

**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) What are the difference between Active and Passive attack ? Explain with suitable example.
- (b) How many keys are required for 40 people to communicate in symmetric Cryptography and asymmetric Cryptography ?
- (c) What do you mean by HILL Cipher ? By using HILL cipher technique encrypt the message "HELP" with the help of key  $K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$ . Explain decryption process.
- (d) How can we provide authentication and confidentiality using public key cryptography ? Explain with suitable block diagram.
- (e) Encrypt the message using Play fair cipher "Why don't you" and encryption key "KEYWORD".
- (f) Compute  $3^{201} \bmod 11$ . What is the minimum number of the multiplication required for this number ?
- (g) What is the purpose of the S-boxes in DES ? (7x4)
2. (a) User Alice and Bob use Diffie - Hellman Key exchange technique with common prime  $q=71$  and primitive root  $\alpha=7$ .
  - (i) If alice has Private Key  $X_A=5$ , What is alice Public Key  $Y_A$  ?
  - (ii) If Bob has Private Key  $X_B=12$ , What is alice Public Key  $Y_B$  ? What is shared secret key ?
- (b) What is message authentication code ? Explain with suitable example.
- (c) What is the difference between statistical randomness and unpredictability ? Explain Blum Blum Shub Generator algorithm. (6+9+3)
3. (a) Explain Fiestal Cipher with Block diagram.
- (b) What is Birthday attack ? Explain with example. (9+9)
4. (a) Name the types of mode of operation in block cipher and explain Cipher Block Chaining (CBC).
- (b) Use Chinese Remainder Theorem to Solve  $x$ .  
 Given :  $P1 : x=3 \pmod{4}$   
 $P2 : x=2 \pmod{3}$   
 $P3 : x=4 \pmod{5}$
- (c) Determine  $1234^{-1} \bmod 4321$  using extended Euclidean algorithm. (7+7+4)

5. (a) Given  $p=17$ ,  $q=11$  and message  $M=88$ , use RSA algorithm to find cipher text. Also verify your answer.
- (b) Explain all steps of SHA-512 logic (Secure Hash Algorithm) with message digest generation diagram. (8+10)
6. (a) Differentiate between Stream Ciphers and Block Ciphers.
- (b) Using RC4 algorithm encrypt the following plaintext :
- $P = [ 1 2 2 2 ], \text{key} = [ 1 3 ], S = [ 1 2 3 4 ]$
- (c) Explain Miller-Rabin Algorithm for testing of Primality of number with suitable example. (4+8+6)
7. (a) What is the need of Digital Signatures ? What is the difference between direct and arbitrated digital signature ? Explain Digital signature algorithm (DSA).
- (b) Explain the problems with key management and how it affects symmetric cryptography. (9+9)

- o O o -