III-MTech(CSE)-CNS (3.1)

M.Tech (CSE) 3rd Sem-2019

Sub: Cryptography and Network Security

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

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

1.

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

b) List all multiplicative inverse pair in modulus 20. [7]

OR

c) What are the essential ingredients of a symmetric cipher? List and briefly define type of cryptanalytic attack based on what is known to attacker. [7]

d) Find the determinant and the inverse of residues matrix over Z_{10}. [7]

$$\begin{bmatrix} 3 & 4 & 6 \\ 1 & 1 & 8 \\ 5 & 8 & 3 \end{bmatrix}$$

2.

a) Use a Hill cipher to encipher the message “We live in an insecure world”. Use the following key. [7]

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

b) Show the calculation for the corresponding decryption of the ciphertext to recover the original message. [7]

OR

c) The Hill cipher succumbs to a known plaintext attack if sufficient plaintext-ciphertext pair are provided. It is even easier to solve the Hill cipher if a chosen plaintext attack can be mounted. Describe such an attack. [7]

d) Use the Playfair cipher to encipher the message “The key is hidden under the door pad”. The secrete key is “GUIDANCE”. Find out the original message. [7]

3.

a) What is the difference between a block cipher and a stream cipher? [2]

b) Explain the avalanche effect. [2]

c) How many number of permutation are used in a DES cipher algorithm? How many number of permutation are used in the round-key generator? [4]

d) 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

e) Find out the SubByte transformation of $(6C)_{16}$. [8]

f) 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 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.

b) In RSA, given p=13, q=17 and e=5, Encrypt the message “HELLO” using the 00 to 25 encoding scheme. Decrypt the ciphertext to find the original message. [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”

b) Alice uses Bob’s RSA public key (e=7, n=143) to send the plaintext P=8 encrypted as ciphertext C=57. Show how Eve (Attacker) can use the chosen-ciphertext attack if she has access to Bob’s computer to find the plaintext. [6]

5.

a) Given an Elliptic curve E: $y^2 = x^3 + 2x + 2 \bmod 17$ and point P= (5, 1) and Q= (7, 6). Compute 7P and P+Q. [10]

b) Write a detailed note on Digital signatures. [4]

OR

c) What is meant by message digest? [4]

d) Define different criteria of cryptographic hash function. [4]

e) Explain authentication function in detail. [6]