17TE71 USN OF Seventh Semester B.E. Degree Examination, July/August 2021 Cryptography and Network Security Max. Marks: 100

Note: Answer any FIVE full questions.

- Explain the Euclid's algorithm for determining the GCD of two positive integers. Find the GCD of (1970, 1066) using Euclid's algorithm. (10 Marks)
  - b. Briefly explain the following with examples:
    - i) play fair
    - ii)  $(2 \times 2)$  Hill ciphers.

(10 Marks)

Define modular arithmetic operation with necessary properties and prove the same.

(10 Marks)

- Describe simple XOR and one time pad encryption techniques with an example and its difficulties. (10 Marks)
- Illustrate the following with necessary diagrams:
  - Feistel encryption and decryption process
  - ii) Single DES encryption. (12 Marks)
  - Explain the process of AES encryption with necessary diagram

(08 Marks)

- Briefly explain RSA algorithm with example. (06 Marks)
  - Illustrate the diffie Hellman key exchange algorithm with example. b.
  - With the help of neat diagram, explain elliptic curve Arithmetic and Rules.

(06 Marks)

- (08 Marks)
- Differentiate between MD4 and MD5 algorithm.

(06 Marks)

Outline N-Hash algorithm with neat diagram.

(06 Marks) (08 Marks)

Explain discrete logarithmic signature scheme.

- With the neat diagram, explain the operation of Secure Hash Algorithm (SHA). (08 Marks)
  - Explain DSA algorithm with necessary diagram and required example. (12 Marks)
- With necessary diagram, explain the SSH protocol stack layers. 7 a.

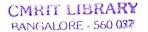
(07 Marks)

Explain SSL protocol stack with session state and connection status parameters.

(07 Marks)

With neat flow diagram, explain IEEE802.11i phases of operation.

(06 Marks)



## 17TE71

- 8 a. Explain SSH transport layer protocol packets exchange and packet formation with required diagram. (08 Marks)
  - b. Explain all the services and protocols of IEEE 802.11i WLAN with necessary diagram.

(12 Marks)

- 9 a. Explain PGP cryptographic functions with relevant diagram. (10 Marks)

  b. Explain the concept of combining security associations internet key exchange with
  - b. Explain the concept of combining security associations internet key exchange with necessary diagrams. (10 Marks)
- 10 a. Describe the cryptographic algorithm used in S/MIME. (08 Marks)
  - b. With relevant diagram, explain all the fields involved in ESP packet. (06 Marks)
  - c. With neat diagram, explain typical scenario of IP security with its applications. (06 Marks)