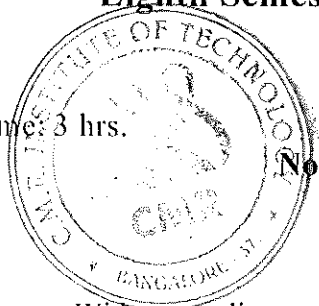


--	--	--	--	--	--	--	--	--	--

Eighth Semester B.E. Degree Examination, June/July 2016
Network Security

Time: 3 hrs.

Max. Marks: 100



Note: Answer FIVE full questions, selecting at least TWO questions from each part.

PART – A

- 1 a. With a neat diagram, explain network access security model with gate keeper function. (05 Marks)
- b. Classify and explain different type of attacks. (08 Marks)
- c. Using the keyword “ENCRYPT” create playfair matrix and obtain ciphertext for the message “MATCHFIXED”. Also write the rules used. (07 Marks)
- 2 a. Explain single round of DES along with the key generation. (10 Marks)
- b. Explain the working of counter mode of block cipher operation. (04 Marks)
- c. Discuss the final evaluation criteria of AES. (06 Marks)
- 3 a. Justify how both confidentiality and authentication are obtained in publickey cryprosystems. (05 Marks)
- b. Write RSA algorithm. (04 Marks)
- c. In Diffie Hellman key exchange $q = 71$, its primitive root $\alpha = 7$ A's private key is 5 B's private key is 12. Find: i) A's public key; ii) B's public key, iii) Shared secret key. (05 Marks)
- d. Explain the distribution of secret key using the public key cryprography with confidentiality and authentication. (06 Marks)
- 4 a. List out the requirements and explain the arbitrated digital signature technique. (10 Marks)
- b. Compare RSA and DSS approach. (06 Marks)
- c. Illustrate replay attack with examples. (04 Marks)

PART – B

- 5 a. Explain the key requirements and features of SET. (10 Marks)
- b. Discuss SSL record in terms of fragment compression and encryption. (10 Marks)
- 6 a. Explain password selection strategies. (08 Marks)
- b. Describe statistical anomaly detection. (06 Marks)
- c. Discuss the different categories of intruders. (06 Marks)
- 7 a. Give the taxonomy of malicious programs. Briefly explain all the software threats. (10 Marks)
- b. Describe digital immune system with diagram. (06 Marks)
- c. Brief on four generations of Antivirus software. (04 Marks)
- 8 a. What is firewall? Explain the various firewall configurations with relevant diagram. (10 Marks)
- b. Write short notes on:
 - i) Data Access Control
 - ii) Concept of Trusted system (10 Marks)

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
 2. Any revealing of identification, appeal to evaluator and or equations written e.g. 42+8 = 50, will be treated as malpractice.