Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII(NEW) • EXAMINATION – WINTER 2016

Subject Code:2170709 Date:21/11/2016

Subject Name:Information and Network Security

Time:10.30 AM to 1.00 PM Total Marks: 70

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

Q.1	**(a)**	What is symmetric key cryptography? What are the challenges of symmetric key cryptography? List out various symmetric key algorithms and explain Caesar cipher in detail.	**07**
	(b)	P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 6, then what will be cipher text value according to RSA algorithm? Explain in detail.	**07**
Q.2	**(a)**	Explain one time Pad in detail. What are the practical issues of this algorithm?	**07**
	(b)	Explain Byte substitution and Shift row operation of AES in detail.	**07**
		OR	
	(b)	Explain DES key generation process in detail.	**07**
Q.3	**(a)**	What is PKI? What are the components of PKI? Explain Certificate Authority in detail.	**07**
	(b)	"Only Hashing dose not ensures integrity of message in network communication" – Justify your answer with suitable example.	**07**
		OR	
Q.3	**(a)**	Consider the scenario where user A wants to send bulk data (data is in GBs) to user B using networking. Data exchange has to be done in confidential manner. The key which is used for encryption can be intercepted by an attacker. Which is the most efficient and protected way to achieve secure communication? Justify your answer in detail.	**07**
	(b)	What is SSL? Which security services does it offers? How does it works?	**07**
Q.4	**(a)**	What is Kerberos? How Kerberos authenticates the users for authorized service access?	**07**
	(b)	Write a short note on "Digital Signature Algorithm".	**07**
		OR	
Q.4	**(a)**	Explain Diffie - Hellman key exchange algorithm	**07**
	(b)	Differentiate between hashing and encryption. What are the practical applications of hashing? Compare MD5 and SHA1 hashing algorithms.	**07**
Q.5	**(a)**	Write a short note on Message Authentication Code.	**07**
	(b)	Write a short note on:	
		i. Cipher text only attack	**04**
		ii. Timing attack	**03**
		OR	
Q.5	**(a)**	What is SSH? How does SSH works?	**07**
	(b)	Write a short note on "Hill Cipher".	**07**

****