Q. Code: 966368

Reg. No.

B. E / B. TECH.DEGREE EXAMINATIONS, MAY 2023

Third Semester

CS18603 – CRYPTOGRAPHY AND NETWORK SECURITY

(Computer Science and Engineering)

(Regulation2018)

TIME: 3 HOURS **MAX. MARKS: 100**

COURSE OUTCOMES	STATEMENT	RBT LEVEL
CO 1	Understand OSI security architecture, Classical Encryption techniques and acquire fundamental knowledge on the concepts of finite fields and number theory	2
CO 2	Understand various Private and Public Key cryptographic algorithms.	3
CO 3	To learn about hash functions and digital signature algorithms.	3
CO 4	Understand about Authentication Applications and System Security.	4
CO 5	Acquire knowledge in various network security models.	3

PART- A (10x2=20Marks)

(Answer all Questions)

		CO	RBT LEVEL
1.	State alternative form of Fermat‟s theorem with example.	1	2
2.	Find the GCD of (2740, 1760) using Euclid‟s Algorithm.	1	4
3.	Illustrate about avalanche effect.	2	3
4.	Write down the purposes of the S-box in DES.	2	3
5.	List the types of functions that may be used to produce an authenticator.	3	2
6.	Compare MAC, hash practices and Digital Signature.	3	4
7.	Give the typical phases of operation of a virus or worm?	4	2
8.	Show how entities constitute a full service in Kerberos environment?	4	3
9.	List the limitations of SMTP.	5	2
10.	Differentiate transport and tunnel mode in IPsec.	5	4

PART- B (5x 14=70Marks)

		Marks	CO	RBT LEVEL
11. (a)	State Chinese Remainder Theorem and find X for the given set of congruent equations using CRT.	**(14)**	1	4

$X=1 \pmod{5}$
$X=2 \pmod{7}$
$X=3 \pmod{9}$
$X=4 \pmod{11}$

	(OR)			
(b)	Solve using Playfair cipher method. Encrypt the word "Semester Result" with the keyword "Examination". Discuss the rules to be followed.	**14**	**1**	**4**
12. (a)	With neat diagram illustrate cipher block modes of operation.	**14**	**2**	**3**
	(OR)			
(b)	Illustrate detail about AES with neat diagram.	**14**	**2**	**3**
13. (a)	Explain the steps involved in SHA algorithm for encrypting a message with maximum length of less than 2128 bits and produces as output a 512-bit message digest, with neat diagram.	**14**	**3**	**2**
	(OR)			
(b)	Explain digital signature standard with necessary diagrams in detail.	**14**	**3**	**2**
14. (a)	Suggest and explain about an authentication scheme for mutual authentication between the user and the server which relies on symmetric encryption.	**14**	**4**	**4**
	(OR)			
(b)	Examine how firewalls help in establishing a security framework for an organization.	**14**	**4**	**4**
15. (a)	Analyse the methodologies involved in computing the keys in SSL/TLS protocol.	**14**	**5**	**4**
	(OR)			
(b)	Using the PGP cryptographic functions, analyse the security features offered for emails in detail.	**14**	**5**	**4**

PART- C (1x 10=10Marks)

(Q.No.16 is compulsory)

		Marks	CO	RBT LEVEL
16.	Alice and Bob use the Diffie – Hellman key exchange technique with a common prime number 11 and a primitive root of 2. If Alice and Bob choose distinct secret integers as 9 and 3, respectively, then compute the shared secret key and assess the same.	**10**	**2**	**5**

****