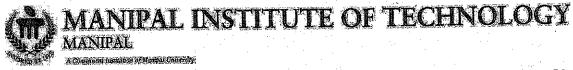
Reg. No.		



I SEMESTER M.TECH. (COMPUTER NETWORKING AND ENGINEERING) END SEMESTER EXAMINATIONS, NOV/DEC 2016

SUBJECT: INFORMATION SECURITY [ICT5103]

REVISED CREDIT SYSTEM (29/11/2016)

Time: 3 Hours

MAX. MARKS: 50

Instructions to Candidates:

- Answer ALL the questions.
- Missing data may be suitably assumed
- 1A. With a general block diagram explain the working of DES algorithm.
- (5)

(3)

- 1B. Generate a cipher text on applying Rail fence of depth 3 on the plain text "send more money cash not needed". What cipher text is generated using the row transposition method on the same plain text using the key 3 1 4 2 5?
- 1C. Explain how masquerade and denial of service attack affect the system. (2)
- 2A. Explain with neat diagram the AES key expansion process.

 Shown below is the original matrix and a matrix for the Round key.

 i) Apply the shift row transformation process on the original matrix

 ii) Round key application process on the original matrix using the Round key

ļ	AC	19	28	57
	77	FA	D1	5C
	66	DC	29	00
	F3	21	41	6A

matrix.

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

Original matrix

Round Key

- 2B. Compute the multiplication of $(m_1 \times m_2)$ modulo m(x) where $m_1 = (01010111)$, $m_2 = (10000011)$ and $m(x) = x^8 + x^4 + x^3 + x + 1$ using finite field GF(2⁸).
- 2C. Using Euclid's algorithm compute the gcd of 1970, 1066.

(2)

(5)

(3)

3A. Explain various designs that are used to secure the database when multilevel security is desired.

3B.	Users A and B use the Diffie-Hellman key exchange technique with a common	(3
	prime $q=11$ and a primitive root $a=7$.	•
	i. If user A has private key $X_A = 3$, what is A's public key Y_A ?	
	ii. If user B has private key $X_B = 9$, what is B's public key Y_B ?	
	iii. What is the shared secret key?	
	iv. If a third user C is the man in the middle and he has the private key X _{AC} =8 used	
	between A and C and X_{BC} = 6 between B and C what is the shared secret key used	
	by A and B with regard to C.	
3C.		(2
÷	p=3; q=11, e=7; M=2.	
4A.	With neat diagram show the two ways in which the IPSec ESP services can be used	(5
	in a network. Compare the two modes for their functionalities.	\-
4B.	Explain the various types of firewalls used in network security.	(3
40	How does the process of segmentation help in solving the problems of memory	•
40.	addressing?	(2
:	auuressing:	
5A.	With neat diagram explain the process involved in the construction of dual	(5
	signature. What is its role in the transaction that takes place between the order	`
	placed and the payment process?	
5B.	With a neat diagram explain how the transmission and reception of PGP message	(3
	takes place.	•
5C.	Explain the certification verification process used in X.509 between two users	(2
	certified by different certification authority.	

ICT 5103 Page 2 of 2