Eccouncil

(212-81v3)

EC-Council Certified Encryption Specialist

Total: **64 Questions**

Link:

MYEXAM.FR

Explanation:

D is correct because X.509 is the internationally recognized specification that defines the syntax, fields, encoding, and processing rules for public-key certificates used across PKIs.
X.509, as an ITU-T recommendation and the foundation for Internet profiles (e.g., RFC 5280), prescribes ASN.1/DER encoding, required and optional extensions, certificate chaining semantics, and validation rules necessary for interoperable certificate use.
Choosing X.509 provides vendor-neutral interoperability, explicit semantics for key usages and subject identifiers (subjectAltName, keyUsage, extKeyUsage), and out-of-the-box compatibility with TLS, S/MIME, and other protocol stacks.
From an operational and compliance perspective X.509 enables predictable trust-path construction, standardized validation behavior, and integration with revocation mechanisms (CRL, OCSP) referenced to the certificate format.
X.509's normative profile for Internet usage is captured by RFC 5280, which is the appropriate technical reference when assessing certificate content, encodings, and processing for production deployment.

Structured critique of the incorrect options:
A. CA — incorrect because a Certification Authority is an organizational role that issues and signs certificates; it is not a specification of certificate format or field semantics.
B. CRL — incorrect because a Certificate Revocation List is a revocation mechanism/document enumerating revoked certificates, not the schema/format of certificates themselves.
C. RFC 2298 — incorrect because an RFC identifier denotes an IETF document; RFC 2298 does not define the international certificate syntax and semantics that X.509 (and its Internet profile RFC 5280) provide.

Reference:
https://datatracker.ietf.org/doc/html/rfc5280" target="_blank">https://datatracker.ietf.org/doc/html/rfc5280
https://www.itu.int/rec/T-REC-X.509/en" target="_blank">https://www.itu.int/rec/T-REC-X.509/en
https://learn.microsoft.com/en-us/windows/win32/seccrypto/x-509-certificate

" target="_blank">https://learn.microsoft.com/en-us/windows/win32/seccrypto/x-509-certificate

Question: 3

What is the basis for the difficulty in breaking RSA?

A. Factoring numbers
B. Hashing
C. Equations that describe an elliptic curve
D. The birthday paradox

Answer: A

Explanation:

Because RSA's private exponent can be derived from the modulus's totient, and that totient is efficiently obtainable only by factoring the RSA modulus N = p·q, RSA's security rests on the practical intractability of integer factorization for large N.

RSA keys are generated by choosing large primes p and q, publishing N = p·q and e, and computing d as the modular inverse of e modulo φ(N); knowledge of p and q yields φ(N) and therefore d, so an adversary that factors N immediately recovers the private key. Conversely, the best-known classical attacks on standard RSA reduce to factoring or to computing equivalent number-theoretic information (no polynomial-time

D. WPA

Answer: C

Explanation:

WPA2 is correct because it implements AES-CCMP authenticated encryption under the 802.11i framework, providing strong, well-analyzed confidentiality and integrity primitives superior to RC4-based and TKIP fixes.

Reasoning: AES-CCMP in WPA2 uses a block-cipher mode that provides both confidentiality and integrity protection with per-packet nonces and robust replay protection; its security relies on well-studied AES primitives and standardized key management (802.1X/EAP or PSK) rather than the ad-hoc fixes of earlier protocols. Compared to alternatives, WPA2's cryptographic design resists the core classes of attacks that exploit weak IV reuse, stream-cipher key mixing, or weak message integrity checks found in legacy schemes; it also enables enterprise-grade authentication and centralized key distribution. While no deployment is invulnerable (e.g., implementation-level attacks such as KRACK demonstrated practical weaknesses that require patching), the protocol design of WPA2 remains the strongest of the listed options when correctly configured and updated. For exam purposes the decisive criteria are the underlying cipher (AES) and AEAD integrity mode (CCMP) mandated by WPA2 and defined in 802.11i.

Why the other options are incorrect:A. WEP — Fundamentally broken: uses RC4 with short IVs and weak IV scheduling, enabling trivial passive key recovery and forgery attacks.
B. TKIP — Interim mitigation for WEP that still uses RC4 and adds per-packet key mixing and the weak Michael MIC, leaving cryptographic design weaknesses exploitable in practice.
D. WPA — Uses TKIP as its primary mode (or RC4-based options) and therefore inherits TKIP/RC4 vulnerabilities; it was a transitional standard before WPA2's AES-CCMP adoption.

References:https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdfhttps://www.wi-fi.org/discover-wi-fi/securityhttps://standards.ieee.org/standard/802_11i-2004.html

Question: 7

Tom is explaining historical cryptography to a class of security students. Which of the following ciphers is a subset of the Vigenère cipher?

A. Scytale
B. Caesar
C. Blowfish
D. Atbash

Answer: B

Explanation:

The correct answer is B, Caesar cipher.

The Caesar cipher is a substitution cipher where each letter in the plaintext is shifted a certain number of positions down the alphabet. This fixed shift is the key. For instance, a Caesar cipher with a shift of 3 would replace 'A' with 'D', 'B' with 'E', and so on.

The Vigenère cipher is a polyalphabetic substitution cipher that uses a keyword to determine the shift for each letter of the plaintext. It's essentially a series of Caesar ciphers applied sequentially, based on the letters of the keyword. If the keyword is only one letter long, the Vigenère cipher becomes identical to a Caesar cipher using that single letter as the shift.

B. Decoherence
C. Funding
D. Power needs

Answer: B

Explanation:

Decoherence is the primary barrier because environmental interactions (noise, thermal photons, materials defects) destroy qubit superposition and entanglement on timescales (T1, T2) that are currently shorter than the durations and fidelities required for error-corrected, large-depth quantum algorithms. Decoherence imposes a hard physical limit on achievable gate fidelity and circuit depth: even with fast gates, accumulated noise drives logical error rates above fault-tolerance thresholds, forcing enormous quantum-error-correction overheads (often thousands of physical qubits per logical qubit) that make scaling impractical today. From a doctoral-level perspective, the problem is not merely a single engineering parameter but a multi-scale open quantum systems challenge involving materials science (two-level system defects), cryogenic and microwave engineering (thermal photons, crosstalk), and control electronics (timing jitter, spectral noise), all of which couple to qubit degrees of freedom and broaden decoherence channels. Theoretical noise models and experimental tomography consistently show that reducing decoherence and correlated noise is necessary before algorithmic parallelism or increased qubit counts translate into useful advantage; consequently, research priorities focus on coherence improvements, error-mitigation, and fault-tolerant architectures. In short, decoherence defines the effective computational window and dominates the resource cost for any realistic, scalable quantum computer.

A. Processing speed — Incorrect: gate speeds are already in the ns–μs range for most platforms and can be increased, but faster gates do not solve error accumulation from decoherence; speed without sufficient coherence and fidelity simply yields noisy results.
B. (Correct) — See above.
C. Funding — Incorrect: while significant funding accelerates research, many well-funded groups still confront fundamental decoherence physics that money alone cannot instantly resolve; capital accelerates iterative improvements but does not remove quantum noise mechanisms.
D. Power needs — Incorrect: cryogenics and control electronics do require power, but energy consumption is an engineering and systems-integration issue secondary to the fundamental coherence and error-rate limitations that determine whether computations are possible at all.

https://www.ibm.com/topics/quantum-decoherencehttps://quantumai.google/learn/quantum-errorshttps://www.nist.gov/programs-projects/quantum-information-science

Question: 10

Which of the following techniques is used (other than brute force) to attempt to derive a key?

A. Password cracking
B. Cryptography
C. Hacking
D. Cryptanalysis

Answer: D

Explanation:

D is correct because cryptanalysis is the scientific discipline that develops and applies systematic, non-brute-force methods to recover cryptographic keys or plaintext by exploiting algorithmic structure,

with no modern confidentiality, integrity, or key management and therefore not a viable or supported add-in for secure email.
B. DES — a deprecated 56-bit symmetric block cipher vulnerable to brute-force attacks; it provides only a primitive encryption primitive (no message format, signatures, or user key management) and is not used as a secure email add-in in contemporary deployments.
C. RSA — a public-key algorithm used within PGP for key exchange and signatures but not a self-contained email solution; specifying "RSA" alone omits the necessary message formatting, MIME handling, armoring, and user-level tooling that add-ins provide.

https://www.rfc-editor.org/rfc/rfc4880.htmlhttps://gnupg.org/https://www.gpg4win.org/

Question: 12

What is the name of the attack where the attacker obtains the ciphertexts corresponding to a set of plaintexts of his own choosing?

A. Kasisiki examination
B. Known plaintext
C. Differential analysis
D. Chosen plaintext

Answer: D

Explanation:

D is correct because a chosen-plaintext attack is the adversary model in which the attacker submits plaintexts of his choosing to an encryption oracle and receives the corresponding ciphertexts.

A chosen-plaintext model is a formal attack model used in cryptographic security definitions and proofs: the adversary's ability to craft plaintext queries and observe resulting ciphertexts enables adaptive probing of algebraic structure, differential behaviour, or oracle responses that are not available in passive models. This model underlies security notions such as IND-CPA and is strictly stronger than passive models because it permits controlled input selection to amplify or reveal weaknesses in the encryption algorithm. Practically, chosen-plaintext access can be exploited to build statistical distinguishers, recover key material via chosen patterns, or mount adaptive cryptanalytic procedures that rely on observed ciphertexts for attacker-selected plaintexts.

A. Kasiski examination — Classical technique to detect key period lengths (e.g., Vigenère) by analyzing repeated ciphertext substrings; it is a ciphertext-analysis method, not a model where the attacker chooses plaintexts, so it does not name the capability described.
B. Known plaintext — The attacker has some plaintext–ciphertext pairs but did not choose the plaintexts; this is a weaker, distinct model and therefore not equivalent to chosen-plaintext.
C. Differential analysis — A specific cryptanalytic technique that typically requires carefully chosen plaintext pairs with controlled differences; it is a method that can operate within a chosen-plaintext model but is not the general name for the attacker capability itself.

Therefore, the correct, general name for the attack model is chosen-plaintext attack.

https://csrc.nist.gov/glossary/term/chosen_plaintext_attackhttps://csrc.nist.gov/glossary/term/known_plaintext_a

Question: 13

RSA (Rivest-Shamir-Adleman) is a widely used public-key cryptosystem for secure data transmission. The core of RSA lies in modular exponentiation, specifically for encryption and decryption.

In RSA encryption, a plaintext message (M) is raised to the power of the public key exponent (e), and the result is taken modulo n, where n is the product of two large prime numbers (p and q). The ciphertext (C) is then C = Me mod n. This ciphertext is what is transmitted.

Option A, P = Cd mod n, represents the decryption process. Here, C is the ciphertext, d is the private key exponent, and P is the recovered plaintext.

Option B, Ce mod n, is incomplete without specifying what it represents. While it resembles part of the encryption process, it doesn't explicitly indicate the outcome (the ciphertext).

Option C, y2 = x3+Ax+B, describes the equation for an Elliptic Curve Cryptography (ECC) which is a different cryptographic algorithm than RSA.

Therefore, option D, Me mod n, precisely describes how a message (M) is encrypted in RSA using the public exponent (e) and modulus (n), producing the ciphertext. This makes it the correct description of the encryption process in RSA.

Further reading:

RSA (Rivest–Shamir–Adleman) Crypto System:
https://www.tutorialspoint.com/cryptography/rsa_algorithm.htm
RSA Cryptography: https://en.wikipedia.org/wiki/RSA_(cryptosystem)

Question: 15

Terrance is trying to describe steganography to a new employee in the security department. For this first discussion, Terrance just wants the new employee to understand the basics. The most common way steganography is accomplished is via which one of the following?

A. MSB
B. ASB
C. LSB
D. RSB

Answer: C

Explanation:

C is correct because Least Significant Bit (LSB) embedding alters only the lowest-order bits of digital samples, providing a high-capacity, low-perceptual-impact channel for hiding data and thus constitutes the most common practical steganographic technique.

LSB steganography embeds payload bits into the least significant bits of pixel color channels or audio samples so modifications are typically ±1 in sample value — below human perceptual thresholds — yielding good capacity with minimal visible/audio distortion. Its implementation is trivial (simple bitwise operations in the spatial domain) and maps directly to common uncompressed formats (BMP, PNG, WAV), which drives its ubiquity in teaching, proofs-of-concept, and many toolkits. The primary trade-offs are fragility to lossy compression and detectability by specialized statistical steganalysis, but those trade-offs still leave LSB as the canonical baseline for hiding information. In exam and operational settings, LSB is the expected answer because it best balances ease of implementation, embedding capacity, and imperceptibility compared with other single-bit-position strategies.

Structured critical evaluation of the other options:

Answer: B

Explanation:

B is correct because the Vigenère cipher applies a sequence of different Caesar-like shifts determined by a keyword, thereby using multiple substitution alphabets (polyalphabetic substitution).
A multi-alphabet (polyalphabetic) cipher is defined by its use of more than one monoalphabetic mapping so that identical plaintext letters can encrypt to different ciphertext letters depending on position or key state. Vigenère implements this by cycling through a set of shift alphabets corresponding to the key characters, which is formally equivalent to switching among multiple substitution alphabets rather than using a single fixed mapping.
This periodic switching disperses plaintext frequency distributions across multiple alphabets, increasing resistance to straightforward monoalphabetic frequency analysis and making cryptanalysis depend on period detection and key recovery techniques.
Security characteristics therefore hinge on key length and entropy; short or reused keys enable Kasiski/Friedman attacks, but the algorithm remains conceptually multi-alphabet.

Structured evaluation of incorrect options:
A. Atbash — incorrect: a single fixed reciprocal monoalphabetic substitution (each plaintext letter maps to exactly one ciphertext letter), so it is single-alphabet.
C. Caesar — incorrect: a single constant rotational shift applied to all plaintext characters, i.e., one monoalphabetic mapping for the whole message.
D. Rot13 — incorrect: a specific Caesar instance with a fixed 13-position shift; it remains a monoalphabetic, single-substitution cipher.

https://www.britannica.com/topic/Vigenere-cipher
https://en.wikipedia.org/wiki/Polyalphabetic_cipher
https://cacr.uwaterloo.ca/hac/

Question: 19

Juanita is attempting to hide some text into a jpeg file. Hiding messages inside another medium is referred to as which one of the following?

A. Steganalysis
B. Cryptography
C. Cryptology
D. Steganography

Answer: D

Explanation:

D is correct because embedding hidden data within a carrier medium to conceal the very existence of a message is the operational definition of steganography.

Steganography is the discipline and set of techniques designed to embed a payload into a host medium so that the presence of the payload is imperceptible while balancing capacity and robustness. In JPEG carriers, embedding typically modifies transform-domain elements (e.g., quantized DCT coefficients) or low-significance bits in ways that exploit human visual system thresholds and JPEG compression characteristics. The distinguishing objective is concealment of existence rather than transformation of content into an unreadable form. Cryptography transforms content to render it unreadable without a key, but it does not remove evidence that a message exists; steganography seeks to hide that evidence. In practice

well-documented biases and vulnerabilities, and is unsuitable for authentication or integrity services.
D. AES — AES is a block cipher that provides confidentiality when used for encryption; AES by itself does not ensure integrity or authenticity unless used in an authenticated mode (for example AES-GCM or AES-CMAC), so selecting “AES” alone does not meet a pure integrity requirement.

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdfhttps://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdfhttps://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf