

Q1) Which of the following is not a **type** of **security** attack?

- a) Interruption
- b) Interception
- c) Modification
- d) Distribution

Q2) What is the process of converting plaintext into ciphertext called?

- a) **Decryption**
- b) Enciphering
- c) **Cryptanalysis**
- d) Coding

Q3) What does the term 'plaintext' refer to in **cryptography**?

- a) Encrypted data
- b) Decrypted data
- c) Original intelligible message
- d) **Key used in encryption**

Q4) Which of the following is not a **symmetric key** cryptographic **algorithm**?

- a) **DES**
- b) AES
- c) **RSA**
- d) Blowfish

Q5) What **type** of **cryptanalysis** is primarily **used** against **symmetric ciphers** like **DES**?

- a) Differential **cryptanalysis**
- b) Integral **cryptanalysis**
- c) Algebraic **cryptanalysis**
- d) Linear **cryptanalysis**

Q6) Which **algorithm** uses a **128-bit block size** and a **variable key size**?

- a) **DES**
- b) AES
- c) RC5
- d) Blowfish

Q7) Who is considered the **inventor** of the **RSA algorithm**?

- a) Rivest, Shamir, and Adleman
- b) Diffie and Hellman
- c) Claude Shannon
- d) Alan Turing

Q8) In **public key cryptography**, what is the **primary use** of the **private key**?

- a) Encrypting messages
- b) Decrypting messages
- c) Generating digital signatures
- d) Both B and C

Q9) Which **algorithm** is known for using a **pair** of **keys**, one for **encryption** and one for **decryption**?

- a) **DES**
- b) **RSA**
- c) AES
- d) Blowfish

Q10) What does **PKI** stand for in **network security**?

- a) **Public Key** Infrastructure
- b) **Private Key** Interface
- c) **Public Key** Information
- d) **Private Key** Implementation