Ref. No. : Ex/IT/PC/B/T/322/2022

B.E. INFORMATION TECHNOLOGY THIRD YEAR SECOND SEMESTER – 2022
INFORMATION SECURITY

Time : 3 hours

Full Marks : 100

CO1:

Attempt any two (2) questions 2x5=10

a) Explain in detail the various aspects of security.

b) Explain the cryptanalytic attacks with diagrams?

c) What is Perfect Secrecy? Describe a system that achieves it.

CO2

Attempt any three (3) questions 3x5=15

a) Find the inverse of the following matrix whose entries are considered as modulo 26.

$$\begin{pmatrix} 11 & 13 \\ 2 & 3 \end{pmatrix}$$

b) Use Extended Euler method to calculate 5^{-1} mod 8.

c) Consider the group $(Z_{13}^{*}, \times)$ and find all the primitive roots of the group.

d) In the Galois field $GF(2^8)$ modulo $x^8 + x^4 + x^3 + x^2 + 1$, calculate the product 0011 1001 times 0110 1100.

CO3:

a) Attempt any one (1) question 10

i. Explain the following terms respect to the keys of DES.

A. Weak key

B. Semiweak key and

C. Possible weak key

What is the probability of randomly selecting a weak, a semi-weak, or a possible weak key?

ii. A block cipher is operates on 4-bit blocks. For one particular key K, it implements the following permutation:

m	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$E_K(m)$	1	B	5	C	7	E	2	A	4	9	F	D	0	3	6	8

Using this key K, decrypt the following three ciphertexts according to the indicated modes of operation.

A. ECB: 1 8 8 B 0 6

B. CBC: 3 0 1 B 2

C. CFB: 1 0 F 6 D

b) Attempt any three (3) questions 3x5 =15

i. The matrix given in CO2(a) is used as a key to a Hill cipher to encrypt a four length string. For a given ciphertext 'YGFI', find the corresponding plaintext.

ii. Discuss the security of additive, multiplicative and affine ciphers against known plaintext attacks.

iii. How the S-boxes of DES are designed? Explain this with a tabular representation of the S-boxes (no need to consider the complex mathematical computation in GF). Suppose S-Box 3 is given below and '100011' is given as input to the S-Box 3. What will be the output?

iv. State four advantages that counter mode has over either CBC or CFB mode.

CO4:

Attempt any three (3) questions 3x5 =15

a) An RSA encryption routine calculates the value me mod n using a square-and multiply algorithm. During the execution of that algorithm, you can briefly hear a buzzing sound (through radio-frequency interference) on an AM radio receiver located near the computer. You record that sound, and discover that it is actually the following sequence of two different sounds H and L: **HHLHHLHLHHL.** 'H' and 'L' represent low sound. What is the value of e?

b) Here is a trivial example. Bob chooses $p = 11$ and $e_1 = 2$. and $d = 3$ $e_2 = e_1^d = 8$. So the public keys are (2, 8, 11) and the private key is 3. Alice chooses $r = 4$ and calculates C_1 and C_2 for the plaintext

c) Form the given Elliptic curve $y^2 = x^3 + x + 1$ in GF(13), find the points on the given curve.

d) Construct a table for the Discrete Logarithm to solve the problems like $y \equiv 5^x \bmod 11$.

CO5:

b) Attempt any one (1) question 8

i. Consider the following key agreement scheme between two entities Alice and Bob. Alice and Bob want to communicate using a conventional.encryption system. To create a key for this system they use a key distribution center, KDC, which publishes $n = pq$ but keeps p and q secret. Alice randomly chooses a number R_a, $0 < R_a < n$ and sends R^3_a mod n to the KDC. Similarly, Bob randomly chooses a number R_b, $0 < R_b < n$, and sends R^3_b mod n to the KDC. Since KDC knows both p and q, it can find R_a and R_b. The KDC sends $R_a + R_b$ mod n to Alice who finds R_b by subtracting her known number R_a. R_b is now the key agreed by Alice and Bob.

Is the above agreement is free from the man-in-the-middle attack? Discuss it.

ii. Explain briefly the concepts: one-way function, one-way hash function, trapdoor one-way function. Describe how a one-way hash function may be used for message authentication.

c) Attempt any two (2) questions 2x6=12

i. Is digital signature safe? Can someone falsify it?

ii. Explain how public key cryptography may be used for identification.

iii. Describe the goals an ideal password authentication scheme should achieve.

CO6:
Attempt any three (3) questions 3x5 =15

a) What is image encryption? Why do we need a special class of encryption methods for images?

b) When an image encryption method is said to key sensitive? How do you measure the key sensitivity of a method?

c) Let I_{MXN} be a gray scale image, design an invertible poly-alphabetic substitution method to change the value of the pixels.

d) Design a method using Fibonacci numbers to change the position of the pixels of a square image.

CO1: Identify, explain and illustrate different types of security attacks and terms related to Cryptography (K2)

CO2: Develop knowledge about mathematical concepts required in cryptography. (K3)

CO3: Illustrate Symmetric Key Cryptosystems and relevant mathematical concepts. (K3)

CO4: Illustrate Asymmetric Key Cryptosystems with relevant mathematical concepts. (K3)

CO5: Demonstrate Message integrity algorithms and Message Authentication Algorithms.(K3)

CO6: Understand and Describe image encryption and its performance measures. (K2)
