Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

ME SEMESTER – I EXAMINATION – SUMMER 2017

Subject Code: 2710211 **Date:11/05/2017**

Subject Name: Information Security

Time:02:30 p.m. to 05:00 p.m. **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 cryptography and cryptanalysis? Explain information security services and security attacks.	**07**
	(b)	Distinguish Block ciphers and Stream ciphers. Explain Output Feedback Mode. What are its advantages over Cipher Block Chaining Mode?	**07**
Q.2	**(a)**	Differentiate symmetric key and asymmetric key cryptography. How digital envelop provides better security than individual technique?	**07**
	(b)	Explain components of PKI in brief.	**07**
		OR	
	(b)	What is Confusion and Diffusion? Explain Feistel Cipher Structure.	**07**
Q.3	**(a)**	What is symmetric key encryption? Find out secret key using Diffie-Hellman key exchange algorithm on which Alice & Bob agreed upon for future communication with given initial values. Prime nos. known to public are n = 5 and g = 17 Alice's private key (x) = 97, Bob's private key (y) = 231	**07**
	(b)	Explain AES key expansion in detail.	**07**
		OR	
Q.3	**(a)**	Why double DES algorithm does not provide enough security? How triple DES overcomes this problem with same key size as used in double DES?	**07**
	(b)	Explain major disadvantages of symmetric key encryption system. How Diffie-Hellman algorithm helps to overcome issue of key exchange? Explain man in the middle attack for Diffie-Hellman key exchange algorithm.	**07**
Q.4	**(a)**	What is factoring problem in RSA? Explain Timing attack and Chosen cipher text attack in brief.	**07**
	(b)	What is Digital certificate? Explain X.509 certificate format in detail.	**07**
		OR	
Q.4	**(a)**	Discuss RSA cryptosystem and compute private key (d) for given prime nos. p=11 & q=7 and public key (e) = 37.	**07**
	(b)	What is Kerberos? Explain in detail how Kerberos protocol works?	**07**
Q.5	**(a)**	Explain digital signature creation and verification process with detail flow.	**07**
	(b)	Differentiate Computer Virus, Worms and Trojan Horse? What are the symptoms of Computer Worm? Explain Morris Worm and Code Red Worm.	**07**
		OR	
Q.5	**(a)**	What is malware and spyware? Explain different methods for malware detection.	**07**
	(b)	What is Message Authentication Code (MAC)? Explain Hash based Message Authentication Code (HMAC).	**07**

****