Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

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

END SEMESTER EXAMINATIONS, NOV 2019

SUBJECT: CYBER SECURITY [ICT- 4152]

REVISED CREDIT SYSTEM
(21/11/2019)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

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

1A. Using the DSS scheme, let q=59, e_0=2, p=709, and d=14. Find values for e_1 and e_2. Choose random constant key r =13.Find the values of S_1 and S_2 if h (M) =100. Also verify the signature scheme. **5**

1B. List and explain the various security services prevalent nowadays. Also map each security service to its relevant security mechanism. **3**

1C. Find the result of 20^{132} mod 77 using FEMA. **2**

2A. Given the hex code of the value after shift-row function of Advanced Encryption Standard $\begin{bmatrix} d4 & e0 & b8 & 1e \\ bf & b4 & 41 & 27 \\ 5d & 52 & 11 & 98 \\ 30 & ae & f1 & e5 \end{bmatrix}$, answer the following by applying the functions of AES. Refer to the Tables Q.2A (i) and Q.2A (ii).

i. Show the value of the State after InvShiftRows.

ii. For the above obtained State value compute the value of the State after InvSubBytes.

iii. For the above obtained State value, display the obtained State matrix as Blocks.

iv. Employ AES-192 key Expansion to obtain W_6 and W_7 for the key stream {0x8E,0x73,0xB0,0xF7,0xDA,0x0E,0x64,0x52,0xC8,0x10,0x53,0x2B,0x80,0x90, 0x79,0xE5,0x62,0xF8,0xEA,0xD2,0x52,0x2C,0x6B,0x7B}. **5**

Table Q.2A(i) : RCON Constants

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.2A(ii) : Inverse Sub Bytes

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

2B. Illustrate how HMAC is computed, with a neat diagram. **3**

2C. Compare data origin authentication with entity authentication with relevant justification. **2**

3A. With suitable diagrams elucidate the process of Hashing and Key Expansion in a single round of Whirlpool. **5**

3B. List and explain the various attacks against digital signatures. **3**

3C. Explain the Play-fair Cipher rules and encrypt the message "we will meet tomorrow" with the key "story". Use 'x' for padding wherever suitable. **2**

4A. Discuss XSRF with a scenario. Also discuss the measures of prevention. **5**

4B. What is Lamport OTP approach? How is it different from other contemporary approaches? **3**

4C. The contents of three buffers are Buf_1= 0xC, Buf_2= 0xB and Buf_3= 0x8.Employing SHA-512 algorithm, find the output for the following cases:

a. Conditional(Buf_1, Buf_2, Buf_3)

b. Majority(Buf_1, Buf_2, Buf_3) **2**

5A. Discuss the Kerberos V5 Message exchanges with a neat diagram. **5**

5B. Consider an ElGamal scheme with a common prime p=11 and a primitive root e_1=2. If Alice has private key d=3 and chooses random integer r= 4, what is the cipher text of message M=7? Decrypt the resultant cipher text and verify the same. **3**

5C. Explain how SSO works. **2**