T.E. CIT) (Sem-VI) (CBSGS) Date-10/12/19

Paper / Subject Code: 37303 / SYSTEM AND WEB SECURITY

TIME: 3 Hours **Marks: 80**

Note: Question Number 1 is Compulsory
Attempt any three Questions from Question number 2 to 6.
Assume Suitable Data if Necessary.

Q1.a.	Compare and Contrast Handshake Protocol in SSL and TLS.	5
	b. Explain any types of Cryptanalytic Attacks.	5
	c. Define Kerberos and name its Server. Briefly explain the duties of each server.	5
	d. Distinguish between diffusion and Confusion.	5
Q2.a.	Explain different Authentication techniques in detail.	10
	b. Explain the RSA Cryptosystem and also Brief the Possible attacks on the RSA Cryptosystem.	10
Q3.a.	Explain Biba and Bella Padulla Model.	10
	b. Explain Buffer Overflow and Incomplete Mediation flaws in a program and how They can be used to attack the system.	10
Q4.a.	Explain the concept of Digital Signature. How it is used to preserve the security goals.	10
	b. Explain the role of IDS in securing a network. Describe different types of IDS.	10
Q5.a.	Distinguish between two modes of IPSec and Explain the security services Provided by them.	10
	b. Explain Secure Socket Layer.	10
Q6.	Write Short Notes on. (Attempt any **Four**, Each Carries 5M)	20

a. Cookies and Secure HTTP
b. SQL Injection Techniques
c. DNS Spoofing
d. Types of Firewall
e. Security Architecture of Windows System

2337C0CD50FE594F32A7EB635D11E67D