IV-MCA-CR (4.4)

2021

Time: 2 Hours **Full Mark: 70**

(Answer all questions and the figures in the right hand margin indicates marks)

1.

a) Which security services are guaranteed when using each of the following methods to send mail at the post office? [6]

i. Regular mail
ii. Regular mail with delivery conformation
iii. Regular mail with delivery and recipient signature
iv. Certified mail
v. Insured mail
vi. Registered mail

b) Find the multiplicative inverse of residue matrix over Z_{10}. [8]

$$\begin{bmatrix} 4 & 2 \\ 1 & 1 \end{bmatrix}$$

OR

c) Briefly explain different kind of cryptanalysis attacks. [6]

d) Show that, how Extended Euclidean algorithm finds the multiplicative inverse of a number in Z_n? Find the multiplicative inverse of 23 in Z_{100}. [8]

2.

a) Use a Hill cipher to encipher the message "COOL". Use the following key. [6]

$$K=\begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$$

b) Discuss the known plaintext attack of above Hill cipher encryption. [8]

OR

a) Construct a Playfair cipher matrix with the keyword 'occurrence' and find out the ciphertext of plaintext string: "let us meet". [6]

b) Discuss encryption and decryption process of Affine cipher. How Affine cipher is vulnerable to chosen plaintext attack. [8]

3.

a) Describe detail functionality of Data Encryption Standard (DES) with block diagram. [8]

b) Use the extended Euclidean to find the inverse of (x^4+x^3+1) in $GF(2^5)$ using the modulus (x^5+x^2+1). [6]

OR

c) Explain SubByte transformation of Advanced Encryption Standard (AES) with example. [8]

d) Show how to multiply (10101) by (10000) in $GF(2^5)$ and use (x^5+x^2+1) as modulus. [6]

4.

a) Briefly explain the idea behind ECC. [6]
   i. What is one-way function in this system?
   ii. What is trapdoor in this system?
   iii. Define the public and private key in this system.
   iv. Describe the security in this system.

b) Given an Elliptic curve E: $y^2 = x^3 + 2x + 2 \bmod 17$ and point P=(5, 1) and Q=(7, 6). Compute 3P and P+Q. [8]

OR

a) Describe the mathematical foundation of RSA algorithm. Perform encryption and decryption of following. [8]
P=17, q=7, e=5, n=119 and message= "6"

c) Briefly explain the idea behind the RSA cryptosystem. [6]
   i. What is one-way function in this system?
   ii. What is trapdoor in this system?
   iii. Define the public and private key in this system.
   iv. Describe the security in this system.

5.

d) Distinguish between a Modification detection code (MDC) and a Message authentication code (MAC). [6]

e) Define and explain Digital signature standard (DSS). [8]

OR

a) Consider Diffie-Hellman scheme with a common prime q=11 and primitive root α=2. [8]
   i. Show that 2 is primitive root of 11.
   ii. If user A has public key Y_A=9, what is A's private key?
   iii. If user B has public key Y_B=3, what is the secret key K shared with A?

f) How Confidentiality and Nonrepudiation security services can achieve by digital signature? Explain. [6]