III-MTECH-CNS (3.1)

2020

Time: 3 Hours **Full Mark: 70**

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

1.

a) Define security mechanisms to provide security services. [6]

b) The plaintext “letusmeetnow” and the corresponding ciphertext “HBCDFNOPIKLB” are given. You know that the algorithm is a Hill cipher, but you don’t know the size of the key. Find the key matrix. [8]

OR

c) Define the three security goals. What is the difference between active and passive attack? Names some of passive and active attacks. [7]

d) Let us define a new stream cipher. The cipher is Affine, but the key depend on the position of the character in the plaintext. If the plain text character to be encrypted is in position i, we can find the keys as follows: [7]

i. The multiplicative key is the (i mod 12)th element in Z_{26}*.

ii. The additive key is the (i mod 26)th element in Z_{26}.

Encrypt the message “cryptography” using this new cipher.

2.

a) Compare DES and AES. Which one is bit-oriented? Which one is byte oriented? [7]

b) Create a table for addition and multiplication for GF(2^4), using (x^4 +x^3+1) as modulus. [7]

OR

c) Define MixColumn Transformation. Why do you think the mixing transformation (MixColumn) in not needed in DES, but is needed in AES? [6]

d) Find out the SubByte transformation of $(5A)_{16}$. [8]

3.

e) Define Fermat’s little theorem and explain its application. [4]

f) Describe the mathematical foundation of RSA algorithm. Perform encryption and decryption of following. [10]
P=17, q=7, e=5, n=119 and message= “6”

OR

g) Define discrete logarithms problem and explain their importance. [4]

h) Define an elliptic curve. List all the points on the elliptic curve E_7(0, -2) and find the sum (3, 2) + (5, 5) on this elliptic curve. [10]

4.

a) Explain criteria of cryptographic hash function. [4]

b) Define RSA digital signature scheme and compare with it to the RSA cryptosystem. [10]

OR

a) Distinguish between an MDC and a MAC. [4]

b) Define Elgamal digital signature scheme by tacking one example. [10]

5.

a) Name seven types of packets used in PGP and explain their purposes. [7]

b) In PGP, explain how sender and receiver exchange the secret key for encrypting message. [7]

OR

a) Briefly describe the purposes of different content types defined by Cryptographic message syntax (CMS). [7]

b) In S/MIME, explain how sender and receiver exchange the secret key for encrypting message.[7]