DHARMSINH DESAI UNIVERSITY, NADIAD
FACULTY OF TECHNOLOGY
B.TECH. SEMESTER VI [CE]
SUBJECT: (CE-618) NETWORK & INFORMATION SECURITY

Examination	**: First Sessional**	**Seat No**	**: ______________**
Date	**: 07/01/2022**	**Day**	**: Friday**
Time	**: 11:00 AM to 12:15 PM**	**Max. Marks**	**: 36**

INSTRUCTIONS:

1. Figures to the right indicate maximum marks for that question.
2. The symbols used carry their usual meanings.
3. Assume suitable data, if required & mention them clearly.
4. Draw neat sketches wherever necessary.

Q.1 Do as directed.

(a) Add and Multiply two numbers in $Z_{19.}$ Numbers are (-321) and 11. **[2]**

(b) Write definition of Index of Coincidence (IC). What is the use of IC method? **[2]**

(c) Find the multiplicative inverse of 23 in Z_{100}. Apply extended euclidian algorithm. **[2]**

(d) Compute Φ (1215). Clearly specify the rules for the computation. **[2]**

(e) Using Fermat's Theorem find 5^{301} mod 11. Show necessary steps of computation. **[2]**

(f) Does 271 Pass the Miller-Rabin Test? Show every step of Computation. **[2]**

Q.2 Attempt ***Any Two*** from the following questions.

(a) Apply Vigenere cipher encryption algorithm for the Plain text "she is listening" with key=MOBILE. Show all the necessary steps. **[6]**

(b) To perform cryptanalysis of affine cipher using chosen-plaintext attack, Eve very briefly obtains access to Alice's computer and has only enough time to type a two-letter plaintext "et". She then tries to encrypt the short plaintext and gets the following result. Cipher text of "et" = "WF". **[6]**
Find out keys used in affine cipher using above information and decrypt the cipher text "REFOCR".

(c) Apply Playfair cipher to encrypt the following text using "COMPUTER" as key. **[6]**
(i) hello (ii) indiax Show all the necessary steps.

Q.3 (a) Alice and Bob want to communicate using RSA algorithm. Alice has selected two prime numbers p=29 and q=37. Alice has selected e=31. Check whether e is valid or not according to RSA? Calculate pair of keys (public and private) on behalf of Alice. Alice sends a message M=28 after doing encryption using private key. Decrypt the answer of encryption using public key of Alice. Show all the necessary steps. **[6]**

(b) Consider the following Super-increasing tuple A'= {7 11 23 43 87 173 357}. Assume Modulus M=1001 and random integer W=41. Encrypt letter 'a' using Knapsack cryptosystem. Decrypt cipher text and show that you are getting the plain text letter 'a' back. **[6]**

OR

Q.3 (a) Alice and Bob want to communicate using RSA algorithm. Alice has selected two prime numbers p=157 and q=167. Alice has selected e=19. Check whether e is valid or not according to RSA? Calculate pair of keys (public and private) on behalf of Bob. Alice sends a message M=3 after doing encryption using public key of Bob. Decrypt the answer of encryption using private key of Bob. Show all the necessary steps. **[6]**

(b) Find the value of ‘x’ for the following set of congruent equations using Chinese remainder Theorem. **[6]**

$$x \equiv 3 \pmod{5}$$
$$x \equiv 6 \pmod{7}$$
$$x \equiv 4 \pmod{11}$$

Show all the necessary steps.