No. of Printed Pages : **2**

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) Show that permutation operation over 3-bit binary is group.

(b) Give the characteristics of Hill Cipher.

(c) Apply the statistical attack over cipher text "Yljhqèuh flskhu lv wkh vhtxhqfh ri Fdhvdu flskhuv" and find the key value used for encryption using ceaser cipher.

(d) Compute 21^{-1} mod 103 using extended Euclidian algorithm.

(e) Explain the Euler's totient function using suitable example.

(f) Explain the point doubling and point addition in elliptic curve cryptography.

(g) How does RC4 Stream Cipher key generation work ? **(7x4)**

2. (a) The Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of electronic data. Explain working of round key generation in DES.

(b) Find the multiplication of $(x^6+x^4+x+1) \otimes (x^7+x^6+x^3+x)$ in GF(2^8) using irreducible polynomial $m(x)=x^8+x^4+x^3+x+1$.

(c) Apply the Chinese Remainder Theorem (CRT) for $x=5$ mod 10, $x=4$ mod 9 and $x=3$ mod 8 and find the value of x. **(6+5+7)**

3. (a) What is secret sharing scheme ? Explain working of Shamir's secret sharing protocol using suitable example.

(b) Compute the index of coincidence for "Counting the frequency of letters is an important part of the cryptanalysis". **(9+9)**

4. (a) Explain the following terms :

1. Quadratic residue

2. Primitive element in the group

3. Order of Group

4. Order of the element in the group

(b) What is factorization and discrete logarithm problem ? How factorization problem makes RSA more secure ? Prove the correctness of RSA decryption.

(c) List and explain the fields of X.509 digital certificate standard. **(4+6+8)**

5. (a) Consider the parameters $p = 283$, $q = 47$, $g = 60$ and public key, $B = 216$. Show working of encryption and decryption using ElGamal cryptosystem.

(b) Explain Digital Signature Standard (DSS).

(c) Compute 11^{13} mod 53-using fast exponentiation computation method. **(6+4+8)**

6. (a) Differentiate the SHA1 and MD5 algorithm.

(b) List and explain the PRNG Requirements. Explain working of Blum Blum Shub Generator using suitable example.

(c) Find the factors of 6994241 using Pollard p–1 factorization method (Take Bias $B = 8$). **(4+6+8)**

7. (a) Explain Electronic Code Book (ECB) Mode of block cipher.

(b) Demonstrate the Diffie-Hellman key exchange using $p = 11$, $g = 2$, $x_A = 9$, $x_B = 4$.

(c) Solve $3^x = 5$ mod 7 using Shank's Baby step Giant Step algorithm. **(5+5+8)**

- o 0 o -