Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
(A constituent unit of MAHE, Manipal)

VII SEMESTER B.TECH. (COMPUTER & COMMUNICATION ENGINEERING)

MAKEUP EXAMINATIONS, 2019

SUBJECT: CYBER SECURITY [ICT- 4152]

REVISED CREDIT SYSTEM
(26/12/2019)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

- Answer **ALL** the questions.
- Missing data may be suitably assumed.

1A. Explain with neat diagrams the various types of hash functions based on block ciphers. **5**

1B. Perform encryption and decryption using the Knapsack algorithm for the given super increasing tuple= {2, 3, 6, 10}, multiplier r= 7 and modulus n= 22. Use Plain text = {1011}. Decrypt the resultant cipher text and verify the same. Use {4,1,3,2} as the permutation table **3**

1C. Distinguish, with suitable examples between:

i. Substitution ciphers and Transposition ciphers.

ii. Stream and Block Ciphers. **2**

2A.

i. In a Substitution Permutation Network proposed by Shanon prove $LE_{i-1} = RE_i \otimes F[LE_i, K_i]$ and also verify the validity of the same.

ii. List the strengths of DES algorithm.

iii. If hexadecimal 2B is given as an input to S-Box 1 (S [1]) what will be its corresponding output? Refer Table Q.2A for S-Box 1.

Table Q.2A: S-Box 1

	S[1]															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

5

2B. Explain Fiat-Shamir Protocol, with message exchange diagram. **3**

2C. Employing Whirlpool algorithm, find the output for the following :

i. If length of the original message is 3071 bits, compute the number of zeros needed

2C. in the padding bits.

ii. Calculate the round constant 2 [RC-2]. Refer to the Table Q.2C.

Table Q.2C: Sub Bytes

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*A*	*B*	*C*	*D*	*E*	*F*
0	18	23	C6	E8	87	B8	01	4F	36	A6	D2	F5	79	6F	91	52
1	16	BC	9B	8E	A3	0C	7B	35	1D	E0	D7	C2	2E	4B	FE	57
2	15	77	37	E5	9F	F0	4A	CA	58	C9	29	0A	B1	A0	6B	85
3	BD	5D	10	F4	CB	3E	05	67	E4	27	41	8B	A7	7D	95	C8
4	FB	EF	7C	66	DD	17	47	9E	CA	2D	BF	07	AD	5A	83	33
5	63	02	AA	71	C8	19	49	C9	F2	E3	5B	88	9A	26	32	B0
6	E9	0F	D5	80	BE	CD	34	48	FF	7A	90	5F	20	68	1A	AE
7	B4	54	93	22	64	F1	73	12	40	08	C3	EC	DB	A1	8D	3D
8	97	00	CF	2B	76	82	D6	1B	B5	AF	6A	50	45	F3	30	EF
9	3F	55	A2	EA	65	BA	2F	C0	DE	1C	FD	4D	92	75	06	8A
A	B2	E6	0E	1F	62	D4	A8	96	F9	C5	25	59	84	72	39	4C
B	5E	78	38	8C	C1	A5	E2	61	B3	21	9C	1E	43	C7	FC	04
C	51	99	6D	0D	FA	DF	7E	24	3B	AB	CE	11	8F	4E	B7	EB
D	3C	81	94	F7	9B	13	2C	D3	E7	6E	C4	03	56	44	7E	A9
E	2A	BB	C1	53	DC	0B	9D	6C	31	74	F6	46	AC	89	14	E1
F	16	3A	69	09	70	B6	C0	ED	CC	42	98	A4	28	5C	F8	86

2

3A. Using the following Symmetric key ciphers, perform the encryption for the text "MIT Manipal". Use 'X' for padding.

i. Affine cipher with the key (7, 2).

ii. Vigenere cipher using keyword "Student".

iii. Rail fence cipher with key =4. **5**

3B. What is meant by session hijacking? Mention various approaches for storing session tokens. **3**

3C. Define the terms Masquerading and Repudiation with relevant examples. **2**

4A. Alice chooses p= 19, e_1 =10, d = 16 and a random variable r to be 5. For the message M=14, show the signature generation and verification using ElGamal Digital Signature Scheme. **5**

4B. With relevant diagrams elucidiate and compare OFB and Counter mode **3**

4C. What is same origin policy? Give example. **2**

5A. What is Kerberos realm? Discuss various message exchanges in Kerberos realm protocol. **5**

5B. What is WAF? Discuss the various approaches of its implementation. **3**

5C. Perform encryption and decryption using RSA algorithm for the given parameters p=5, q=7, e=7 and message M=12. **2**