Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

VII SEMESTER B.TECH. (INFORMATION TECHNOLOGY)

END SEMESTER EXAMINATIONS, NOVEMBER 2018

SUBJECT: INFORMATION AND WEB SECURITY [ICT- 4102]

REVISED CREDIT SYSTEM

(24/11/2018)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

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

1A. Ryan and Terri are communicating using the El Gamal cryptosystem with prime p = 23 and primitive root $e_1 = 7$.

i. Terri creates her public key by choosing the exponent d = 5. What is Terri's public key?

ii. Ryan wants to send the message '3' to Terri. Demonstrate how Ryan encrypts the message. Take r=3.

iii. To ensure the integrity Ryan signs the document. For the above mentioned values show the signing and verification using El Gamal scheme.

iv. Terri receives the encrypted message $(C_1, C_2) = (9, 6)$ from Ryan. What is his plaintext message taking p = 23 and d=5? **5**

1B. Answer the following questions with respect to entity authentication

i. Explain Lamport one time password used in Entity Authentication.

ii. Define Zero Knowledge Protocol **3**

1C. What is the amount of padding required for a message of size 6143 bits if the hash algorithm used is

i. SHA- 512

ii. Whirlpool **2**

2A. With suitable diagrams elucidate the various hash function schemes which use block cipher as compression function. **5**

2B. In RSA public key cryptosystem, public key of the user is 31 and modulus (n) is 3599. **3**

Determine private key of the user. Also show the encryption and decryption of the message M =20.

2C. Give the benefits of IP security along with the examples of applications of IPsec. 2

3A. Using Hill Cipher show the encryption with detailed steps of the message "PLAINTEXT"

using the key matrix $\begin{bmatrix} 5 & 1 & 6 \\ 4 & 9 & 8 \\ 3 & 10 & 12 \end{bmatrix}$.

Use the mapping A= 00... Z = 25. 5

3B. Assume a client C wants to communicate with a server S using Kerberos 4 protocol. Illustrate the steps in the communication process with a neat diagram. 3

3C. Explain IEEE 802.11i phases of operation. 2

4A. Using Schnorr Scheme let q= 11, p =23, e_1= 2 and d= 9. Find the public and private keys. Choose r= 3, if M = 8 and h (88) =5, find the values of S_1, S2 and V. Is S_1 congruent to V mod p? 5

4B. Define security attacks. Explain the various security attacks prevalent nowadays. 3

4C. Differentiate between stream and block cipher with suitable examples. 2

5A. Given the hex code of the plaintext {18 64 5A 8E 0A 68 EF B2 B9 6A D7 10 B5 FB 79 D4} and the initial cipher key {0F 47 0C AF 15 D9 B7 7F 71 E8 AD 67 C9 59 D6 98} answer the following by applying the functions of Advanced Encryption Standard. Refer the tables 5A (i) and 5A (ii).

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 W_4 and W_5 for the initial key stream given above. 5

Table 5A(i) : RCON Constants

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

Table 5A(ii) : Sub Bytes

	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

5B. List the different protocols of SSL. Explain in detail Handshake protocol. 3

5C. What is PGP?Examine how authentication and confidentiality is maintained in PGP. 2