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) State the primary elements of a public-key cryptosystem.

(b) How does man-in-the-middle attack work in Diffie-Hellman ? Explain with a suitable scenario.

(c) What are the common testing for primality in practice ? Briefly explain any one of them.

(d) What are the basic arithmetical as well as logical functions used in SHA ?

(e) Cite the difference between the AES decryption algorithm and equivalent inverse cipher.

(f) Compare a monoalphabetic cipher with a polyalphabetic cipher with the help of a suitable example.

(g) Consider field 'F', mathematically prove that its only ideals are (0) and F itself. **(7x4)**

2. (a) Assume that the equation $abc=1$ holds in a group G. Does it follow that $bca=1$? That $bac=1$? Justify your answer.

(b) Consider a ring R, if every $x \in$ R satisfies $x^2=x$, then prove mathematically that R must be commutative.

(c) Demonstrate mathematically that there are infinitely many primes of the form $6n-1$. Explain with a suitable example. **(6+6+6)**

3. (a) Explain substitution cipher along with its mathematical representation. Decrypt the message GZD KNK YDX MFW JXA if it was encrypted using a shift cipher with shift of 5.

(b) What is a Discrete logarithm problem ? Evaluate the tradeoff between Security and efficiency in cryptographic protocols based on this problem. **(9+9)**

4. (a) With the help of a suitable example explain the working of RC4 stream cipher.

(b) What are AES and Triple-DES algorithms ? Differentiate between DES and Triple-DES based on several characteristics such as number of rounds, algorithm type, security and block size, etc. **(9+9)**

5. (a) What is a Birthday attack ? Explain the Birthday Paradox Problem mathematically.

(b) What are the fundamental principles underlaying the Blum-Blum-Shub pseudo-random number generator and how it differs from other pseudo-random number generation algorithms ? **(12+6)**

6. (a) State the requirements that a public key cryptosystem must fulfill to be considered as a secure algorithm.

(b) Write the steps for the RSA algorithm : Key generation, Encryption/Decryption function

(c) Consider that Charlie has a set of blocks that have been encoded with the RSA algorithm and he does not have the private key. Assume that n = pq and e is the public key. Assume a scenario when his friend David tells him that he knows one of the plain text blocks which has a common factor with n. Does this help Charlie in any way ? **(6+6+6)**

7. (a) State the properties of a digital signature. List the requirements that a digital signature scheme must satisfy. Differentiate between a direct and an arbitrated digital signature.

(b) Cite examples of replay attacks and list three general approaches to deal with them. **(9+9)**

- o O o -