M.Tech 1st Semester Cyber Forensics and Information Security Examination, December–2017

MATHEMATICAL FOUNDATIONS OF INFORMATION SECURITY

Paper-MTCF-101

Time allowed : 3 hours] *[Maximum marks : 100*

Note : *Attempt **five** questions in total, selecting **one** question from each section & **Question No. 1 which is compulsory.** All questions carry equal marks.*

1. Write a note on following : 5×4=20

(a) Applications of factoring

(b) Primality Test

(c) Enciphering Matrices

(d) Elgamal Encryption.

Section–A

2. State and prove Fermat's Little theorem. Also list the Applications of Chinese Remainder Theorem. 20

3. Write a note on Euler's phi function. Also define Jacobi Symbol. Also find square root of a = 186 modulo p=401. 20

Section–B

4. Explain DES Algorithm in detail by using suitable diagram and examples. Also explain double DES and Triple DES. 20

5. Write a note on following : 20
   (a) Permutation cipher
   (b) Hill cipher

Section–C

6. Explain RSA public-key Encryption Algorithm. Also describe and explain key generation Algorithm with the help of suitable example. 20

7. What do you mean by Knapsack problem ? Explain in detail any one method to solve knapsack problem. 20

Section–D

8. Describe and explain Pollard's 'Rho method' in detail by taking suitable example. 20

9. Write a note on following : 20
   (a) Continued fraction method
   (b) Factor base Algorithm