

CBCS SCHEME

17TE71

USN

--	--	--	--	--	--	--	--	--	--



Seventh Semester B.E. Degree Examination, July/August 2021 Cryptography and Network Security

Time: 3 hrs.

Max. Marks: 100

Note: Answer any FIVE full questions.

- 1 a. 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) (2×2) Hill ciphers. (10 Marks)
- 2 a. Define modular arithmetic operation with necessary properties and prove the same. (10 Marks)
b. Describe simple XOR and one time pad encryption techniques with an example and its difficulties. (10 Marks)
- 3 a. Illustrate the following with necessary diagrams :
i) Feistel encryption and decryption process
ii) Single DES encryption. (12 Marks)
b. Explain the process of AES encryption with necessary diagram. (08 Marks)
- 4 a. Briefly explain RSA algorithm with example. (06 Marks)
b. Illustrate the diffie – Hellman key exchange algorithm with example. (06 Marks)
c. With the help of neat diagram, explain elliptic curve Arithmetic and Rules. (08 Marks)
- 5 a. Differentiate between MD4 and MD5 algorithm. (06 Marks)
b. Outline N-Hash algorithm with neat diagram. (06 Marks)
c. Explain discrete logarithmic signature scheme. (08 Marks)
- 6 a. With the neat diagram, explain the operation of Secure Hash Algorithm (SHA). (08 Marks)
b. Explain DSA algorithm with necessary diagram and required example. (12 Marks)
- 7 a. With necessary diagram, explain the SSH protocol stack layers. (07 Marks)
b. Explain SSL protocol stack with session state and connection status parameters. (07 Marks)
c. With neat flow diagram, explain IEEE802.11i phases of operation. (06 Marks)

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, $42+8 = 50$, will be treated as malpractice.

- 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 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)
