**53 (IT 811) CGNS**

**2019**

# CRYPTOGRAPHY AND NETWORK SECURITY

Paper : IT 811

*Full Marks : 100*

Time : Three hours

***The figures in the margin indicate full marks for the questions.***

*Answer* ***any five*** *questions.*

1. *(a)* Differentiate between SECRET KEY versus PUBLIC KEY Cryptography. 2

*(b)* Consider a hill cipher $m$=2 (block size = 2) with key $K$ shown below :

$$K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$$

(i) What is the ciphertext corresponding to the plaintext: (HELP)?

(ii) What is the plaintext corresponding to the ciphertext: (HIAT)? 6+8=14

(c) What are the principal elements of a Public key cryptosystem? 4

2. (a) Discuss security services in Cryptography. 10

(b) With a clear diagram, discuss S-DES key generation with the help a 10-bit key *(K)* = (10100 00010). 10

3. (a) Explain RSA. 2

(b) Perform encryption and decryption using RSA algorithm for the following parameters:

$p=3$, $q=11$, ciphertext $(C)=7$ and plaintext $(M)=5$. 5+5=10

(c) In a public key system using RSA, you intercept the ciphertext $C=10$ sent to a user whose public key is $e=5$, $n=35$. What is the plaintext $M$? 8



4. (a) Discuss Euclid's Algorithm. Use Euclid's algorithm to find *gcd* (1970, 1066). 3+7=10

(b) Define Singular Elliptic Curve. How Elliptic Curve is symmetric? 2+2=4

(c) Define the Euler's phi function and hence find the value of $\phi(240)$. 3+3=6

5. (a) Discuss the various categories of traditional cipher in details. 15

(b) What is Digital Signature and how it works? 5

6. (a) What is Digital Signature? Describe a scheme to produce Digital Signature. 3+7=10

(b) Solve the modular arithmetic: 1×4=4

(i) 27 *mod* 5

(ii) −18 *mod* 14

(iii) −7 *mod* 10

(iv) 1/11 *mod* 26

(c) Do each of the following inverses exist? If yes, what are they? If no, explain why not. 3+3=6

(i) $102^{-1} (mod\ 411)$

(ii) $77^{-1} (mod\ 411)$

7. Write short notes on the following: ***(any five)*** 5×4=20

(a) Authentication and Authorization

(b) Active attacks and Passive attacks

(c) S/MIME IP security

(d) IPSec services

(e) Firewall

(f) Stream & Block Ciphers.