Y/K/TX

Reg. No:

Final Assessment Test – November 2024

VIT
Vellore Institute of Technology

Course: **CSI3002** - **Applied Cryptography and Network Security**

Class NBR(s): **1930/1934/1937/1940** Slot: **A1**

Time: **Three Hours** Max. Marks: **100**

- ➢ **KEEPING MOBILE PHONE/ELECTRONIC DEVICES EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE**
- ➢ **DON'T WRITE ANYTHING ON THE QUESTION PAPER**

Answer ALL Questions

(10 X 10 = 100 Marks)

1. (a) Find out whether the following relationship holds: 5 is a primitive root of 11. **[3]**

   (b) Use Euler's theorem to find a number 'x' between 0 and 28 with x^{85} congruent to 6 modulo 35. **[3]**

   (c) Using Successive Squaring and reducing modulo n, calculate 2^{513} mod 10. **[4]**

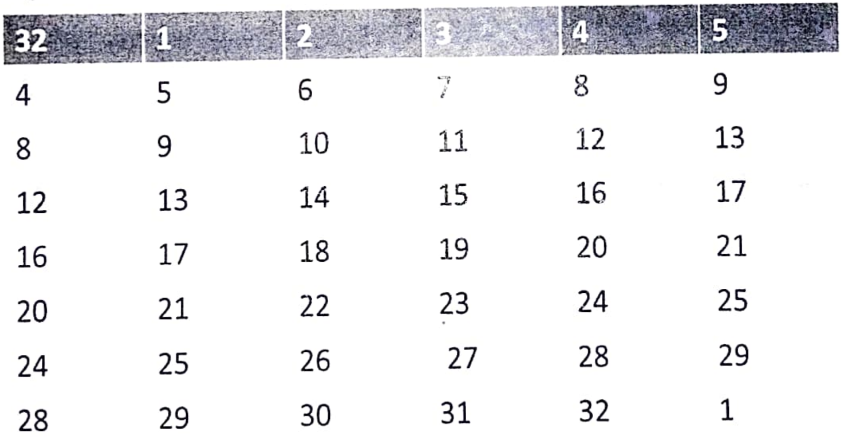
2. a) Given a 64-bit key K for Data Encryption Standard (DES) Algorithm. Determine the number of key bits after the parity bits have been discarded. **[2]**

   K = 01101000 10101011 01101100 11010010 00010001 00110100 00001000 10101100

   b) Given key (K_1) and right half of the Input message (R_0) compute f(R_0, K_1) function. **[8]**

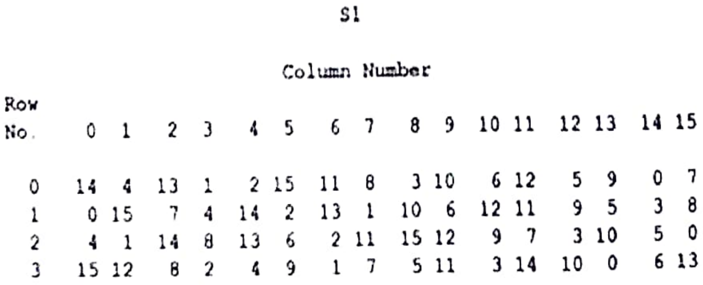
   K1 = 000110 110000 001011 101111 111111 000111 000001 110010

   R_0= 1111 0000 1010 1010 1111 0000 1010 1010



32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Fig.1: E-bit selection table



S1

Column Number

Row No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Fig.2: S – box

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Fig.3: P Table

3. Find the third-round key of AES-128 using the following second round key which is given in hexadecimal, S-Box table and round constant 04.

56	C7	76	A0
08	1A	43	3A
20	B1	55	F7
07	8F	69	FA

Fig.4: Second Round Key

		Y															
		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
X	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	4D	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

Fig.5: S-Box Table

4. (a) In the Diffie-Hellman protocol, each participant selects a secret number x and sends the other participant αx mod q for some public number α. What would happen if the participants sent each other xα for some public number α instead? Give at least one method Alice and Bob could use to agree on a key. Can Eve break your system without finding the secret numbers? Can Eve find the secret numbers? [3]

(b) Let E be the Elliptic Curve E: $y^2 = x^3 + x + 1$. Let P= (4,2) and Q= (0,1) be points on E modulo 5. Solve the Elliptic Curve Discrete Logarithm Problem for P and Q, finding a positive integer *n* such that Q = *n*P. [7]

5. (a) Suppose we have a set of blocks encoded with the RSA algorithm and we don't have the private key. Assume *n* = *pq*, *e* is the public key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with *n*. Does this help us in any way? [5]

(b) Given the requirement that the RSA modulus n=p*q must be at least 1024 bits long, where p and q are prime numbers of equal bit size, what is the minimum bit size of p and q? [2]

(c) In RSA encryption algorithm, prime numbers are p=17 and q=31. Generate public key and private key pairs. [3]

6. (a) If a message is 1500 bytes long, how many iterations (512-bit blocks) will the MD5 algorithm perform during the message digest computation? [2]

(b) Compute the value of the padding field, length filed, and number of blocks in MD5 if the length of the message is, [4]

I) 4000 bits II) 5000 bits

(c) In MD5, compute the output of a process block in round 1, if the Initial buffer values are [4]

A – 01234567 B – 89abcdef

C – fedcba98 D – 76543210

7. Suppose in the HMAC algorithm, the Message M = "CrypTo" and the Key K = "TT". Find out the 'S_i' and 'S_o' based on the Hex Conversion of ASCII characters where the length of the hash code 'n' is 4 bits.

ASCII Character	Hexadecimal	ASCII Character	Hexadecimal
A	41	a	61
B	42	b	62
C	43	c	63
D	44	d	64
E	45	e	65
F	46	f	66
G	47	g	67
H	48	h	68
I	49	i	69
J	4A	j	6A
K	4B	k	6B
L	4C	l	6C
M	4D	m	6D
N	4E	n	6E
O	4F	o	6F
P	50	p	70
Q	51	q	71
R	52	r	72
S	53	s	73
T	54	t	74
U	55	u	75
V	56	v	76
W	57	w	77
X	58	x	78
Y	59	y	79
Z	5A	z	7A

8. a) A company's server certificate has expired, and they are unable to process secure transactions. Outline the steps they should take to renew the certificate and restore secure services. **[4]**

b) Define a certification authority (CA) and its relation to public-key cryptography. **[3]**

c) How does PKI ensure non-repudiation in digital transactions? Explain with an example. **[3]**

9.a) i. In the Needham-Schroeder protocol, [4]

1) How is Alice authenticated by the KDC?
2) How is Bob authenticated by KDC?
3) How is the KDC authenticated to Alice?
4) How is the KDC authenticated to Bob?
5) How is Alice authenticated to Bob?
6) How is Bob authenticated to Alice?

ii. Draw and explain the authentication process between say a user and server using Kerberos with a neat diagram. [6]

OR

9.b) i. Why does PGP maintain Rings with every user? Explain how the messages are generated by PGP with a neat sketch. [7]

ii. List the functions included in MIME to enhance the security and how they are processed. [3]

10.a) i) [4]

1) A host receives an authenticated packet with the sequence number 181. The replay window spans from 200 to 263. What will the host do with the packet? What is the window span after this event?
2) A host receives an authenticated packet with the sequence number 208. The replay window spans from 200 to 263. What will the host do with the packet? What is the window span after this event?

ii) How is the security achieved in the Transport and Tunnel modes of IPSec? Also, explain with a neat sketch, the role of AH and ESP. [6]

OR

10.b) i) The combination of key exchange, hash, and encryption algorithms defines a cipher suite for each Secure Socket Layer (SSL) session. Explain the following two SSL cipher suites with proper sequence. [4]

1) SSL_RSA_WITH_DES_CBC_SHA
2) SSL_RSA_WITH_RC4_128_MD5

ii) SSL defines four protocols in two layers. Explain in detail about each phase in the Initial protocol. [6]

⇔⇔⇔ **Y/K/TX** ⇔⇔⇔