

[Time:2.30 Hrs]

[ Marks:75 ]

Please check whether you have got the right question paper.

- N.B:
1. All question are compulsory.
  2. Figures to the right indicate full marks.

**Q.1 Attempt any Three of the following:**

**15**

a. Explain the following term with example

- i) PRIME NUMBERS
- ii) CONGRUENCES

b. Write down the pseudocode for EUCLIDEAN ALGORITHM?

Find the greatest common divisor of 414 and 662 using EUCLIDEAN ALGORITHM?

c. First write down the rule and compute the following term

- i)  $(15 + 17) \% 7$  using the Modular Addition
- ii)  $(12 \times 13) \% 5$  using the Modular Multiplication
- iii)  $(10/3) \bmod 7$  using the Modular Division
- iv)  $A=3, m=11$  using the Modular Inverse

d. States the FERMAT'S LITTLE THEOREM?

Use the FERMAT'S LITTLE THEOREM to find the Modular Inverse of 3 modulo 7?

e. State the Euler's theorem and calculate the following,

i)	$3^6 \bmod 7$
ii)	$2^4 \bmod 5$
iii)	$4^6 \bmod 7$

f. Write down the Chinese remainder theorem and explain the following term

- i) Quadratic residue
- ii) Quadratic Reciprocity Theorem
- iii) Jacobi Symbol

**Q.2 Attempt any Three of the following:**

**15**

- a. Explain the following term,
  - i) Symmetric Key Encryption
  - ii) Asymmetric Key Encryption
- b. Define the shift cipher? Write down the encryption rule for shift cipher?  
Encrypt the HELLO using the shift key  $k=3$
- c. Write down the algorithm for substitution cipher and substitution cipher Method?  
Plain Text: I am studying Data Encryption  
Key: 4  
What is the output of Plain Text using substitution cipher?
- d. Define AFFINE CIPHER? Encrypt the plaintext: "CDOE", using the key:  $A=5$ ,  $B=3$ ,  
using Affine cipher.  
Below table show the Alphabet and their value

A	B	C	D	E	F
0	1	2	3	4	5
G	H	I	J	K	L
6	7	8	9	10	11
M	N	O	P	Q	R
12	13	14	15	16	17
S	T	U	V	W	X
18	19	20	21	22	23
Y	Z				
24	25				

- e. Define VIGENÈRE CIPHER? Write down the encryption rule and find out the ciphertext of  
below plaintext  
Plaintext: UNIVERSITYOFMUMBAI  
Keyword: CDOE
- f. Briefly describe the Data Encryption Standard Algorithm?

**Q.3 Attempt any Three of the following:**

**15**

- Explain the Legendre and Jacobi Symbols?
- Write down the advantage of MILLER-RABIN ALGORITHM? Solve the below problem, Apply Miller-Rabin Algorithm using base 2 to test whether the number 341 is composite or not?
- Explain the attack on RSA?
- Explain the DIFFIE-HELLMAN KEY AGREEMENT?
- Describe the ELGAMAL CRYPTOSYSTEM?
- Explain the ELLIPTIC CURVES CRYPTOGRAPHY?

**Q.4 Attempt any Three of the following:**

**15**

- Write note on KEY DISTRIBUTION PATTERNS?
- Write down the PKIX Services?
- Describe the working of Public-Key Infrastructure?
- Define the secure socket layer and explain the Handshake protocol and Record protocol?
- What are the step involved in CERTIFICATE LIFE CYCLE?
- What is Trust Model? Write a short note on following term,
  - Hierarchical Trust Model
  - Bridge Trust Model
  - Hybrid Trust Model
  - Mesh Trust Model

**Q.5 Attempt any Three of the following:**

**15**

- Write down the difference Between AES and DES Algorithms?
- What are the application of hash functions?
- Explain the RABIN CRYPTOSYSTEM?
- Briefly describe the KNAPSACK PROBLEM?
- Briefly describe the STATION-TO-STATION PROTOCOL?
- What is Pretty Good Privacy? Describe its working?

\*\*\*\*\*