Question Paper

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

MANIPAL ACADEMY OF HIGHER EDUCATION

FIFTH SEMESTER B.TECH MAKEUP EXAMINATIONS, JANUARY 2023

INFORMATION SECURITY [ICT 3172]

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

A

Answer all the questions.

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

1) A) Compare the Message Authentication Code computation and Master Secret Generation in SSL and TLS with respect to efficiency. Also elucidate how TLS produces variable length key material? List the cryptographic secrets needed to be recomputed after session resumption with suitable reasoning. (5)

B) For the attacks listed below, define them and explain the security principle breached. Also mention how can it can prevented. (3)

a). Masquerade

b). Traffic Analysis

c). Repudiation

C) Differentiate between CA and CRL. What are various occasions to revoke certificates? (2)

2) A) Given the hex code of the plaintext {a4 9c 7f f2 68 9f 35 2b 6b 5b ea 43 02 6a 50 49} and the initial key {8e 73 b0 f7 da 0e 64 52 c8 10 f3 2b 80 90 79 e5 62 f8 ea d2 52 2c 6b 7b} answer the following by applying the functions of Advanced Encryption Standard- AES 192. Refer to the tables Q. 2 (a) and Q.2 (b). (5)

Table Q.2 (a): 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 Q.2(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

B) Compare and contrast encryption and decryption in Feistel cipher structure? Prove your view with relevant justifications and steps. (3)

C) Discuss three cases, where the MAC is vulnerable to threat and attacks? (2)

3) Using Rabin Cryptosystem perform the following: (5)

A) i. Consider p=7 and q=11 find the cipher text for the plain text M=5.

ii. How does Bob identify the correct plain text?

iii. Compute the decrypted plain text.

iv. How does the receiver determine proper plaintext after decryption?

B) Compare the compression function of SHA 512 without the last operation (final adding) with a Fiestel cipher of 80 rounds by showing similarities and differences. Also discuss the problem introduced during the elimination of final addition in SHA 512 compression engine?. (3)

C) Discuss on different attacks that may be possible on RSA digital signatures (2)

4) Specify the roles of various servers in Kerberos version 4. Demonstrate the sequence of message exchanges between client and these servers in the same. Identify the disadvantages of this scheme. (5)

A)

B) Let 'PRIVATE KEY' be the bitwise complement of 'PUBLIC KEY'. If the complement of plaintext block and key is taken, then whether the result of encryption has any impact? Prove your answer with relevant data and steps. (3)

C) Distinguish between different firewalls based on their functionalities (2)

5) How digital certificate is different from digital signature? Write the X.509v3 certificate format with usage of different fields. (5)

A)

B) For p=101, q=23 , s1=5, s2=7 and s3= 3. For the first round consider r=13. Show three rounds of the Feige- Fiat Shamir protocol by calculating the values and filling in the entries of a table (3)

C) Demonstrate the sequence of messages exchanged in SSL Handshake protocol? (2)

-----End-----