Exam Date & Time: 05-Dec-2023 (02:30 PM - 05:30 PM)

MANIPAL ACADEMY OF HIGHER EDUCATION

VII SEMESTER B.TECH END SEMESTER EXAMINATIONS, NOV-DEC 2023

Cipher Systems [ECE 4069]

Marks: 50 **Duration: 180 mins.**

A

Answer all the questions.

Instructions to Candidates: Answer ALL questions Missing data may be suitably assumed

1) Solve for the number that is least non-negative integer using appropriate algorithm for the congruent equations

A) $3x \equiv 31 \bmod 533$ (5)

$4x \equiv 51 \bmod 633$

B) Construct the GF(2^4) using $p(x)=1+x+x^4$.

Determine (3)

i. Sum of $\alpha^5+\alpha^{21}+\alpha^{11}$ and (ii) Inverse of $(\alpha + \alpha^2)$

C) Determine the number of primitive roots in mod (6618) (2)

2) Calculate the plain text observing the cipher text message "**EKJ?QBU.AAKV**" using Hill cipher with **encryption key** (5)

A) $A=\begin{bmatrix} 21 & 6 & 9 \\ 1 & 3 & 24 \\ 8 & 5 & 7 \end{bmatrix}$

Assume alphabet with **A=0, to Z=25** & ' ' (space)=26, '**.**' (Dot) = 27, '**?**'=28

B) Applying 4 layer Rail fence cryptosystem to decipher the received cipher text

(D AOKOTC NODC. OOYDG UNP L). consider alphabet including special characters with dot, space (2)

C) Determine the output of 7^{th} round function DES, given the output of **XOR with Key** inside the round function results into "110101 101011 001100 111111 101101 000000 110111 101001". (3)

3) Calculate the plain text from the cipher text “00010010” using s-DES with encryption key : 0110110110. (5)

A)

B) List the operations carried in sequence on input state fed in second round of AES. Determine the output of shift row transformation in second round, if the input state given to **shift row transformation**, is given below: (2)

$$\left[\begin{bmatrix} 0A & 1B & 2C & 3D \\ 4E & 5F & 60 & 71 \\ 82 & 93 & A4 & B5 \\ C6 & D7 & E8 & F9 \end{bmatrix}\right]$$

C) Calculate the inverse Sub Byte transformation of AF. Show the computation steps clearly. Verify the result using the table. (3)

4) Determine the public key declared by Alice using ElGamal cryptosystem considering g=7, p=67 and Alice private key d=10. Using the public key Bob encrypts the plain text with its own private key r=14 and transmits (39,15), (39,0), (39,34), (39,23) to Alice. Determine the message decrypted by Alice. (5)

A) Consider the 26-letter alphabet with A=0 ...Z=25.

B) Determine the public keys shared by user 1 and user 2 and the common key generated using Diffie Hellman Key exchange for the choice of g=7, n=319. The private key chosen by User 1 & user 2 are 31 (3)

& 29 respectively.

C) Determine the formatted block in Hex representation that is used by SHA 512, if the message consists of ABC....Z. Use ASCII code for A to Z in Hex are 41 to 5A respectively. (2)

5) Explain with neat diagrams and equations the working of compression function of SHA 512. (4)

A)

B) Determine the sum of points (6,35) & (5,8) for Elliptic curve defined by $E_{97}(3,21)$ (3)

C) Determine the inverse of $2(\alpha, \alpha^8)$ for Elliptic curve defined by $E_{2^4}(\alpha^4,1)$ (3)

-----End-----