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

B.E. INFORMATION TECHNOLOGY 3rd YEAR 2nd SEMESTER SUPPLEMENTARY EXAM – 2023

INFORMATION SECURITY

Time : 3 hour **Full Marks : 100**

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

Attempt any **two (2)** questions 2×5=10

a) What is cryptanalysis? Discuss this briefly.

b) What are the different types of security services?

c) What is the difference between an unconditionally secure cipher and a computationally secure cipher?

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

Attempt any **three (3)** questions 3×5=15

a) State Euler's theorem. Then derive Fermat's theorem from Euler's theorem.

b) Find the multiplicative inverse of 11 in Z_{22} using extended Euclidean algorithm.

c) Find the particular solution of the equation $21x + 14y = 35$.

d) Prove that set of permutations of $\{1, 2, 3\}$ with the composition operation is a group.

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

a) Attempt any **one (1)** question 10

i. Draw and explain in detail, the key generation in AES algorithm and its expansion format.

ii. Explain Triple DES and its applications.

b) Attempt any **three (3)** questions 3×6 =18

i. Find the result of multiplying $P_1 = (x^5 + x^2 + x)$ by $P_2 = (x^7 + x^4 + x^3 + x^2 + x)$ in GF(2^8) with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$.

ii. Find all the primitive roots of the group $<Z_{10}*, \times>$.

iii. Find the desired text.

1. Convert the given text "SYEDAMMAL" into ciphertext using Rail fence Technique.
2. Apply Caesar cipher and k=5 decrypt the given ciphertext "YMJTYMJWXNIJTKXNQJSHJ".

iv. Consider an LFSR defined by the recurrence relation $Zi+4 = (Zi+Zi+_3 +Zi+_2) \bmod 2$. Comments on the periodicity of the resulting key stream.

[Turn over

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

Attempt any **three (3)** questions 3×5 =15

a) Prove that list of prime numbers is infinite.

b) Find an integer that has a remainder 3 when divided by 7, 13, and remainder is 6 when divided by 12.

c) Perform encryption and decryption using RSA algorithm for P=7; q=11; e=17; M=8.

d) Using square-and-multiply technique to compute 17^{22} mod 21.

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

a) 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. List the properties of a hash function.

b) Attempt any **one (1)** question 9

i. Describe the Diffie-Hellman key exchange scheme. Assume p=11, g= 5, x= 2 and y=3. Find the key.

ii. Discuss the Elgamal signature scheme with a proper diagram.

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

Attempt any **three (3)** questions 3×5 =15

a) What is the difference between diffusion and confusion?

b) Explain the avalanche effect. How are these measured?

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

d) What is the expected entropy of an encrypted grayscale image? Write down the expression used to compute the entropy of an image.

e) Design a substitution method to modify the pixels' intensity value of a gray scale image.