Roll No.: ……

SGT UNIVERSITY

END TERM THEORY EXAMINATION JULY-2022

Faculty/College of Study:	**Engineering & Technology**	**Year/Semester:**	**6th Semester**
Program:	**B.Tech. (CSE) Gen./Apple/IBM/MLAI)**	**Duration:**	**03:00 Hrs.**
Course/Subject:	**Cryptography & Network Security**	**Maximum Marks:**	**60**
Course/Subject Code:	**13020610**	**Batch:**	**2019**

Instructions:-

1. Write Your Roll No. on the Question Paper.
2. Candidate should ensure that they have been provided correct question paper. Complaint(s) in this regard, if any should be made within 15 minutes of the commencement of the exam. No complaint(s) will be entertained thereafter.
3. All Questions are compulsory. Marks are indicated against each question.
4. Illustrate your answer with diagram wherever required.

SECTION-A

(Very Short Answer Type Questions)

Note: All Questions are compulsory: - [12X1=12 Marks]

S. No.	Question	Marks Allotted
1	A PRG is a deterministic algorithm. Is the above statement being correct?	1
2	SSL in web security stands for	1
3	Consider an instance of shift cipher with the probability distribution over the message space as follows: P[M=a] = 0.4, P[M=b] = 0.2, P[M=c] = 0.4. What is the probability that the ciphertext is 'R'?	1
4	State the sufficient key-space principle.	1
5	In vernam cipher (also known as one time pad), whether the honest user are allowed to reuse the secret key?	1
6	What is attack complexity of vigenere cipher?	1
7	Are shift ciphers COA secure?	1
8	A scheme is KPA-secure if and only if it is CPA-secure. Is the above statement being correct?	1
9	What is basic assumption for the security of RSA encryption algorithm?	1
10	What are the conditions that must be satisfied by the encryption scheme to become perfectly secure encryption scheme?	1
11	Stateful variant of Counter mode is secure where as that of OFB mode is insecure. Id the above statement being correct?	1
12	What is DDH assumption of Diffie-Hellman key exchange algorithm?	1

SECTION-B
(Short Answer Type Questions)

Note: All Questions are compulsory: - **[4X2=8 Marks]**

S. No.	Question	Marks Allotted
13	State the perfect security definition with the help of challenge response game of indistinguishability.	2
14	Write the formal security definition of semantic security.	2
15	State the two limitations of perfectly secure cipher.	2
16	Explain the Kerchkhoff's principle for secure ciphers.	2

SECTION-C
(Descriptive Answer Type Questions)

Note: All Questions are compulsory: - **[4X4=16 Marks]**

S. No.	Question	Marks Allotted
17	Explain Linear Feedback Shift Register (LFSR) with the help of diagram **OR** Explain RC4 stream cipher in detail with the help of diagram.	4
18	What is a Birthday attack? How Birthday attack can be used to find collisions in Hash functions. **OR** Discuss the Digital Signature Algorithm (DSA) in detail.	4
19	Discuss in detail the confusion and diffusion paradigm. **OR** Discuss the Substitution Permutation Network (SPN) and the desirable properties of SPN.	4
20	For every encryption scheme that is perfectly secure if it holds that for every distribution over the message space $\mathcal{M}$, every m,$m_0 \in \mathcal{M}$, and every c $\in C$: $Pr[C = c \mid M = m_0] = Pr[C = c \mid M = m_1]$ Then, prove that $Pr[M = m \mid C = c] = Pr[M = m]$ **OR** Prove that Vigenere cipher is not perfectly secure.	4

SECTION-D
(Long Answer Type Questions)

Note: All Questions are compulsory: - **[4X6=24 Marks]**

S. No.	Question	Marks Allotted
21	Discuss in detail various Block-cipher modes of operation (ECB, CBC, OFB and CTR mode) with the help of neat diagrams.	6
22	Explain in detail Diffie-Hellman key exchange algorithm with the help of neat diagram.	6
23	With the help of neat diagram explain DES encryption algorithm. Also, discuss the pitfalls of DES algorithm. **OR** Explain the algorithm of AES in detail with necessary diagrams.	6
24	For p = 11 and q = 3 and choose e=3. Apply RSA algorithm where Plain text message=14 and thus find the Cipher text. Also Apply RSA algorithm for decryption of cipher text and thus find the plain text. **OR** Discuss in detail the El Gamal encryption scheme and prove its security in COA model. Also, discuss the implementation issues of El Gamal encryption scheme.	6