PVP 19

Code: 19BS1403

II B.Tech - II Semester – Regular Examinations – AUGUST 2021

ENGINEERING MATHEMATICS – IV
(Number Theory and Cryptography)
(Common to CSE, IT)

Duration: 3 hours Max. Marks: 70

Note: 1. This question paper contains two Parts A and B.
2. Part-A contains 5 short answer questions. Each Question carries 2 Marks.
3. Part-B contains 5 essay questions with an internal choice from each unit. Each question carries 12 marks.
4. All parts of Question paper must be answered in one place

PART – A

1. a) Explain prime factorization with example.

b) Define the terms Cryptography and Cryptanalysis

c) Illustrate the difference between Diffusion and confusion.

d) Compare Conventional encryption and Public-Key Encryption.

e) How MAC is different from hash function?

PART – B
UNIT – I

2.	a)	State Fermat's theorem and solve 7^{2019} mod 13.	6 M
	b)	Explain Miller Rabin Algorithm with example.	6 M

OR

3.	a)	State Euler's Theorem. Solve 4^{99} mod 35 by using Euler's Theorem.	6 M
	b)	Solve GCD(1970,1066) using Euclid's algorithm	6 M

UNIT – II

4. a) Explain Symmetric Cipher Model with neat sketch. 6 M

b) Apply play fair cipher method to Encrypt the word "Semester Result" with keyword "Examination". 6 M

OR

5. a) Explain in detail about any Two Transposition Ciphers. 6 M

b) Develop Cipher text of the given text "Andhra Pradesh" using rail fence technique. 6 M

UNIT-III

6. a) Draw the general structure of DES and explain how encryption and decryption are carried out. 6 M

b) Why is it important to study the Fiestel cipher structure and explain the mathematical description of each round in the Fiestel structure. 6 M

OR

7. a) Explain the substitution bytes transformation and add round key transformation of AES cipher. 6 M

b) Illustrate any two modes of operation in Stream cipher. 6 M

UNIT – IV

8. a) Explain RSA Algorithm. 6 M

b) Demonstrate the encryption and decryption for the RSA algorithm parameters. P=3, Q=11, E=7, M=5 6 M

OR

9. a) Discuss briefly about Diffie-Hellman key exchange algorithm with its pros and cons. 6 M

b) With a neat diagram, differentiate and describe in detail the encryption and authentication in public key cryptography. 6 M

UNIT – V

10. a) Demonstrate any two simple hash functions with examples. 6 M

b) Write about Message Authentication Functions with examples. 6 M

OR

11. a) What is MAC? Explain various situations in which a message authentication code is used. 6 M

b) Describe HMAC Algorithm. 6 M