



Seventh Semester B.E. Degree Examination, Dec.2023/Jan.2024
Cryptography

Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Module-1

- 1 a. Define following terms :
 - i) Cryptography
 - ii) Ciphertext
 - iii) Encryption
 - iv) Decryption
 - v) Kerchoff's principles. (10 Marks)
- b. Perform simple cipher substitution for below message "meet me after the toga party" and explain the mathematical equations with key = 3. (10 Marks)

OR

- 2 a. With a neat diagram, explain the fiestel structure of DES method. (10 Marks)
- b. Encrypt the message "Meet me at the usual place at ten rather than eight O'clock". Using the hill cipher with key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show your calculation and result. (10 Marks)

Module-2

- 3 a. Perform encryption using RSA algorithm following $P = 3, Q = 11, e = 3$ and $M = 9$. (10 Marks)
- b. Evaluate a Diffie - Hellman key exchange concept for prime number $q = 71$ and primitive root $\alpha = 7$.
 - i) If user A has private key $X_A = 5$, what is A's public key $Y_A = ?$
 - ii) If user B has private key $X_B = 12$, what is B's public key $Y_B = ?$
 - iii) What is shared key? (10 Marks)

OR

- 4 a. Compare how Diffie - Hellman key exchange algorithm useful in evaluating man - in - middle attack concept. (10 Marks)
- b. Consider an Elgamal scheme with common prime $q = 71$, and primitive root $\alpha = 7$.
 - i) If B has private key $Y_B = 3$, and A choose the random integer $k = 2$, what is the ciphertext of $M = 30$?
 - ii) If A now choose a different value of k so that the encoding of $M = 30$, is $c = (59, C_2)$ what is integer C_2 ? (10 Marks)

Module-3

- 5 a. Discuss elliptic curve cryptography for analog of Diffie - Hellman key exchange and explain with neat steps. (10 Marks)
- b. Explain pseudorandom number generation based on asymmetric cipher. (10 Marks)

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
 2. Any revealing of identification, appeal to evaluator and/or equations written eg, $42+8=50$, will be treated as malpractice.

OR

- 6 a. Apply the distribution of public key with respect to directory, authority and certificate. (10 Marks)
b. Explain secret key distribution with confidentiality and authentication. (10 Marks)

Module-4

- 7 a. What are X.509 standards? Explain the structure of X.509 certificate with neat diagram. (10 Marks)
b. Explain Kerberos version 5 message exchange with neat diagram. (10 Marks)

OR

- 8 a. Write a note on:
i) S/MIME functionality (10 Marks)
ii) Types of S/MIME message. (10 Marks)
b. Explain internet mail architecture with its key components. (10 Marks)

Module-5

- 9 a. Explain the applications of IPsec with example. (10 Marks)
b. Summarize the below :
i) IPsec documents (10 Marks)
ii) IPsec services. (10 Marks)

CMRIT LIBRARY
BANGALORE - 560 037

OR

- 10 a. Explain transport and tunnel modes of operations in ESP. (10 Marks)
b. Explain ESP packet format with Top level format and substructure of payload data. (10 Marks)
