Seat No.: _____ **Enrolment No._____**

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) - EXAMINATION – SUMMER 2017

Subject Code: 2170709 **Date: 02/05/2017**

Subject Name: Information and Network Security

Time: 02.30 PM to 05.00 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)**	(1) Briefly explain any two active security attacks. (2) Discuss the following terms in brief: - brute force attack - cryptography	**04** **03**
	(b)	Explain single round of DES algorithm. Support your answer with neat sketches.	**07**
Q.2	**(a)**	Elaborate AES encryption with neat sketches.	**07**
	(b)	Discuss Electronic code book and cipher feedback mode with neat diagrams.	**07**
		OR	
	(b)	Explain playfair cipher substitution technique in detail. Find out cipher text for the following given key and plaintext. Key = ENGINEERING Plaintext=COMPUTER	**07**
Q.3	**(a)**	(1) Write differences between substitution techniques and transposition techniques. (2) Explain triple DES with two keys.	**03** **04**
	(b)	Write requirements for hash function and briefly explain simple hash function.	**07**
		OR	
Q.3	**(a)**	(1) Discuss the following terms in brief. - authentication - data integrity (2) Explain avalanche effect in DES and discuss strength of DES in brief.	**03** **04**
	(b)	Explain RSA algorithm in detail with suitable example.	**07**
Q.4	**(a)**	Explain any one approach to Digital Signatures.	**07**
	(b)	Discuss Diffie-Hillman key exchange algorithm in detail.	**07**
		OR	
Q.4	**(a)**	(1) Give differences between hash function and message authentication codes. (2) What are the principal elements of public-key cryptosystem? Explain in brief.	**03** **04**
	(b)	Write a detailed note on : Kerberos.	**07**
Q.5	**(a)**	Write a note on : Message Authentication Codes	**07**
	(b)	(1) Briefly explain web security threats. (2) Discuss SSL architecture in brief.	**03** **04**
		OR	
Q.5	**(a)**	Explain various general categories of schemes for the distribution of public keys.	**07**
	(b)	Write a note on : X.509 Certificate Format.	**07**

****