



CRYPTOGRAPHY AND NETWORK SECURITY

1st Internal – Exam-Ready Question Bank

9 questions – Part A | 4 questions – Part B | 3 questions – Part C

PART A – 2 MARK QUESTIONS

Write short, direct answers with important technical terms.

Q1. Define network security and list any two security services. (2 Marks)

Answer: Network security protects network resources and information from unauthorized access, modification, disclosure, and disruption. Two security services are confidentiality and authentication.

Q2. Define cryptography and identify its two major types. (2 Marks)

Answer: Cryptography protects information using mathematical techniques to ensure confidentiality, integrity, and authentication. It changes readable data into unreadable form to prevent unauthorized access and tampering. Its two types are symmetric-key cryptography and public-key (asymmetric) cryptography.

Q3. State what is meant by a block cipher and a stream cipher. (2 Marks)

Answer: A block cipher encrypts fixed-size blocks of data. A stream cipher encrypts data one bit or byte at a time using a generated key stream.

Q4. Explain the purpose of a public key and a private key in public key cryptography. (2 Marks)

Answer: The public key is openly distributed and is used for encryption. The private key is kept secret and is used for decryption.

Q5. State the mathematical conditions required for selecting RSA keys e and d . (2 Marks)

Answer: For RSA: $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$. The value d is the multiplicative inverse of e modulo $\phi(n)$, so $e \cdot d \equiv 1 \pmod{\phi(n)}$.

Q6. Differentiate between plaintext and ciphertext. (2 Marks)

Answer: Plaintext is the original readable information. Ciphertext is the transformed unreadable information produced by encryption.

Q7. State the basic components of a model for network security. (2 Marks)

Answer: A basic network security model has a sender, receiver, message, security transformation, secret information/key, and a trusted third party.



Q8. Define steganography and mention one difference between steganography and cryptography. (2 Marks)

Answer: Steganography hides the existence of a message. Cryptography changes the message into an unreadable form to protect its content.

Q9. List the main components of the DES algorithm. (2 Marks)

Answer: DES uses an initial permutation, 16 Feistel rounds, and a final permutation. It uses a 64-bit block and a 56-bit effective key.

PART B – 5 MARK QUESTIONS

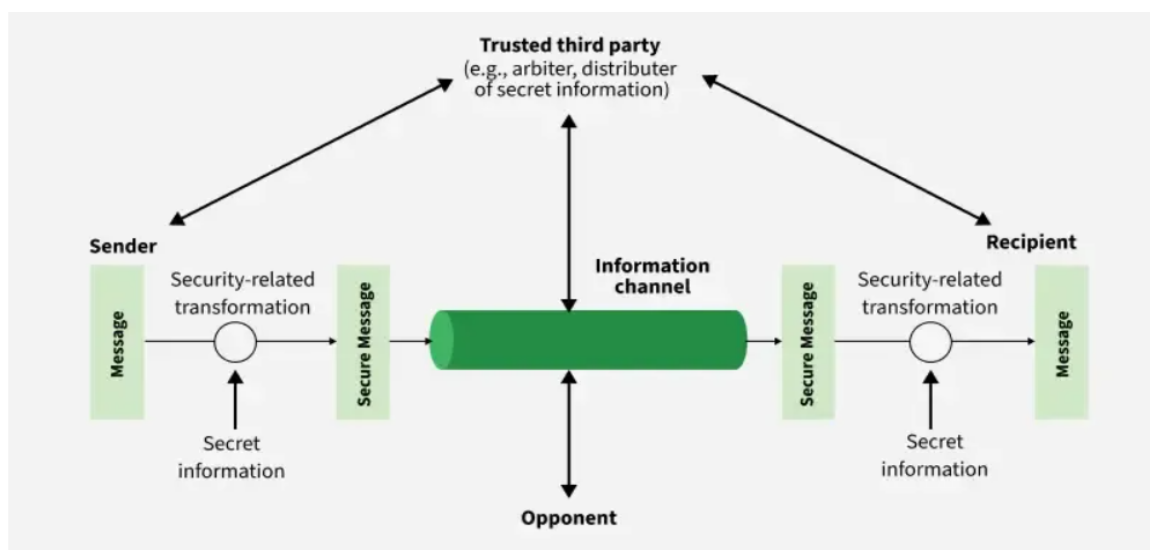
Use clear points, headings, and source-supported comparisons.

Q1. Explain the model for network security with a suitable diagram. (5 Marks)

Answer: The model shows how a sender sends a protected message to a recipient through an insecure information channel.

Main components:

- Sender: Source of the original message; it sends data securely to the intended recipient.
- Message: Original plain data generated by the sender. It is vulnerable if sent directly.
- Security-related transformation: The sender applies encryption or a digital signature to protect the message.
- Secret information: Cryptographic keys or credentials used in the transformation; they must remain confidential.
- Secure message and information channel: The encrypted or signed message is transmitted over an insecure channel such as the Internet.
- Opponent: An unauthorized entity that may intercept, read, modify, or disrupt the message.
- Trusted third party: Assists in key distribution, authentication, or verification and creates trust between sender and receiver.
- Receiver and recipient: The receiver decrypts or verifies the message using corresponding secret information so the recipient gets the original message securely.



Model for Network Security

Source diagram: Model for Network Security.

Q2. Compare cryptography and steganography. (5 Marks)

Answer: The supplied comparison is given below.



For more notes, scan & check

Basis	Steganography	Cryptography
Definition	Covered writing.	Secret writing.
Information handling	Information is hidden.	Information is transformed.
Data alteration	The structure of data is not usually altered.	The structure of data is altered.
Visibility	The fact that secret communication is taking place is hidden.	Only a secret message is hidden.
Security services	Provides confidentiality only.	Provides confidentiality, integrity, and non-repudiation.
Mathematical involvement	Not many mathematical transformations are involved.	Uses number theory and mathematics to modify data.

Q3. Explain the concept of public key cryptography. (5 Marks)

Answer: Public key cryptography securely exchanges information and authenticates users by using a pair of keys.

Components:

- Plaintext: Readable or understandable message given as input to the encryption algorithm.
- Ciphertext: Output of the encryption algorithm; it cannot be understood directly.
- Encryption algorithm: Converts plaintext into ciphertext.
- Decryption algorithm: Takes ciphertext and the matching key, then produces the original plaintext.
- Public and private key: One key is used for encryption and the other for decryption. The public key is known to everyone, while the private key remains secret.

Working:

- Key pair generation: A user generates a public key and a private key.
- Encryption: The sender obtains the recipient public key, encrypts the message with it, and sends the encrypted message over a network.
- Decryption: The recipient uses the private key to decrypt the message and recover the original plaintext.

Q4. Differentiate block cipher and stream cipher and analyze their suitability for different applications. (5 Marks)

Answer: The supplied resource gives the following source-supported comparison.

Key	Block Cipher	Stream Cipher
Definition	Encrypts plaintext one block at a time.	Encrypts plaintext one byte at a time.
Conversion of bits	Converts more bits at a time; it can convert 64 bits or more.	Only 8 bits can be transformed at a time.
Principle	Uses both confusion and diffusion.	Uses only confusion.
Decryption	Comparatively complex because more bits are encrypted together.	Uses XOR, which can be easily reversed to plaintext.



For more notes, scan & check

Key	Block Cipher	Stream Cipher
Implementation	Feistel Cipher is the most common implementation.	Vernam Cipher or Caesar Cipher is the main implementation.

PART C – 10 MARK QUESTIONS

Write the answers in clear steps with the required formulae.

Q1. Describe and analyze DES in detail. (10 Marks)

Answer: Data Encryption Standard (DES) is a symmetric block cipher. It encrypts data in 64-bit blocks and produces a 64-bit ciphertext from a 64-bit plaintext input.

Main features:

- Key length: DES starts with a 64-bit key. Every eighth bit is skipped to form a 56-bit effective key.
- Rounds: DES encrypts text in 16 rounds. Each round uses a 48-bit subkey generated from the 56-bit effective key.
- Feistel basis: DES uses the Feistel cipher attributes of substitution (confusion) and transposition (diffusion).
- Initial permutation: The 64-bit plaintext enters an Initial Permutation (IP) that rearranges the bit order according to a predefined table.

Key transformation and round subkeys:

- The 56-bit effective key is split into two 28-bit halves: Left Half (C_i) and Right Half (D_i). Here i represents the Feistel round number.
- For each of the 16 rounds, the halves undergo a circular left shift. Circular Left Shift and Permutation Choice 2 generate a different 48-bit round subkey (K_i) for every round.
- Each 48-bit subkey (K_i) is XORed with the expanded right half in the Feistel round.

Final stage:

- After 16 rounds, two 32-bit blocks, left and right, are obtained.
- The two 32-bit halves are swapped to form a 64-bit block. This is the 32-bit swap in the DES encryption algorithm.
- Finally, the block undergoes Inverse Initial Permutation (IP^{-1}), the inverse of the initial permutation.

Source note: the supplied material asks to draw either a block diagram or a flow chart for the working.

Q2. For RSA, let $p = 3$, $q = 11$, and $e = 3$. Apply the RSA algorithm to calculate n , $\phi(n)$, the public key e , the private key d , and demonstrate encryption and decryption of $M = 5$. (10 Marks)

Formulae used:

$$n = p \times q$$

$$\phi(n) = (p - 1)(q - 1)$$

$$(d \times e) \bmod \phi(n) = 1$$

$$C = M^e \bmod n$$

$$M = C^d \bmod n$$

Step 1 - Find n and $\phi(n)$:

Take the supplied prime numbers $p = 3$ and $q = 11$, then calculate n and $\phi(n)$.

$$n = p \times q = 3 \times 11 = 33$$

$$\phi(n) = (p - 1)(q - 1) = (3 - 1)(11 - 1) = 2 \times 10 = 20$$

Step 2 - Select e and find d :

Since $\gcd(3, 20) = 1$, the supplied answer selects $e = 3$. Find d such that $(d \times 3) \bmod 20 = 1$.



For more notes, scan & check

$(7 \times 3) \bmod 20 = 21 \bmod 20 = 1$; therefore $d = 7$.

Public key $(n, e) = (33, 3)$

Private key $(n, d) = (33, 7)$

Step 3 - Encryption:

For the supplied message $M = 5$, use the public key $(33, 3)$ to obtain the ciphertext.

$$C = M^e \bmod n = 5^3 \bmod 33 = 125 \bmod 33 = 26$$

Therefore, ciphertext 26 is sent over the network.

Step 4 - Decryption:

Use the private key $(7, 33)$ to recover the original message from ciphertext 26.

$$M = C^d \bmod n = 26^7 \bmod 33 = 5$$

Therefore, the recovered message is $M = 5$.

Q3. For RSA, let $p = 13$, $q = 17$, and $e = 5$. Apply the RSA algorithm to calculate n , $\phi(n)$, the private key d , and demonstrate encryption and decryption of $M = 9$. (10 Marks)

Refer to Notes.



GPT-6 ASTRA
~K/S



For more notes, scan & check