Sub Code: BCST-802/BITT-802/BCST-803(F) **ROLL NO……..……..**

VIIIth SEMESTER EXAMINATION, 2022 – 23

IVth Year, B.Tech. – Computer Science & Engineering/Information Technology

Cryptography and Network Security

Duration: 3:00 hrs **Max Marks: 100**

Note: - Attempt all questions. All Questions carry equal marks. In case of any ambiguity or missing data, the same may be assumed and state the assumption made in the answer.

Q 1.	Answer any four parts of the following. a) What is the OSI security architecture? Explain. b) Describe RSA algorithm. Illustrate the security issues in RSA algorithm. c) Describe how Diffie-Hellman algorithm is used to exchange secret key between two parties. Explain the algorithm. d) Describe the birthday attack against any hash function, give the mathematical basic of the attack. e) What is Schnorr digital signature scheme? How a user generates a signature with the help of private key and public key? f) What are firewalls? What are different types of firewalls? Explain.	5x4=20
Q 2.	Answer any four parts of the following. a) What is difference between a monoalphabetic cipher and a polyalphabetic cipher? b) List and briefly define types of cryptanalytic attacks based on what is known to the attacker. c) State the requirements for hash functions. d) What is Elliptic Curve Cryptography? Also differentiate between Elliptic Curve Cryptography and RSA. e) How does PGP provide authentication and confidentiality for email services and for file transfer applications? f) Explain ESP packet format. Why does ESP include a padding field?	5x4=20
Q 3.	Answer any two parts of the following. a) What is DES? Explain. Also explain difference between double DES and triple DES. b) Explain the general format of a certificate using X.509. How is an X.509 certificate revoked? c) Explain IP Security architecture. What are the roles of the Oakley key determination protocol and ISAKMP in IPsec?	10x2= 20
Q 4.	Answer any two parts of the following. a) State and prove Fermat's theorem. Also determine the value of 3^{2005} mod 500. b) What are the types of attacks addressed by message authentication? What are two levels of functionality that comprise a message authentication or digital signature mechanism? c) Analyze the Cryptographic algorithms used in S/MIME. Explain S/MIME certification processing.	10x2= 20
Q 5.	Answer any two parts of the following. a) Explain SHA-1 algorithm in detail. Why SHA-1 is more secure than MD5? b) Describe and illustrate the Chinese Remainder theorem. c) What is Secure Electronic Transaction? Illustrate the working of Secure Electronic Transaction (SET) in detail.	10x2= 20

****