No. of Printed Pages : **1**

Sl. No.

C8-R4 : INFORMATION SECURITY

NOTE :

1. Answer question 1 and any FOUR from questions 2 to 7.

2. Parts of the same question should be answered together and in the same sequence.

Time: 3 Hours | Total Marks: 100

1. (a) Explain the basic symmetric encryption model.

(b) Describe blum blum shub generator.

(c) What is the difference between public and private key cryptosystems?

(d) What is a hash function? List its applications.

(e) For Encoding rule, A=0, B=1…Z=25,(Consider Key string gold). Encrypt the following using vigenere cypher :

proceed meeting as agreed.

(f) How does password based authentication works?

(g) Explain SHA-256/384/512 hash functions. **(7x4)**

2. (a) What is Euler's totient function? Explain using Euler's theorem.

(b) What is birthday paradox? How it can be exploited in a collision resistant attack? **(10+8)**

3. (a) What is a digital signature? How it works? What are the possible attacks and forgeries that can attack a signature?

(b) Explain Chinese Remainder Theorem. **(8+10)**

4. (a) Explain Cipher Block Chaining (CBC) operation mode. Can CBC ensure integrity? Why or Why not?

(b) What is the meet-in-the-middle attack? **(10+8)**

5. (a) Factor number 105 by Trial Division method.

(b) Using Extended Euclid's algorithm, find multiplicative inverse of 550 and 1769.

(c) Explain the shift row transformation for AES. **(7+4+7)**

6. (a) How a challenge response system is implemented using symmetric key cipher?

(b) How does symmetric key distribution takes place when two nodes, A and B have an encrypted link to a common node C? **(8+10)**

7. (a) Explain station-to-station protocol.

(b) What are the attacks suffered by the authentication protocols? Explain in detail attack on RSA and attacks on ElGamal. **(8+10)**

- o 0 o -