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

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

A Constituent Institution of Manipal University

VII SEMESTER B.TECH. (INFORMATION TECHNOLOGY)

END SEMESTER EXAMINATIONS, NOVEMBER 2017

SUBJECT: INFORMATION AND WEB SECURITY [ICT- 4102]

REVISED CREDIT SYSTEM
(21/11/2017)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

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

1A. Raj uses ElGamal for creating a secure system which projects Confidentiality, Integrity, Nonrepudiation and Authentication. Given the prime p=13, e_1 = 2, r=5 and d =3.

i) Encrypt the message "11".
ii) Decrypt the cipher text to get back the plain text.
iii) Calculate the two signatures S1 and S2.
iv) Show the verification process for the above calculated signatures.
v) Show with suitable justifications how Confidentiality, Integrity, Nonrepudiation and Authentication is maintained in the above communication scenario. 5

1B. Answer the following with suitable entity authentication mechanisms.

i) Mention and explain with a neat diagram the approach used in password protection which makes dictionary attack infeasible. 3
ii) Which password approach is immune to guessing attack?

1C. Differentiate between the functionalities of Ticket-granting server and Authentication server in Kerberos 4. 2

2A. Using SHA-512 protocol answer the following questions.

i) What is the padding required in SHA-512 if the length of the message is 5121bits?
ii) Show how W66 is made in SHA-512.
iii) Draw and explain the structure of a single round in SHA-512.
iv) The contents of three buffers are Buf1= 0x9, Buf2= 0xA and Buf3= 0xE.Find the output for the following cases:
a) Conditional(Buf1, Buf2, Buf3)
b) Majority(Buf1, Buf2, Buf3) 5

2B. Alice uses Bob's RSA public key (e= 7, p=11 and q=13) to encrypt a message. If the cipher text obtained on encryption is "48", generate the original message. Also list the various possible attacks which can compromise the security of this system. 3

2C. Briefly explain any four services provided by IPsec. 2

3A. Given the hex code of the plaintext {00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F} and the initial key {24 75 A2 B3 34 75 56 88 31 E2 12 00 13 AA 54 87} answer the following by applying the functions of Advanced Encryption Standard. Refer to Table Q.3A (a) and Table Q.3A (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 W_4 and W_5 for the initial key stream given above. 5

3B. Describe in brief the principle services provided by Pretty Good Privacy protocol (PGP). 3

3C. Describe the role of the following in providing Wireless LAN security conforming to IEEE 802.11.

i) Distribution System.
ii) Coordination Function. 2

4A. Using Rabin Cryptosystem with p=7 and q=11. Encrypt M= "10" and decrypt the same to find four possible plain texts. How the actual plain text gets identified from the four decrypted cipher texts in Rabin Cryptosystem? 5

4B. Encrypt "Information and Web" using Vigenère Cipher with key "Cyber". Output of this is given as input to a columnar transposition system having keyword "Security". Compute the final solution for the above mentioned scenario. Also show the decryption process for the same. 3

4C. Using the Table Q.4C, issue the message digest which you think will be given by Random Oracle Model for the following set of messages with suitable justifications.

i) AB1234CD8765BDAD
ii) 4523AB1352CDEF45126

Note that the Oracle uses the following principle for digest calculation.
" If the letter in the message is an alphabet, Oracle interprets it as 1. If the letter in the message is a digit, Oracle interprets it as 0" . The corresponding hex value is stored in the table.
Example : A1 : 10 which is 2 in hex. Value 2 is stored in the table. 2

5A. Using Hill Cipher show the encryption and decryption of the message "HerbertYardley". Use following details for the same.

i) Use mapping sequence for letter(a-z) as a = 01… z = 26.
ii) Use the following key matrix

$$\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$$ 5

5B. Compare and contrast attacks on digital signatures with attacks on cryptosystem. 3

5C. Explain in brief any type of active/ passive attack that threaten

i) Confidentiality
ii) Integrity
iii) Availability 2

Table Q.3A (a): 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.3A (b): 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

Table Q. 4C : Random Oracle

Message	Message Digest
4523AB1352CDEF45126	13AB
723BAE38F2AB3457AC	02CA
AB45CD1048765412AAAB6662BE	A38B