No. of Printed Pages : **2**

Sl. No.

C8-R4 : INFORMATION SECURITY

NOTE :

1. **Answer question 1 and any FOUR questions from 2 to 7.**
2. **Parts of the same question should be answered together and in the same sequence.**

Total Time : 3 Hours **Total Marks : 100**

1. (a) Explain cryptanalysis. Discuss any one technique for it.

(b) What is digital signature ? Explain its use with the help of an example.

(c) Explain limitation of DES in detail.

(d) Write short note on Kerberos.

(e) What is elliptic curve cryptography ?

(f) How can we achieve web security ?

(g) Explain various key management techniques. **(7x4)**

2. (a) Explain RSA algorithm.

(b) Compare block ciphers with stream ciphers

(c) What are the types of security attacks ?

(d) In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6, what is the secret key they exchanged ? **(4+4+5+5)**

3. (a) What are the limitations of firewalls ?

(b) Write a short note on Pretty Good Privacy.

(c) Explain DES algorithm with suitable examples. Discuss its advantages and limitations.

(d) In an RSA cryptosystem, a participant A uses two prime numbers p = 13 and q = 17 to generate her public and private keys. If the public key of A is 35, then find the private key of A . **(4+4+5+5)**

4. (a) What are the advantages of steganography comparing with cryptography ?

(b) List three approaches to message authentication.

(c) What is the remainder when 13^{18} is divided by 19 ? Explain the AES algorithm.

(d) What is password management ? **(4+4+5+5)**

5. (a) What are the different approaches to public key management ?

(b) Explain how S/MIME is better than MIME.

(c) What is the remainder of $19^{2200002}/23$?

(d) How does MD5 work ? **(4+4+5+5)**

6. (a) Explain the AES algorithm.

(b) Describe in detail about Conventional Encryption Model.

(c) Find all solutions of $x^2 \equiv 1 \pmod{144}$ (Using Chinese remainder theorem). **(6+6+6)**

7. (a) Describe the categories and operating models of Intrusion Detection Systems (IDS) in detail.

(b) What is a buffer overflow ? How is it used against a web server ? Explain. **(9+9)**

- o O o -