Seat No:________________ Enrollment No:________________

PARUL UNIVERSITY

FACULTY OF IT & COMPUTER SCIENCE

<<Parul Institute of Computer Application>>

<<BCA/IMCA>>2017-18 Mid Term Examination

Semester:5 **Date: (6/09/17)**
Subject Code: (05101304 /05301304) **Time: (2hr)**
Subject Name: (Network Security) **Total Marks: 40**

Instructions:
1. Figures to the right indicate full marks.
2. Make suitable assumptions wherever necessary.

Q.1	**Answer the following.**	**[10]**
(a)	Answer the following short questions of 1 mark each 1. What is cryptanalysis? 2. What is ciphertext? 3. Which are three component of OSI architecture?	[3]
(b)	Solve following short questions. (7 questions of 1 mark each)	[7]
	1. DES stands for ______________________. 2. AES is asymmetric encryption algorithm: true / false. 3. 3DES takes 64 bit block as an input : true / false. 4. Masqurade is _______________ type of attack. 5. In _______________ attack, attacker will not change the message. 6. P box stands for ____________________. 7. DES uses _______________ size of sub key.	
Q.2	**Answer the following.**	[10]
(a)	**Give answers for following Questions of 2 Marks each.** 1. What is private key and public key encryption ? 2. What is substitution and transposition cipher?	[4]

(b)	**Give answers for following Questions of 3 Marks each** 1. Explain Network security model. 2. Explain key generation algorithm of DES	[6]
Q.3	**Attempt any TWO.**	**[10]**
1	Write a short note on : Public key Infrastructure -PKI	[5]
2	Write a short note on AES	[5]
3	Write a short note on fiestel structure with example (encryption & decryption)	[5]
Q.4	**Answer the following.**	**[10]**
(a)	**Answer the following.** Write a short note on OSI architecture Attacks	[5]
(b)	**Answer the following.** Write a short note on private and public key cryptography with advantage and disadvantages.	[5]
	OR	
(b)	**Answer the following.** Explain cryptography with bifurcation and their details.	[5]