Total number of printed pages–3

53 (CS 717) CRNS

2017

CRYPTOGRAPHY AND NETWORK SECURITY

Paper : CS 717

Full Marks : 100

Time : Three hours

The figures in the margin indicate full marks for the questions.

*Answer **any five** questions.*

1. Answer the following : ***(any four)*** 5×4

   (a) Define cipher and ciphertext in cryptography.

   (b) What do you mean by cryptanalysis ? What is its importance ?

   (c) What do you mean by public-key and private-key cryptography ?

   (d) Write a short note on Message Authentication Code.

   (e) Write a short note on brute force attack.

Contd.

2. *(a)* Describe Hill cipher algorithm.

(b) Consider a Hill cipher m=3 (block size=3) with key K shown below

$$K = \begin{pmatrix} 25 & 3 & 7 \\ 5 & 9 & 21 \\ 11 & 8 & 13 \end{pmatrix}$$

(i) What is ciphertext corresponding to the plaintext "VOW" ?

(ii) What is the plaintext corresponding to the ciphertext "TQX" ? 10+10

3. *(a)* What are the drawback of double DES ? How do you overcome the above drawback in triple DES ?

(b) Give the description of AES. 10+10

4. *(a)* Describe the RSA algorithm.

(b) Perform the encryption and decryption using the RSA algorithm, where p=3, q=11, e=7 and M= 5. Also identify the public key and private key. 8+12

5. *(a)* What is trapdoor one-way function? How this concept use in cryptography?

   (b) Define the Euler's phi function and hence find the value of $\phi(12)$.

   (c) Describe an efficient algorithm to check the primeness. 5+10+5

6. *(a)* Describe the ElGamal encryption and decryption system.

   (b) Describe Diffie-Hellman key exchange algorithm. 10+10

7. Write short notes on the following: ***(any four)*** 5×4

   (a) Hash function in cryptography

   (b) Digital signature

   (c) Firewall

   (d) Discrete logarithmic problem

   (e) Frequency analysis in cryptography.