UNIVERSITY OF SRI JAYEWARDENEPURA

Bachelor of Computing Honours in Information Systems

CIS2052 – Information Systems Security

Model Answers

Q1(a)

The plain text P = “Welcome to FoC” will be encrypted to the cipher text C = “Ygneqok vq Itx” by the Caesar cipher.

Answer: False – Caesar cipher uses a uniform shift. The ciphertext given does not match any consistent shift of the plaintext.

Q1(b)

The Advanced Encryption Standard (AES) is an example of a stream cipher.

Answer: False – AES is a symmetric block cipher (128-bit blocks), not a stream cipher. Stream ciphers encrypt bit-by-bit or byte-by-byte (e.g., RC4).

Confusion and Diffusion

Confusion: Mixing up the relationship between the secret key and the ciphertext so that studying the ciphertext does not reveal the key. Example: Substitution (S-boxes) in AES.

Diffusion: Spreading the influence of each plaintext bit across many ciphertext bits, so that a small change in plaintext changes many bits in ciphertext. Example: ShiftRows and MixColumns in AES.

Threat, Vulnerability, Attack, Countermeasure

Threat: A potential cause of harm to an information system. Example: A hacker trying to steal data.

Vulnerability: A weakness in a system that can be exploited. Example: Weak passwords.

Attack: The exploitation of a vulnerability by a threat agent. Example: Phishing to steal credentials.

Countermeasure: A control taken to reduce or eliminate vulnerabilities. Example: Using multi-factor authentication.

Q2(a)

Key properties of Hash Functions:

1. Fixed-Length Output – regardless of input size (e.g., SHA-256 → 256-bit).

2. One-Way Function – infeasible to recover input from hash.

3. Collision Resistance – hard to find two different inputs with same hash.

4. Avalanche Effect – small input change causes large hash change.

Importance: Ensures data integrity (checksums), password storage, and digital signatures.

Q2(b)

A Message Authentication Code (MAC) is a short piece of information used to verify the integrity and authenticity of a message using a secret key.

HMAC: Combines a hash function (e.g., SHA-256) with a secret key. Formula (simplified): HMAC = Hash(Key + Message + Key). Example: Used in SSL/TLS.

Q2(d)

Applications of Hash Functions:

1. Password Storage – store only hashes of passwords.

2. Digital Signatures – hash is signed to ensure integrity and authenticity.

3. Data Integrity – verify downloads and files using checksums (e.g., SHA-256).

Q3(a)

Symmetric Key Encryption uses the same secret key for encryption and decryption.

Advantages: (1) Fast for large data. (2) Simple to implement.

Disadvantage: Key distribution problem – securely sharing the secret key is difficult.

Q3(b)

AES is a symmetric block cipher with 128-bit block size and key sizes of 128, 192, or 256 bits. It is more secure and efficient than DES (56-bit key) and 3DES (slow, legacy). AES replaced DES/3DES because of its stronger security and performance.

Q3(c)

Block Cipher: Encrypts fixed-size blocks (e.g., 128 bits). Example: AES.

Stream Cipher: Encrypts data bit-by-bit or byte-by-byte. Example: RC4.

Difference: Block = chunks, better diffusion; Stream = continuous, faster for real-time data.

Q3(d)

Cipher Block Chaining (CBC): Each plaintext block is XORed with previous ciphertext block before encryption. Advantage: Hides plaintext patterns.

Counter (CTR): Encrypts counter values and XOR with plaintext. Advantage: Fast, supports parallel processing and random access.

Q4(c)

Digital Signature: A cryptographic technique using private keys to sign a message hash, ensuring integrity and authenticity. Receiver verifies with sender’s public key. If the hash matches, message is authentic and unaltered.