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**	**Duration:**	**03:00 Hrs**
Course/Subject:	**Web Security**	**Maximum Marks:**	**60**
Course/Subject Code:	**13020669**	**Batch:**	**2018**

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	SSL in web security stands for	1
2	What is Trojan Horse?	1
3	DOS stands for	1
4	AES is symmetric encryption scheme. Is above statement being correct?	1
5	DES is symmetric cryptography stands for	1
6	What are substitution techniques?	1
7	Difference between cryptography and steganography.	1
8	VPN stands for	1
9	What is basic assumption for the security of RSA encryption algorithm?	1
10	What is non-repudiation.	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	Differentiate between IDS and IPS.	2
14	State the difference between virus and worm	2
15	State the difference between symmetric and asymmetric cryptography.	2
16	State the difference between Trojan horse and virus.	2

SECTION-C
(Descriptive Answer Type Questions)

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

S. No.	Question	Marks Allotted
17	What is a Firewall and why is it used?	4
18	What is a Birthday attack? How Birthday attack can be used to find collisions in Hash functions.	4
19	Discuss the Digital Signature Algorithm (DSA) in detail.	4
20	Explain DDOS attack and how to prevent it?	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.	6