All the Multiple Choice Question and Answer (MCQs) have been compiled from the books of Data Communication and Networking by the well known author behrouz A forouzan.

This Data Communication and Networking – Cryptography multiple choice Questions and Answers (MCQ) PDF covers the below lists of topics.

1. Cryptography Multiple Choice Question and Answer.

**Practice now to sharpen your concept.**

**1. _____ is the science and art of transforming messages to make them secure and immune to attacks.**
   A. Cryptography
   B. Cryptoanalysis
   C. either (a) or (b)
   D. neither (a) nor (b)

**2. The _____ is the original message before transformation**
   A. ciphertext
   B. plaintext
   C. secret-text
   D. none of the above

**3. The _____ is the message after transformation**
   A. ciphertext
   B. plaintext
   C. secret-text
   D. none of the above

**4.** A(n) _____ algorithm transforms plaintext to ciphertext
   A. encryption
   B. decryption
   C. either (a) or (b)
   D. neither (a) nor (b)

**5.** A(n) _____ algorithm transforms ciphertext to plaintext
   A. encryption
   B. decryption
   C. either (a) or (b)
   D. neither (a) nor (b)

**6.** A combination of an encryption algorithm and a decryption algorithm is called a _____.
   A. cipher
   B. secret
   C. key
   D. none of the above

**7.** The _____ is a number or a set of numbers on which the cipher operates
   A. cipher
   B. secret
   C. key
   D. none of the above

**8.** In a(n) _____ cipher, the same key is used by both the sender and receiver.
   A. symmetric-key

B. asymmetric-key
C. either (a) or (b)
D. neither (a) nor (b)

**9.** **In a(n) _____, the key is called the secret key.**
   A. symmetric-key
   B. asymmetric-key
   C. either (a) or (b)
   D. neither (a) nor (b)

**10.** **In a(n) _____ cipher, a pair of keys is used.**
   A. symmetric-key
   B. asymmetric-key
   C. either (a) or (b)
   D. neither (a) nor (b)

| Answer key for MCQ SET- 1 | |
|---|---|
| Q-1 | Correct Answer :Cryptography |
| Q-2 | Correct Answer :plaintext |
| Q-3 | Correct Answer :ciphertext |
| Q-4 | Correct Answer :encryption |
| Q-5 | Correct Answer :decryption |
| Q-6 | Correct Answer :cipher |
| Q-7 | Correct Answer :key |
| Q-8 | Correct Answer :symmetric-key |
| Q-9 | Correct Answer :symmetric-key |
| Q-10 | Correct Answer :asymmetric-key |

## Cryptography multiple choice questions and answers MCQ Set-2

**1.** **In an asymmetric-key cipher, the sender uses the_____ key.**
   A. private
   B. public
   C. either (a) or (b)
   D. neither (a) nor (b)

**2.** **In an asymmetric-key cipher, the receiver uses the _____ key**
   A. private
   B. public
   C. either (a) or (b)
   D. neither (a) nor (b)

**3.** **A _____ cipher replaces one character with another character.**
   A. substitution
   B. transposition
   C. either (a) or (b)
   D. neither (a) nor (b)

**4.** **_____ ciphers can be categorized into two broad categories: monoalphabetic and polyalphabetic.**
   A. Substitution
   B. Transposition
   C. either (a) or (b)
   D. neither (a) nor (b)

**5.** The _____ cipher is the simplest monoalphabetic cipher. It uses modular arithmetic with a modulus of 26.
   A. transposition
   B. additive
   C. shift
   D. none of the above

**6.** The Caesar cipher is a _____cipher that has a key of 3.
   A. transposition
   B. additive
   C. shift
   D. none of the above

**7.** The _____ cipher reorders the plaintext characters to create a ciphertext.
   A. substitution
   B. transposition
   C. either (a) or (b)
   D. neither (a) nor (b)

**8.** A(n) _____ is a keyless substitution cipher with N inputs and M outputs that uses a formula to define the relationship between the input stream and the output stream
   A. S-box
   B. P-box
   C. T-box
   D. none of the above

**9.** A(n) _____is a keyless transposition cipher with N inputs and M outputs that uses a table to define the relationship between the input stream and the output stream
    A. S-box
    B. P-box
    C. T-box
    D. none of the above

**10.** A modern cipher is usually a complex _____cipher made of a combination of different simple ciphers.
    A. round
    B. circle
    C. square
    D. none of the above

| Answer key for MCQ SET- 2 | |
|---|---|
| Q-1 | Correct Answer :public |
| Q-2 | Correct Answer :private |
| Q-3 | Correct Answer :substitution |
| Q-4 | Correct Answer :Substitution |
| Q-5 | Correct Answer :shift |
| Q-6 | Correct Answer :shift |
| Q-7 | Correct Answer :transposition |
| Q-8 | Correct Answer :S-box |
| Q-9 | Correct Answer :P-box |
| Q-10 | Correct Answer :round |

**Cryptography multiple choice questions and answers MCQ Set-3**

**1.** DES is a(n) _____ method adopted by the U.S. government.
   A. symmetric-key
   B. asymmetric-key
   C. either (a) or (b)
   D. neither (a) nor (b)

**2.** DES has an initial and final permutation block and _____
rounds
   A. 14
   B. 15
   C. 16
   D. none of the above

**3.** The DES function has _____ components
   A. 2
   B. 3
   C. 4
   D. 5

**4.** DES uses a key generator to generate sixteen _____ round keys
   A. 32-bit
   B. 48-bit
   C. 54-bit
   D. 42-bit

**5.** _____ DES was designed to increase the size of the DES key
   A. Double
   B. Triple
   C. Quadruple

   D. none of the above

**6.** _____ is a round cipher based on the Rijndael algorithm that uses a 128-bit block of data
   A. AEE
   B. AED
   C. AER
   D. AES

**7.** AES has _____ different configurations
   A. two
   B. three
   C. four
   D. five

**8.** ECB and CBC are _____ ciphers
   A. block
   B. stream
   C. field
   D. none of the above

**9.** One commonly used public-key cryptography method is the _____ algorithm
   A. RSS
   B. RAS
   C. RSA
   D. RAA

**10.** The _____ method provides a one-time session key for two parties
   A. Diffie-Hellman
   B. RSA
   C. DES
   D. AES

| Answer key for MCQ SET- 3 | |
| --- | --- |
| Q-1 | Correct Answer :symmetric-key |
| Q-2 | Correct Answer :16 |
| Q-3 | Correct Answer :4 |
| Q-4 | Correct Answer :48-bit |
| Q-5 | Correct Answer :Triple |
| Q-6 | Correct Answer :AES |
| Q-7 | Correct Answer :three |
| Q-8 | Correct Answer :block |
| Q-9 | Correct Answer :RSA |
| Q-10 | Correct Answer :Diffie-Hellman |