Q. Code: 628787

Reg. No. | | | | | | | | | | | | | |

B.E. / B.TECH. DEGREE EXAMINATIONS, MAY 2024

Sixth Semester

CS18603 – CRYPTOGRAPHY AND NETWORK SECURITY

(Computer Science and Engineering)

(Regulation 2018 / 2018 A)

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 (10 x 2 = 20 Marks)

(Answer all Questions)

		CO	RBT LEVEL
1.	List the types of security attacks with examples	**1**	**1**
2.	How many keys are required for two people to communicate each other?	**1**	**1**
3.	Brief the strengths of triple DES.	**2**	**2**
4.	Write down the difference between S DES, DES and AES.	**2**	**2**
5.	In what extent MD5 is stronger than MD4? State the reason.	**3**	**2**
6.	Write a comparison table of different versions of SHA parameters.	**3**	**2**
7.	State the difference between threats and attacks.	**4**	**3**
8.	Consider the client C wants to communicate server S using Kerberos procedure. How can it be achieved?	**4**	**3**
9.	How one can achieve end-to-end privacy in e-mail?	**5**	**3**
10.	Why E-mail compatibility function needed in PGP?	**5**	**2**

PART- B (5 x 14 = 70 Marks)

		Marks	CO	RBT LEVEL
11. (a)	Encrypt the following using play fair cipher using the keyword MONARCHY and the Plain text is. “MEET ME AFTER THE CLASS”. Use X as blank space.	**(14)**	**1**	**2**

(OR)

(b)	State and Prove Chinese remainder theorem for X and also find X for the given set of congruent equations using CRT $x \equiv 2 \pmod 3$ $x \equiv 3 \pmod 5$ $x \equiv 2 \pmod 7$	**(14)**	**1**	**2**
12. (a)	Analyze Diffie-Hellman key Exchange problem with a common prime number p=13, and a primitive root k=7. Show that 7 is a primitive root of 13. If Alice has a public key C=5, what is Alice's private key A? If Bob has a public key D=12, what is Bob's private key B?	**(14)**	**2**	**3**
	(OR)			
(b)	Examine the structure of AES Cipher and the transformations that constitutes in each round.	**(14)**	**2**	**3**
13. (a)	Discuss the data integration and authentication mechanism function in SHA- 512?	**(14)**	**3**	**3**
	(OR)			
(b)	Demonstrate how the integrity achieved by MD5 algorithm using compression function.	**(14)**	**3**	**3**
14. (a)	Discuss Client Server Mutual Authentication system with example and flow diagram..	**(14)**	**4**	**3**
	(OR)			
(b)	Discuss about firewall security mechanism in detail.	**(14)**	**4**	**3**
15. (a)	Discriminate SSL and TLS cryptographic security protocol mechanism in detail.	**(14)**	**5**	**3**
	(OR)			
(b)	Analyze the security features related to PGP in email security mechanism.	**(14)**	**5**	**3**

PART- C (1 x 10 = 10 Marks)

(Q.No.16 is compulsory)

		Marks	CO	RBT LEVEL
16.	Consider a ticket booking for the movie and illustrate the entire transaction life cycle with necessary steps.	**(10)**	**5**	**5**

****