Ref. No.: Ex/IT/PC/B/T/322/2023

B.E. INFORMATION TECHNOLOGY THIRD YEAR SECOND SEMESTER – 2023
INFORMATION SECURITY

Time: 3 hours **Full Marks: 100**

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

Attempt any **two (2)** questions 2x5=10

a) In any cryptosystem, let P be the domain of the plaintext and C be the domain of the ciphertext. Prove that $|P| \leq |C|$.

b) Among monoalphabetic and polyalphabetic cipher, which one is more vulnerable? Justify your statement.

c) Define integrity and non repudiation with example.

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

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

a) Suppose $K=(k_{i,j})_{mxm}$ is a matrix over Z_n such that det(K) is invertible over Z_n. Then $K^{-1} = (\det(k))^{-1}K^*$, where K^* is the adjoint matrix of K in Z_n. Find the inverse of the matrix $\begin{pmatrix} 10 & 5 & 12 \\ 3 & 14 & 21 \\ 8 & 9 & 11 \end{pmatrix}$ where n=26.

b) Find the multiplicative inverse of 11 in Z_{26} using extended Euclidean algorithm.

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

d) Test whether the polynomial $x^8 + x^4 + x^3 + x^2 + 1$ of degree 8 in GF(2) is reducible or not.

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

a) Attempt any one (1) question 10

i. Draw the flow diagram to generate the round keys of AES-128.

ii. Discuss the 'One Time Pad (OTP)' concept. Prove that OTP is perfectly secure.

b) Attempt any **three (3)** questions 3x6 =18

i. Consider the function $h : Z_q \times Z_q \rightarrow Z_p^*$ defined as $h(x, y) = a^x b^y \bmod p$, where a, b are distinct primitive roots of mod p and p, q are prime with $p = 2q + 1$.
If $h(x_1, y_1) = h(x_2, y_2)$, for $(x_1, y_1) \neq (x_2, y_2)$, then prove that $d = \gcd(y_2 - y_1, p - 1) \in \{1, 2\}$.

ii. Suppose that we have a block cipher where n = 64. If there are ten 1's in the ciphertext, how many trial-and-error tests does Eve need to do to recover the plaintext from the intercepted ciphertext in each of the following cases?
   1. The cipher is designed as a substitution cipher.
   2. The cipher is designed as a transposition cipher.

[Turn over

iii. This problem deals with the affine cipher with the key parameters a = 7, b = 22. Decrypt the text below:
f a l s z z t y s y j z y j k y w j r z t y j z t y y n a r y j [space is given for readability]

iv. Consider an LFSR defined by the recurrence relation $z_{i+4} = (z_i + z_{i+3}) \bmod 2$. Find the period of the resulting key stream.

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

Attempt any three (3) questions 3x5 =15

a) State the Euler's theorem and use this theorem find the value of $71^{-1} \bmod 100$.

b) Let p be a prime >1, then prove that $(p-1)! \equiv -1 \pmod p$.

c) Solve the system of congruences using CRT

$$x \equiv 2 \bmod 11$$
$$x \equiv 12 \bmod 17$$
$$x \equiv 1 \bmod 11$$

d) Discuss the Chosen-ciphertext attack on RSA.

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

Attempt any one (1) question 8

i. Suppose h: X → Y is a hash function such that |X| =N and |Y|=M. For any $y \in Y$, let $h^{-1}(y)=\{x: h(x) =y\}$. Say, $s_y = |h^{-1}(y)|$ and prove that $\sum_{y \in Y} s_y = N$.
ii. A hash function must be satisfied certain criterion. Discuss those criterions.

b) Attempt any one (1) question 9

i. Present the RSA signature scheme. Suppose Alice has RSA public key n = 143, e = 103 and private key d = 7. What is the signature corresponding to the message M = 8?
ii. Discuss the Elgamal signature scheme with proper diagram.

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

Attempt any three (3) questions 3x5 =15

a) Describe the steps involved in implementing a secure image encryption system.

b) Write a pseudo code of Arnold's transform to change the position of the pixels' of a square image.

c) What is the expected correlation among the adjacent pixels of a cipher image? Derive the expression of correlation coefficient.

d) Define the differential attack. How we can claim an image encryption algorithm is robust against the differential attack?