Reg. No. | | | | | | | | | | |

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

VII SEMESTER B.TECH. (INFORMATION TECHNOLOGY)
END SEMESTER EXAMINATIONS, NOV 2019
SUBJECT: INFORMATION AND WEB SECURITY [ICT- 4102]
REVISED CREDIT SYSTEM
(21/11/2019)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

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

1A. Given the hex code of the plaintext {0xA4, 0x9C, 0x7F, 0xF2, 0x68, 0x9F, 0x35, 0x2B, 0x6B, 0x5B, 0xEA, 0x43, 0x02, 0x6A, 0x50, 0x49} and the initial key { 0xC0, 0xAF, 0xDF, 0x39, 0x89, 0x2F, 0x6B, 0x67, 0x57, 0x51, 0xAD, 0x06, 0xB1, 0xAE, 0x7E, 0xC0 } answer the following by applying the functions of Advanced Encryption Standard. Refer to the tables. Refer the appropriate Table Q.1A (a) and Table Q.1A (b)

i. Show the original State displayed as 4X4 matrix.
ii. Show the value of the State after SubBytes.
iii. Show the value of the State after ShiftRows.
iv. Using Key Expansion method compute W4 and W5 for the specified initial key stream given above. **5**

1B. With suitable classification, illustrate the different types of security attacks. State which CIA-traid they threaten. **3**

1C. What is the difference between second preimage resistance and collision attack? **2**

2A. Consider an ElGammal digital signature scheme with a common prime p=467 and a primitive root 2. If Alice has a private key=127 and chooses random integer= 213, what is the cipher text for the message=100? Decrypt the resultant cipher text and verify the same. **5**

2B. Describe the idea of Merkle-Damgard scheme and why is this idea is important for the design of cryptographic function? **3**

2C. What is the minimum and maximum number of padding bits that can be added to a message in SHA-512 with suitable examples? **2**

3A. Bob selects two primes no's, 23 and 7. Alice wishes to send plaintext 24. Use Rabin crypto system to verify sender receives the same plain text? **5**

3B. State the similarities and dissimilarities between Whirlpool cipher and AES. **3**

3C. Explain the following
i. Replay attack
ii. Denial of service attack **2**

4A. With the timing diagram, IEEE 802.11i Phases of Operation for capability discovery, authentication and association **5**

4B. Briefly explain the idea behind the knapsack cryptosystem

i. What is the one-way function in this system?

ii. What is the trapdoor in this system?

iii. Define public and private keys in the system. **3**

4C. Consider the following:
Plaintext: "PROTOCOL"
Secret key: "NETWORK"
What is the corresponding cipher text using play fair cipher method? **2**

5A. What is zero knowledge protocol? Explain Feige-Fiat-Shamir Protocol with message exchanges. **5**

5B. Is it possible in SSL for the receiver to reorder SSL record blocks that arrive out of order? If so, explain how it can be done? If not, why? **3**

5C. List and explain various S/MIME functionalities. **2**

Table Q.1A (a): RCon constant look up Box

Round	*Constant (RCon)*	*Round*	*Constant (RCon)*
1	$(\underline{01}\ 00\ 00\ 00)_{16}$	6	$(\underline{20}\ 00\ 00\ 00)_{16}$
2	$(\underline{02}\ 00\ 00\ 00)_{16}$	7	$(\underline{40}\ 00\ 00\ 00)_{16}$
3	$(\underline{04}\ 00\ 00\ 00)_{16}$	8	$(\underline{80}\ 00\ 00\ 00)_{16}$
4	$(\underline{08}\ 00\ 00\ 00)_{16}$	9	$(\underline{1B}\ 00\ 00\ 00)_{16}$
5	$(\underline{10}\ 00\ 00\ 00)_{16}$	10	$(\underline{36}\ 00\ 00\ 00)_{16}$

Table Q.1A (b): AES S-box Table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16