Total No. of Questions : 5] *[Total No. of Printed Pages :2*

Roll No......................................

IT - 801

B.E. VIII Semester

Examination, June 2016

Information Security

Time : Three Hours

Maximum Marks : 70

Note: i) Answer five questions. In each question part A, B, C is compulsory and D part has internal choice.

ii) All parts of each questions are to be attempted at one place.

iii) All questions carry equal marks, out of which part A and B (Max.50 words) carry 2 marks, part C (Max.100 words) carry 3 marks, part D (Max.400 words) carry 7 marks.

iv) Except numericals, Derivation, Design and Drawing etc.

1. a) Write any two difference between diffusion and confusion.

b) What is the purpose of the S-boxes in DES?

c) Explain the avalanche effect.

d) Define play fair cipher and polyalphabetic cipher with suitable example.

OR

Encrypt the message "Cryptography" using the hill cipher with key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show your calculation.

2. a) What is Euler's totient?

b) What are three broad categories of application of public key cryptosystems?

c) Explain factoring problem in RSA.

d) Users A and B use the Diffie-Hellman key exchange technique a common prime q = 71 and a primitive root α = 7

i) If user a has private key $X_A = 5$ what is A's public key Y_A?

ii) If user B has private key $X_B = 12$, what is B's public key Y_A?

OR

Explain elliptic curve cryptography with suitable example.

3. a) In the context of kerberos, What is realm?

b) Write any two difference between kerberos 4 and kerberos 5?

c) What is chain of certificate?

d) Explain secure socket layer and transport layer security.

OR

Discuss IP security in detail.

4. a) List different type of phishing attack.

b) List different types of viruses.

c) Differentiate between viruses and worms.

d) Define following term:

i) Format string

ii) SQC injection attack

OR

Define E-mail security in detail. Why E-mail security is important?

5. a) Why access control is more important in security?

b) Define uniform resource locator.

c) Write difference between HTTP and HTTPS.

d) What is firewall? List the type of firewalls and explain. Draw a schematic diagram of a packet filtering router used as a firewalls.

OR

Write a short notes

i) Encrypted tunnel

ii) IDS

******