**53 (CS 717) CANS**

**2016**

# 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. Write the short notes on : ***(any five)*** 5×4

   *(a)* Brute force attack

   *(b)* Monoalphabetic and polyalphabetic cipher

   *(c)* Playfair cipher. Is it substitution cipher ?

   *(d)* Message Authentication Code (MAC)

   *(e)* Diffusion and Confusion.

(f) Digital signature

(g) Firewall.

2. Explain hill cipher. Encrypt the message "we are final year cs student" using the hill cipher with key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$.

Explain how frequency analysis helps in cryptanalysis. 5+10+5

3. Describe in details the DES cipher algorithm (with diagram/flow chart representation). Describe Meet-in-the-middle attack in DES. How to solve it ? 10+5+5

4. Describe the AES (or IDEA) cipher algorithm. (with diagram/flow chart representation) Describe the strength and key space of the algorithm. 15+5

5. What is trapdoor-one-way function ? How this concept use in cryptography ? Define Euler's phi (totient) function and hence find the value of $\varphi(12)$. Describe an efficient algorithm to check the primeness of a number. 5+5+5+5

6. Describe the RSA algorithm. Perform the encryption and decryption using the RSA algorithm, where $p=5$, $q=11$, $e=3$ and $M=9$. Also identify the public key and private key.

6+12+2

7. What is the hash function (use in cryptography) ? What are the properties of this hash function ? What do you mean by message authentication ? How hash function use in message authentication ?

5+5+5+5