

MANIPAL INSTITUTE OF TECHNOLOGY MANIPAL

VII SEMESTER B.TECH (INFORMATION TECHNOLOGY)

END SEMESTER EXAMINATIONS, ------

SUBJECT: E-COMMERCE AND NETWORK SECURITY [ICT 439]

REVISED CREDIT SYSTEM XXXXXXXX

Time: 3 Hours

MAX. MARKS: 50

Instructions to Candidates:

- ✤ Answer ANY FIVE FULL questions.
- ✤ Missing data may be suitably assumed.
- 1A. Alice uses Bob's RSA Public key (e=7, n=143) to send a plain text p=8 encrypted as a Cipher Text C= 57. Show how Eve can use the chosen cipher text attack, if Eve has the (05) access to Bob's computer to find the plaintext.
- **1B.** Explain in detail a Security Association. Specify the parameters that identify the Security (03)Association.
- **1C.** A transposition block has 10 inputs and 10 outputs. What is the order of the permutation group? What is the key size? (02)

2A.	Using S-DES, decrypt the string (10100010) using the key (0111111101). Show intermediate results after each function (IP, F_k , SW, F_k , IP ⁻¹). Then decode the first 4 bits of the plaintext string to a letter and the second four bits to another letter where we encode A through P in base 2 (i.e. A=0000, B=0001, P=1111)	(05)
2B.	TGT and TGS used a lot in Kerberos version 4 and 5. What do they mean? Where is it used and how it is used in Kerberos?	(02)
2C.	What is e-cash? Explain its properties.	(02)
3A. 3B.	With relevant steps and block diagrams, explain the message digest generation using SHA-1 Algorithm With a neat diagram explain PKIX Architectural Model.	(05) (03)
3C.	Differentiate between confusion and diffusion. How these two terms are applicable in cryptography?	

(02)

4A. 4B.	Explain how round keys can be generated in AES-128 by using key expansion process with suitable illustration What are digital copyrights? Explain.	(05) (03)
4C.	Write an algorithm for encryption using Playfair cipher technique.	(02)
5 A		(05)
5 A.	What is TLS? How does the TLS function P_Hash(Secret, Seed) works?	(05)
5B.	What do you mean by timing attack? Analyze the timing attack in DES.	(03)
5C.	What is an S-P network? Explain.	(02)
6A.	With a neat diagram, explain X.509 digital certificate and its various fields.	(05)
6B.	Discuss the three authentication procedures that are used across a variety of applications.	(03)
6C.	Find the possible corrupted bits in the plaintext for the following cases:	
	i. In Electronic Code Book (ECB) mode, bit 17 in cipher text block 8 is corrupted during	
	transmission.	
	ii. In Output Feed Back (OFB) mode the entire cipher text block 11 is corrupted during transmission.	(02)