Question Paper

Exam Date & Time: 06-Dec-2023 (02:30 PM - 05:30 PM)

MANIPAL ACADEMY OF HIGHER EDUCATION

FIFTH SEMESTER B.TECH (COMPUTER AND COMMUNICATION ENGINEERING) END SEMESTER EXAMINATIONS, DECEMBER 2023

INFORMATION SECURITY [ICT 3172]

Marks: 50 **Duration: 180 mins.**

A

Answer all the questions. Section Duration: 180 mins

Instructions to Candidates: Answer ALL questions Missing data may be suitably assumed

1) Agent Smith was a top-secret agent for the government. He finds a piece of crucial information that he encrypts with a trail of algorithms as follows. Perform the required encryption and decryption process as listed below to decode his messages: (5)

A)

i. Decrypt "MEVTDIFTERVXIAGN" using Vigenere Cipher with the key "CAREFUL".

ii. Decrypt "JRAWS" with Multiplicative Cipher using Key =7.

iii. Decrypt "CANNHCGADODNIOLO" using Rail Fence Cipher with the key =3.

iv. Decrypt "RASYxWFEAxBECNOAHRRxEOKEU" with Key =" INDIA" using Columnar Cipher.

v. Decrypt "PTWVYAHUATLZZHNL" using Additive Cipher with Key =7 . Use the decrypted text as the key to Playfair Cipher to decrypt the message "ITUMBAKNECSORTLSQDMSNVANBLFMTKPRTRTENYNV".

Note :

- Merge i/j in the grid and use x as dummy character.
- Use mapping a/A=0 .....z/Z=25

B) Alice and Bob were two cryptographers tasked with establishing a secure communication channel across an unsafe network using the Diffie-Hellman key exchange protocol. They employ the prime number p: 97 and the Generator number α: 2. The private keys in question are Bob's private key b: 27 and Alice's private key a: 13. Calculate their common secret key. (3)
Also, justify why Diffie-Hellman key exchange is more secure than traditional methods of key exchange

C) Identify the significance of S-boxes in contributing to the security of the Data Encryption Standard (DES) algorithm. Calculate the output of the S-box for the following inputs: (2)

i. 011011 Sbox 5

ii. 111001 Sbox 6

Table 1C:S-Boxes

S[5]

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

S[6]

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

2) Given the hex code of the plaintext {34 24 1B 6C 52 7C 13 0D 70 2D 68 41 39 2B 7D 60} and the initial cipher key {EF 95 74 19 5C CE 9B 27 6E 73 7F 9A 1E 88 6F 05}, answer the following by applying the functions of Advanced Encryption Standard [Refer Tables 2A(i) and 2A(ii)]. (5)

A)

i. Show the original State displayed as a 4X4 matrix.

ii. Show the value of the State after SubBytes.

iii. Show the value of the State after ShiftRows.

iv. Using the Key Expansion method compute W_4 and W_5 for the initial key stream given above.

Table 2A(i) : RCON Constants

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

Table 2A(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

B) How do meet-in-the-middle attacks exploit vulnerabilities in the Data Encryption Standard (DES), and what is the significance of implementing double and triple DES as protective measures? Analyse and interpret the security implications of these encryption schemes. (3)

C) Examine the three different cases which threatens the security of MAC. (2)

3) Distinguish preimage and second preimage resistances with examples. (5)

A) Compute the following with respect to SHA512.

i. What is the leftmost digit of the result, when majority function is applied to buffers A,B and C with initial contents 0x7,0xA and 0xE respectively .

ii. What is the leftmost digit of the result, when conditional function is applied to buffers E,F and G with initial contents 0x9,0xA and 0XF respectively.

B) List three security services and mechanisms identified by X.800. Is there any relationship existence between two? (3)

C) Evaluate the vulnerability of Schnorr schemes in selective forgery when value of p =29 and q=7? Justify your answer. (2)

4) Compare the attacks on RSA signature scheme with possible forgeries in elgamal digital signature schemes. (5)

A)

B) One of the schemes of entity authentication using fixed password approach is to store the hash of the password in password file. What is the possible attack for this scheme? How it can be mitigated ? (3)

C) Let Alice be the client who want to securely communicate with Bob using SSL. The cipher suite exchanged between Alice and Bob is SSL_RSA_WITH_DES_CBC_SHA. Illustrate with suitable message exchange, how premaster key is established between Alice and Bob. (2)

5) Compare Flat Multiple KDC and Hierarchical KDC. Let K_A be the secret key established between Alice and Key Distribution Center (KDC). Also Let K_B be the secret key established between BOB and Key Distribution center. Illustrate with suitable message exchange, how KDC generates a session key K_{AB} using Needam-schroeder protocol to be used by Alice and Bob. (5)

A)

B) Illustrate the working of packed filtering firewall with suitable filtering rule. (3)

C) What are the different types of SSL payload that can be encapsulated when processing is done by the Record protocol. Also write the fields of Record Protocol Header (RPH). (2)

-----End-----