Total number of printed pages: 5 **D/V/DCSE504**

2023

Cryptography and Network Security

Full Marks: 100

Time: Three hours

The figures in the margin indicate full marks for the questions.

*Question 1 (A, B, C) is compulsory, attempt **any three** from the rest.*

1. A Multiple Choice Questions 1 x 20 = 20

i. The study of encryption method is known as
   (A) biometric
   (B) cryptography
   (C) demography
   (D) none of these

ii. Mechanism to protect private network from outside attack is
   (A) formatting
   (B) digital signature
   (C) antivirus
   (D) firewall

iii. Digital signature needs a/an _____ system.
   (A) symmetric key
   (B) asymmetric key
   (C) Neither A nor B
   (D) Both A and B

iv. Message _____ means that the data must arrive at the receiver exactly as sent.
   (A) authentication
   (B) confidentiality
   (C) integrity
   (D) none of these

v. In asymmetric key cryptography, the private key us kept by
   (A) Sender
   (B) Receiver
   (C) Sender and receiver
   (D) All the connected devices to the network

vi. The method of hiding the secrete is
   (A) Cryptography
   (B) Steganography
   (C) Stenography
   (D) Cryptanalysis

vii. Which of the following are the applications of cryptography?
   (A) Digital signature
   (B) Authentication
   (C) Key generation
   (D) All the above

viii. Which of the following stage of cryptography are the readable non-encrypted data?
   (A) Plain Text
   (B) Encryption
   (C) Cipher text
   (D) Decryption

ix. At which end encryption is performed?
   (A) Transmitter
   (B) Receiver
   (C) Channel
   (D) Both a and b

x. Which of the following is not a type of symmetric-key cryptography technique?
   (A) Caesar cipher
   (B) Data Encryption Standard (DES)
   (C) Diffie Hellman cipher
   (D) Playfair cipher

xi. Which of the following attacks is a passive attack?
   (A) Masquerade
   (B) Modification of message
   (C) Denial of service
   (D) Traffic analysis

xii. Which of the following options correctly defines the Brute force attack?
   (A) Brutally forcing the user to share the useful information like pins and passwords.
   (B) Trying every possible key to decrypt the message.
   (C) One entity pretends to be some other entity
   (D) The message or information is modified before sending it to the receiver.

xiii. "A key is a string of bits used by a cryptographic algorithm to transform plain text into ciphertext." Which of the following is capable of becoming a key in a cryptographic algorithm?
   (A) An integer values
   (B) A square matrix
   (C) An array of characters (i.e. a string)
   (D) All of the above

xiv. Conventional cryptography also known as ….. encryption.

(A) asymmetric-key
(B) logical-key
(C) symmetric-key
(D) None of these

xv. Public key cryptography is a ..... cryptosystem
(A) Symmetric
(B) Asymmetric
(C) Symmetric & Asymmetric both
(D) None of these

xvi. Which is the cryptographic protocol that is used to protect an HTTP connection?
(A) Resource reservation protocol
(B) SCTP
(C) TLS
(D) ECN

xvii. The DES (Data Encryption Standard) cipher follows the fiestal structure. Which of the following properties are not shown by the fiestal structure?
(A) The input text is divided into two parts: one being left half and another one being right half.
(B) Swapping of the left and right halves are performed after each round.
(C) The plain text is converted into a matrix form first
(D) None of the above

xviii. What is the full-form of RSA in the RSA encryption technique?
(A) Round Security Algorithm
(B) Rivest, Shamir, Adleman
(C) Robert, Shamir, Addie
(D) None of the above

xix. Consider the following steps,
i. Substitution bytes
ii. Shift Rows
iii. Mix columns
iv. Add round key
The above steps are performed in each round of which of the following ciphers?
(A) Rail fence cipher
(B) Data Encryption Standard (DES)
(C) Advance Encryption Standard (AES)
(D) None of the above

xx. Decryption is a process to unveil the _____.
(A) Unsecured data
(B) Secured data

(C) Insecure

(D) None of the mentioned above

B State True or False 1 x 10 = 10

i. The asymmetric cipher plaintext are encrypted with one key and decrypted with other key

(A) True

(B) False

ii. A process of studying cryptographic system is known as Cryptanalysis

(A) True

(B) False

iii. A key is a value that works with a cryptographic algorithm to produce a specific cipher text.

(A) True

(B) False

iv. A Public key size and conventional cryptography's secret key size are closely related with one another.

(A) True

(B) False

v. Authentication exchange preserves the Access Control

(A) True

(B) False

vi. Non repudiation can be achieved by Notarization

(A) True

(B) False

vii. DoS affects the confidentiality service

(A) True

(B) False

viii. In confusion the plaintext bits are dissipated in to long range of ciphertext bits

(A) True

(B) False

ix. Hill Cipher is an example of Asymmetric Cipher

(A) True

(B) False

x. Private Key and Public Key are used in Data Encryption Standard

(A) True

(B) False

C. Fill in the blanks 1 x 10 = 10

i. In _____ messages are hidden inside other data/images.

ii. Attacker use replica of a genuine website used for collecting user sensitive information is known as _____.

iii. In _____ cipher 5 x 5 matrix is used.

iv. Traffic Analysis is a type of _____ attack.

v. In _____ cipher the key same as long as the plaintext message is used and discarded after used.

vi. The sequence of characters or bits position are rearranged in _____ technique.

vii. _____ protects internal network from external threats.

viii. Sequence of bits/bytes/characters are encrypted and decrypted in _____ cipher.

ix. AES is a type _____ cipher algorithm.

x. _____ is used to authenticate the source/sender.

2 a. What is the OSI security architecture? Explain the Model for Network Security. 10

b. What is the difference between passive and active security threats? List and briefly define categories of passive and active security attacks. 10

3. a. What is a Security Service? List and briefly define categories of security services. 10

b. What are Security Mechanisms? List and briefly define categories of security mechanisms. 10

4 a. What are the two general approaches to attacking a cipher? List and briefly define types of cryptanalytic attacks based on what is known to the attacker. 10

b. Encrypt the message "ATTACK POSTPONED" using the Hill cipher with the key 10

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$$

Show your calculations and the result.

5 a. Explain the Fiestel Cipher Structure for Encryption and Decryption. 10

b. Explain the i-th round DES Encryption algorithm. 10

6 Write Short Notes (any four) 5 x 4 = 20

a. Notarization

b. Public Key Cryptosystem

c. RSA Algorithm

d. Digital Signature

e. Denial of Service

f. Brute Force Attack

xxXxx