether the input is a short password, a document, or a large file. This predictable digest size enables hashes to be stored, compared, signed, and incorporated efficiently into security protocols.

“One-way” means that recovering a feasible original input from a given digest is computationally infeasible. More precisely, a secure cryptographic hash function provides preimage resistance: given a hash value, an attacker should not be able to practically find a message that hashes to that value. This property supports integrity checking, digital-signature workflows, and secure password-storage designs when hashes are used with appropriate salts and password-hashing schemes. NIST’s Secure Hash Standard defines approved hash algorithms and their fixed digest sizes, while NIST’s cryptographic-hash-function glossary describes the relevant security properties. See NIST FIPS 180-4 Secure Hash Standard and NIST: Cryptographic Hash Function.

QUESTION NO: 10

What must occur in order for a cipher to be considered â€˜brokenâ€™?

A. Uncovering the algorithm used

B. Decoding the key

C. Finding any method that is more efficient than brute force

D. Rendering the cipher no longer useable

ANSWER: C

Explanation:

Finding any method that is more efficient than brute force is correct because, in cryptanalysis, a cipher is considered broken when an attacker can exploit a weakness with less work than an exhaustive search of the entire key space. The attack does not need to recover every possible key, reveal the cipher’s internal algorithm, or be immediately practical on ordinary hardware. Its significance is that it establishes a cryptanalytic shortcut: the security claim based on the cipher’s full brute-force complexity no longer holds. For example, if a key of a given size would normally require trying all possible keys, but a structural weakness enables key recovery, plaintext recovery, distinguishing the cipher from a random permutation, or another meaningful attack with lower computational complexity, that constitutes a break in the cryptanalytic sense. This convention is important because cryptographic designs are evaluated not merely by whether they resist today’s feasible attacks, but by whether their intended security margin remains intact against known analytical techniques. Bruce Schneier describes this standard as finding an exploitable weakness with complexity below brute force. See the discussion of cryptanalysis at Wikipedia: Cryptanalysis and the NIST Cryptographic Standards and Guidelines resources at NIST CSRC.

QUESTION NO: 11

Which of the following is a protocol for exchanging keys?

A. DH

B. EC

C. AES

D. RSA

ANSWER: A

Explanation:

DH is correct because Diffie-Hellman is a key-agreement protocol designed to allow two parties to establish a shared secret over an insecure public channel. Each party creates a private value, derives and exchanges a corresponding public value, then combines the received public value with its own private value. Both parties consequently arrive at the same shared secret without transmitting that secret itself. The derived secret can then be used as keying material for symmetric encryption, typically after processing through an appropriate key-derivation function.

Diffie-Hellman is foundational to modern cryptographic protocols and is available in finite-field and elliptic-curve forms, commonly called DH and ECDH. Its essential purpose is key establishment rather than direct bulk-data encryption. For

secure implementations, the exchanged public values must be authenticated, such as through certificates or digital signatures, to prevent an active adversary from performing a man-in-the-middle attack. NIST describes Diffie-Hellman-based schemes as key-establishment techniques in NIST SP 800-56A Rev. 3. RFC 2631 also specifies Diffie-Hellman key agreement for use in cryptographic protocols: RFC 2631.

QUESTION NO: 12

Which of the following are security services provided by an authenticated encryption mode such as AES-GCM? (Choose two)

A. Confidentiality

B. Integrity and authentication

C. Nonrepudiation

D. Public-key distribution

E. Certificate revocation

ANSWER: A B

Explanation:

Confidentiality and **Integrity and authentication** are correct. AES-GCM is an authenticated encryption with associated data (AEAD) mode. It encrypts plaintext to protect its confidentiality and creates an authentication tag that permits the recipient to detect unauthorized modification and verify that the data was produced by a party possessing the symmetric key. Associated data can be authenticated without being encrypted.

GCM does not provide nonrepudiation because all holders of the shared symmetric key can create valid authentication tags. Correct nonce management is essential: a nonce must not be reused with the same key, because nonce reuse can seriously compromise GCM security. See NIST SP 800-38D.

QUESTION NO: 13

Which of the following statements about steganography are true? (Choose two)

A. It conceals the existence of a message

B. It can embed data in a digital cover object

C. It always provides strong cryptographic confidentiality

D. It requires a public/private key pair

E. It is identical to a digital signature

ANSWER: A B

Explanation:

It conceals the existence of a message and **it can embed data in a digital cover object** are correct. Steganography hides information within a cover medium such as an image, audio file, video, or text so that the communication may not be apparent to an observer. For example, data may be embedded by modifying selected least significant bits of image samples or by using other methods designed to minimize perceptible changes.

Steganography is distinct from encryption. Encryption transforms message content into ciphertext that is visible but intended to be unreadable without a key; steganography seeks to obscure the presence of the message itself. The two techniques can be combined by encrypting data before embedding it in a cover object. See NIST: Steganography and RFC 4949: Internet Security Glossary.

QUESTION NO: 14

You are studying classic ciphers. You have been examining the difference between single substitution and multi-substitution. Which one of the following is an example of a multi-alphabet cipher?

A. Rot13

B. Caesar

C. Atbash

D. Vigenère

ANSWER: D

Explanation:

Vigenère is a multi-alphabet, or polyalphabetic substitution, cipher. It encrypts alphabetic plaintext using a repeating keyword: each keyword character selects a different Caesar-style substitution shift for the corresponding plaintext character. Consequently, the same plaintext letter can encrypt to different ciphertext letters at different positions, depending on the active character in the key. This use of multiple substitution alphabets distinguishes Vigenère from a monoalphabetic substitution cipher, which applies one fixed substitution mapping throughout a message.

A common way to visualize the Vigenère process is with the *tabula recta*, a table containing shifted alphabets. For each plaintext position, the row selected by the key letter and the column represented by the plaintext letter determine the ciphertext character. Although Vigenère was historically important because polyalphabetic substitution obscures simple single-letter frequency patterns more effectively than a fixed substitution, it is not secure by modern cryptographic standards. Repeated-key Vigenère can be attacked by determining the likely key length and then analyzing the separate Caesar-shift streams. See the Encyclopaedia Britannica overview of the Vigenère cipher and the Khan Academy explanation of Vigenère encryption.

QUESTION NO: 15

Which of the following statements about ephemeral Diffie-Hellman key exchange are true? (Choose two)

A. It creates a new temporary key pair for a session

B. It can provide forward secrecy

C. It inherently authenticates both parties

D. It requires the shared secret to be transmitted directly

E. It uses only symmetric-key operations

ANSWER: A B

Explanation:

It creates a new temporary key pair for a session and **it can provide forward secrecy** are correct. In ephemeral Diffie-Hellman, each party generates short-lived private and public values for the particular connection. The derived shared secret is used with a key-derivation function to create session keys. If the ephemeral private values are erased after use, later compromise of a long-term authentication key does not ordinarily permit decryption of previously recorded sessions.

Diffie-Hellman alone does not authenticate the communicating parties. It must be combined with certificates, signatures, pre-shared keys, or another authentication mechanism to prevent an active man-in-the-middle attack. TLS 1.3 uses ephemeral key exchange to provide forward secrecy. See RFC 8446: The Transport Layer Security Protocol Version 1.3 and NIST SP 800-56A Rev. 3.

QUESTION NO: 16

Which of the following are valid key sizes for AES (choose three)?

A. 192

B. 56

C. 256

D. 128

E. 512

F. 64

ANSWER: A C D

Explanation:

The valid AES key sizes are **128**, **192**, and **256** bits. AES is the symmetric block-cipher standard specified by the U.S. National Institute of Standards and Technology in FIPS 197. While AES always encrypts fixed-size 128-bit blocks, the standard defines three approved key lengths. AES-128 uses a 128-bit key and performs 10 encryption rounds; AES-192 uses a 192-bit key and performs 12 rounds; and AES-256 uses a 256-bit key and performs 14 rounds. The selectable key lengths allow implementations to use a strength level appropriate to their security requirements, compatibility needs, and cryptographic policy. In particular, AES-256 is commonly selected where a larger security margin or policies requiring a 256-bit symmetric key are applicable. These three sizes are not merely conventional labels: they are the precise key lengths included in the AES standard, and conforming AES implementations support one or more of these standardized variants. NIST's formal AES specification identifies 128, 192, and 256 bits as the supported cipher-key lengths; its AES overview likewise describes AES as operating on 128-bit blocks with keys of these three lengths. See NIST FIPS 197: Advanced Encryption Standard (AES) and NIST Approved Cryptographic Algorithms.

QUESTION NO: 17

A protocol for key aggreement based on Diffie-Hellman. Created in 1995. Incorporated into the public key standard IEEE P1363.

A. Blum Blum Shub

B. Elliptic Curve

C. Menezes-Qu-Vanstone

D. Euler's totient

ANSWER: C

Explanation:

Menezes-Qu-Vanstone is correct because MQV is an authenticated key-agreement protocol derived from Diffie-Hellman key exchange. Its name comes from its designers, Alfred Menezes, Minghua Qu, and Scott Vanstone, who introduced the scheme in 1995. MQV combines each party's long-term static key pair with an ephemeral key pair during the shared-secret computation. This design provides authentication as part of establishing the keying material, rather than merely producing an unauthenticated Diffie-Hellman shared secret. The protocol can operate in traditional finite-field groups and has an elliptic-curve form commonly called ECMQV. MQV was specified as a key-establishment scheme in the IEEE 1363 family of public-key cryptography standards, matching the historical clue in the question. NIST's key-establishment guidance identifies MQV among the Diffie-Hellman-based authenticated key-agreement schemes and documents the broader requirements for such schemes, including use of static and ephemeral key material. See NIST SP 800-56A Rev. 3 and the IEEE 1363 standard record.

QUESTION NO: 18

Which of the following are recommended practices for protecting passwords in a stored credential database? (Choose two)

A. Use a unique random salt for each password

B. Use a slow password-hashing function

C. Store passwords using reversible encryption

D. Use one common salt for all users

E. Use unsalted MD5 hashes

ANSWER: A B

Explanation:

Use a unique random salt for each password and **use a slow password-hashing function** are correct. A unique salt prevents identical passwords from producing identical stored values and makes generic precomputation attacks ineffective across the database. A deliberately expensive password-hashing scheme increases the cost of each offline password guess after a database compromise. Modern password-storage schemes include Argon2id, scrypt, bcrypt, and PBKDF2 when configured with suitable work factors.

Passwords should not be encrypted with a reversible algorithm for ordinary password verification, and a single shared salt offers substantially less protection than an independently generated salt per credential. NIST provides password-verifier requirements, and OWASP provides practical password-storage guidance. See NIST SP 800-63B and the OWASP Password Storage Cheat Sheet.

QUESTION NO: 19

A number that is used only one time, then discarded is called what?

A. IV

B. Nonce

C. Chain

D. Salt

ANSWER: B

Explanation:

Nonce is correct because the term means “number used once.” In cryptography, a nonce is a value generated for a particular operation, message, or protocol exchange and must not be reused in the context in which uniqueness is required. It is commonly random, pseudorandom, or sequentially generated, depending on the cryptographic scheme. Its one-time nature lets a protocol associate a value with a fresh transaction, helping prevent replay of a previously valid authentication request or message. Nonces are also essential inputs in many authenticated-encryption modes and challenge-response authentication mechanisms, where repeating a nonce with the same key can undermine security. The precise requirement is generally uniqueness rather than unpredictability, although protocols may require both properties when the nonce also serves as a challenge. NIST describes nonce values as values used to ensure uniqueness in cryptographic operations and specifies nonce requirements for authenticated encryption in its guidance on GCM. See NIST’s nonce glossary entry and NIST SP 800-38D.

QUESTION NO: 20

What does the OCSP protocol provide?

A. Revoked certificates

B. Hashing

C. VPN connectivity

D. Encryption

ANSWER: A

Explanation:

Revoked certificates is the correct answer because the Online Certificate Status Protocol (OCSP) enables a relying party, such as a browser or application, to obtain the current revocation status of a specific X.509 certificate. The party sends an OCSP request to an OCSP responder, which returns a signed response indicating a status such as *good*, *revoked*, or *unknown*. This lets certificate users determine whether a certificate should still be trusted—for example, whether it has been revoked because its private key was compromised or it was issued improperly.

OCSP is defined by RFC 6960 and is commonly used as a more targeted, potentially more timely certificate-status mechanism than downloading and searching an entire certificate revocation list. In practice, certificate status may also be conveyed through OCSP stapling, where a server obtains a recent OCSP response and provides it during the TLS handshake. The protocol's core purpose remains checking whether a certificate has been revoked or is currently valid according to the issuing certificate authority's status information. See RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol—OCSP and the IETF OCSP specification update draft.

QUESTION NO: 21

What is a variation of DES that uses a technique called Key Whitening?

A. Blowfish

B. DESX

C. 3DES

D. AES

ANSWER: B

Explanation:

DESX is the DES-derived block cipher variant that uses key whitening to strengthen DES against brute-force attacks. DESX applies DES with a standard DES key, while additionally XORing the plaintext with an independently derived pre-whitening value before DES encryption and XORing the result with a post-whitening value afterward. These extra keying values increase the effective key material involved in the construction and make exhaustive-key-search techniques against ordinary DES substantially less practical than they would be against DES alone. DESX was introduced by Ronald Rivest and was notably used in Microsoft's implementation of the Windows NT password-encryption mechanism. Key whitening is a general construction technique, but DESX is specifically the named DES variation identified with it. The original description is available in Rivest's paper, The DESX Encryption Algorithm. Further technical background on DESX and its whitening construction is provided by Applied Cryptography material from Bruce Schneier.

QUESTION NO: 22

All of the following are key exchange protocols except for____

A. MQV

B. AES

C. ECDH

D. DH

ANSWER: B

Explanation:

AES is the correct exception because it is a symmetric-key block cipher, not a key-exchange or key-agreement protocol. Its purpose is to encrypt and decrypt data using the same previously established secret key. AES therefore protects the confidentiality of information after communicating parties already possess a shared key; it does not provide a mathematical mechanism through which those parties can establish that key over an untrusted network.

The AES standard specifies encryption with key sizes of 128, 192, or 256 bits and operates on fixed 128-bit data blocks. In a secure cryptographic design, a separate key-establishment process supplies or derives an AES session key, after which AES can encrypt the session's traffic efficiently. NIST's AES specification identifies AES as an encryption algorithm, while NIST key-establishment guidance treats finite-field and elliptic-curve Diffie-Hellman–based mechanisms as methods for establishing shared secret material. This distinction between protecting data and establishing the key used to protect it is central to cryptographic protocol design. See the NIST AES standard (FIPS 197) and NIST SP 800-56A Rev. 3 key-establishment guidance.

QUESTION NO: 23

Nicholas is working at a bank in Germany. He is looking at German standards for pseudo random number generators. He wants a good PRNG for generating symmetric keys. The German Federal Office for Information Security (BSI) has established four criteria for quality of random number generators. Which ones can be used for cryptography?

A. K4

B. K5

C. K3

D. K2

E. K1

ANSWER: A C

Explanation:

K3 and K4 are the applicable BSI quality classes for cryptographic use because they require security properties beyond statistical randomness. K3 requires that an attacker who obtains a portion of the generator's output cannot practically derive other past or future output values or reconstruct the generator's internal state. This is the essential unpredictability requirement for a deterministic generator used to produce secret symmetric keys: observing generated values must not enable prediction of keys generated later.

K4 adds protection against recovery of earlier output and earlier internal states even if the current internal state becomes known. This property is commonly called backward secrecy or resistance to state compromise for past outputs. It provides stronger assurance where protecting previously generated key material matters after a potential compromise.

Consequently, K3 supplies the predictive resistance expected of a cryptographic pseudorandom number generator, while K4 provides that capability together with stronger protection for prior values. BSI's deterministic random-number-generator guidance defines functionality classes and security requirements for such generators; modern cryptographic DRBG design similarly emphasizes resistance to prediction and compromise. See BSI's AIS 20 guidance and NIST's SP 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators.

QUESTION NO: 24

Which of the following are functions of a certificate authority (CA)? (Choose two)

A. Issue public-key certificates

B. Digitally sign issued certificates

C. Store every subscriber private key

D. Encrypt all traffic for certificate subjects

ANSWER: A B

Explanation:

A certificate authority issues certificates and signs certificates using its CA private key. Before issuing a certificate, the CA follows its validation procedures to establish that the requester has satisfied the applicable identity or domain-control requirements. The CA signature binds the subject information and public key contained in the certificate so relying parties can validate the certificate through a trusted certification path.

A CA does not normally retain each subscriber's private key, and it does not encrypt all communications between certificate holders. Certificate issuance, certificate-status management, and revocation publication are PKI functions associated with the CA. The X.509 Internet PKI profile is specified in RFC 5280.