Ex/PG/MTCT/T/222A/2024

Master of Technology in Computer Technology
Second Year Second Semester Examination
2024

Subject: Cryptography

Time: 3 Hours | Full Marks: 100

Answer Any Five Questions

1. (a) Find the multiplicative inverse of 12 in Z_{26} using Extended Euclidean Algorithm.

   (b) Distinguish between a substitution cipher and a transposition cipher.

   (c) Encrypt the message "INDIA IS GREAT" using Affine cipher with key = (15, 20). Ignore the space between words. Decrypt the ciphertext to get the original plaintext.

9+2+9=20

2. (a) List all additive inverse pairs in Z_{20}.

   (b) Distinguish between a monoalphabetic and a polyalphabetic cipher.

   (c) Encrypt the message "I LOVE JU" using Playfair cipher with the key given below. Ignore the space between words. Decrypt the ciphertext to get the plaintext:

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

8+2+10=20

3. (a) Use the extended Euclidean algorithm to find the inverse of $(x^4 + x^3 + 1)$ in $GF(2^5)$ using the modulus $(x^5 + x^2 + 1)$.

   (b) Distinguish between a stream cipher and a block cipher.

   (c) Determine whether the P-box with the following permutation tables are a straight P-box, a compression P-box, or an expansion P-box.

1	1	2	3	4	4

1	2	3	4	5	6

1	3	5	6	7

   (d) A 6 × 2 S-box exclusive-ORs the odd-numbered bits to get the left bit of the output and exclusive-ORs the even-numbered bits to get the right bit of the output. If the input is 110010, what is the output?

10+2+5+3=20

[Turn over

4. (a) Encrypt the plaintext block 01001 using the superincreasing sequence {3, 4, 10, 20, 42} with modulus $m = 90$ and multiplier $a = 17$.

   (b) State how keys are generated in RSA.

   (c) In a secure communication, the RSA public and private keys are chosen as (7, 33) and (3, 33) respectively. Show the encryption of a message m=2 and the decryption of the corresponding cipher text using these keys.

8+6+6=20

5. (a) How many rounds are there in a DES encryption/decryption? Describe a single round of DES. What are the roles of expansion P-Box?

   (b) What is an AES state? Describe the structure of each round in AES at the encryption site.

   (c) Briefly describe the different transformations that are used in each round of AES encryption.

6+6+8=20

6. (a) Describe CBC mode of operation of block ciphers. Explain one drawback of it.

   (b) Explain how CFB mode can be used as a stream cipher.

   (c) Describe the Rabin Scheme of iterated hash function.

   (d) Determine the number of padding bits for SHA-512 hash if the length of the message is 5120 bits.

6+6+6+2=20