Department of Computer Science UET Lahore, New Campus

Semester:

Spring-2023

EXAM: Mid Term

CS 364-Information Security

Time Limit: 100 minutes Total Marke: 35

Name: Muhammadumam Regd. No. 2020-SE-35 Section:

CLO1[5] CLO4[30] 7.4

Q. Na.	Questions List the key security services desired in computer networks. For each service, explain what the service means.	MARK
l. CLO I	(ON) LENGROS / INCOMIS, HUMANICAY / NOONE SOUS / CICLESS (ON)	3
2. CLOI	Define following. (attempt any one) 1. Unconditionally secure and computationally secure encryption scheme, 2. Brute Force Attack	2
3.	3. Confusion and Diffusion 1. In the DES algorithm the round key is bit and the Round Input is bits.	_
€LO4	(a) 48, 32 b) 64,32	7
6,1	c) 56, 24 d) 32, 32	
6,	In the DES algorithm the 64 bit key input is shortened to 56 bits by ignoring every 4th bit. a) True (b) False	
	The DES Algorithm Cipher System consists ofrounds each with a round key a) 12 b) 18	
	e) 9 , (d) 16	
	4. The number of unique substitution boxes in DES after the 48 bit XOR operation are	
	b) 4 c) 6 d) 12	
	5. In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via (a) Scaling of the existing bits	
	b) Duplication of the existing bits c) Addition of zeros d) Addition of ones	
	6/ The number of tests required to break the DES algorithm are a) 2.8×10 ¹⁴	
	b) 4.2×10° c) 1.84×10 ¹⁹	
	d)7.2×10 ¹⁶ 7 AES uses a bit block size and a key size of bits. a) 128; 128 or 256	
	b) 64; 128 or 192 c) 256; 128, 192, or 256	
	(d) 128; 128, 192, or 256 For the AES-128 algorithm there are similar rounds and round is different. a) 2 pair of 5 similar rounds; every alternate	
	(b))9; the last c) 8; the first and last d) 10; no	
	9. The 4×4 byte matrices in the AES algorithm are called a)States	
	b) Words	

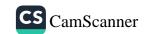
		A COUNTY OF THE PERSON NAMED OF THE PERSON NAM	or fin h							A STATE OF THE PARTY OF THE PAR
		c) Transition	OUS							
	1	d) Permuta	tions							
	1 1	In AES the	4×4 bytes	matrix key	is transform	ed into a ke	ys of size	byten		
	/						principles	sychia a crise to ref		
	/	n) 32								- 1
		b) 64								
		c) 54								
	1	(d))44								
	111	On compari	ing AES wit	th DES, wh	ilch of the fo	llowing fu	nctions from Di	BS does not h	nve an equivale:	nt
	N.M	AES function	on?							
	A.	a) f function								- 1
	'	a) I function	1							
	1	b) permutati	ion p							
		(c) swapping	of halves							- 1
	1 .	d) xor of sul	bkey with fu	inction f						
	1 6	On performi	ing the Mix	Columns to	ansformatic	on for the se	quence of byte	8 ''77 89 AB (CD'' we get	- 1
	1	output								- 1
		a) (01 55 EE	: 44)							
		n) (01 33 EE	5 4(1)							
	1	b) (0A 44 E	r 4/\}							
	1	(0) (08 55 FF	3A}							- 1
		d) (09 44 DI	O 4A}							
	1 1	Conversion of	of the Plaint	ext WILLL	amstalli	NGS to a s	tate matrix lead	Is to?	TI IT	
								1	12/2	IN
	14.	What is the S	Shifted Row	transforma	tion for the	matrix bell	ow7		TAA	
	1								LML	114
	100	DT AF	FF		FE 72	2B	D7		16/11	
	FE	72 28							1 11-15 14	15
				1 (6B 77	A 4	6B		سلسندلينا ا	
	b B	77 A4	1 6B	A	ND 01	FO	63			1
	AD	ol FO	63	1 -	30 D7	AF	FE			- 1
				,	_	7.11				
, ,	1.	Show that 760	e 34 (mod	47. OR 🗸						3
	2.	Find multiplic	ative invers	e using Fer	mat's little t	heorem 5 r	nod 19.			
04										- 1
5.						7 0 11	- - - - -	111 4 -1		
				C			er a block ciphe			5+5
	Р	K 00	01	10	11	table be	low. The table	gives the cipl	nertext C	5+5
	0000	1111	0000	0101	0001	table be	low. The table d when encryp	gives the cipl		5+5
04	0000	1111		10		table be produce of the fe	low. The table d when encryp our keys.	gives the cipl ting the plain	text P with one	5+5
	· 0000 · 0001	1111	0000 0010	0101	0001	produce of the fe Using c	elow. The table ed when encrypour keys. ipher A and the	gives the ciph ting the plain following me	nertext C text P with one	5+5
	0000 0001 0010	1111	0000 0010 0101	0101 1001 0111 0010	0101 0101	produce of the fe Using c	low. The table d when encryp our keys.	gives the ciph ting the plain following me	nertext C text P with one	5+5
	· 0000 · 0001	1111 0001 1010	0000 0010 0101 1010 1001	10 0101 1001 0111 0010 1100	0101 1010 1010	produce of the fe Using c	elow. The table ed when encrypour keys. ipher A and the	gives the ciph ting the plain following mo ciphertext C w	nertext C text P with one	5+5
	0000 0001 0010 0011	1111 10001 1010 0111 1000 1100 1011	0000 0010 0101 1010 1001 1110	10 0101 1001 0111 0010 1100 1011	0001 1111 0101 1010 0100	table be produce of the following coperation	elow. The table of when encrypour keys. ipher A and the on, decrypt the color of 1101 0100 11	gives the ciph ting the plain following mo ciphertext C w	nertext C text P with one	5+5
	0000 0001 0010 0011 0100 0101 0110	1111 10001 1010 0111 1000 1100 1011 0000	0000 0010 0101 1010 1001 1110 0111	10 0101 1001 0111 0010 1100 1011 1110	0001 1111 1000 1111 0101 1010 0100	table be produce of the following coperation C	elow. The table of when encrypour keys. ipher A and the on, decrypt the color of th	gives the ciphting the plaint following monophertext C w 00 0100	nertext C / vith one odes of vith key K:	5+5
	0000 0001 0010 0011 0100 0101 0110 0111	1111 0001 1010 0111 1000 1100 1011 0000 1111	0000 0010 0101 1010 1001 1110 0111 1111	10 0101 1001 0111 0010 1100 1011 1110 0001	0001 1111 0101 1010	table be produce of the four operation C K In all ca	elow. The table of when encryptour keys. ipher A and the on, decrypt the control of 1101 0100 11 000 ses assume any	gives the ciphting the plaint following monophertext C w 00 0100	nertext C / vith one odes of vith key K:	5+5
	0000 0001 0010 0011 0100 0101 0110 0111 1000	1111 0001 1010 0111 1000 1100 1011 0000 1110 1110 1001	0000 0010 0101 1010 1001 1110 0111	10 0101 1001 0111 0010 1100 1011 1110	0001 0111 1000 1111 0101 1010 1110 0110	table be produce of the fi Using c operatio	elow. The table of when encryptour keys. ipher A and the on, decrypt the control of the control	gives the ciphting the plaint following monophertext C w 00 0100	nertext C / vith one odes of vith key K:	5+5
	0000 0001 0010 0011 0100 0101 0110 0111	1111 0001 1010 0111 1000 1100 1011 0000 1111	0000 0010 0101 1010 1001 1110 0111 1111 0001	10 0101 1001 0111 0010 1100 1011 1110 0001 1101	0001 0111 1000 1111 0101 1010 0110 0110 1011	table be produced of the formula of	elow. The table of when encryptour keys. ipher A and the on, decrypt the color of t	gives the cipiting the plaint following me ciphertext C w 00 0100 initial values	nertext C / vith one odes of vith key K:	5+5
	0000 0001 0010 0011 0100 0101 0110 0111 1000 1001	1111 0001 1010 0111 1000 1100 1011 0000 1110 1001 1001	0000 0010 0101 0101 1001 1110 0111 1111 0001 0011 11100 1101 01100	10 0101 1001 1001 0110 0110 1100 1110 0001 1101 1100 0001 0100 0110	0001 0111 1000 1111 0101 1010 0110 011	table be produced of the formula of	elow. The table of when encryptour keys. ipher A and the encrypt the control of the encrypt the control of the encrypt the control of the encrypt in the enc	gives the cipling the plaint following money in the plaint following money in the following money for the plaint following m	nertext C / vith one odes of vith key K:	5+5
	0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1011 1110	1111 0001 1010 0111 1000 1100 1011 0000 1110 1001 0100 0101 1101	0000 0010 0101 1001 1001 1110 0111 0001 1110 0011 1100 0110 1101 0100	10 0101 1001 0111 0010 1100 1011 1110 0001 1101 1000 0000 0110	0001 0111 1000 1111 0101 1010 0110 1110 1110 1101 1101 0010 0010	table be produced of the formula of	elow. The table of when encryptour keys. ipher A and the encrypt the control of the encrypt the control of the encrypt the control of the encrypt in the enc	gives the cipling the plaint following money in the plaint following money in the following money for the plaint following m	nertext C / vith one odes of vith key K:	5+5
	0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1110 1110	1111 0001 1010 0111 1000 1100 1011 0000 1110 1001 1001 1101 0101 1101 0101	0000 0010 0101 1010 1010 1110 0111 1111 0011 1110 0011 1100 1101 1100	10 0101 1001 0111 0010 1100 1101 1110 1100 0000 0100 0110 1111	0001 0111 1000 1010 1010 1010 1011 1011 1001 1001 1001 1000 1100	table be produced of the formula of	elow. The table of when encryptour keys. ipher A and the on, decrypt the control of the control	gives the cipling the plaint following money in the plaint following money in the following money for the plaint following m	nertext C / vith one odes of vith key K:	5+5
	0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1011 1110	1111 0001 1010 0111 1000 1100 1011 0000 1110 1001 0100 0101 1101	0000 0010 0101 1001 1001 1110 0111 0001 1110 0011 1100 0110 1101 0100	10 0101 1001 0111 0010 1100 1011 1110 0001 1101 1000 0000 0110	0001 0111 1000 1111 0101 1010 0110 1110 1110 1101 1101 0010 0010	table be produced of the fusing coperation of	elow. The table of when encryptour keys. ipher A and the on, decrypt the control of the control	gives the cipling the plaint following money in the plaint following money in the following money for the plaint following m	nertext C / vith one odes of vith key K:	5+5
	0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1110 1110	1111 0001 1010 0111 1000 1100 1011 0000 1110 1001 1001 1101 0101 1101 0101	0000 0010 0101 1010 1010 1110 0111 1111 0011 1110 0011 1100 1101 1100	10 0101 1001 0111 0010 1100 1101 1110 1100 0000 0100 0110 1111	0001 0111 1000 1010 1010 1010 1011 1011 1001 1001 1001 1000 1100	table be produced of the formula of	elow. The table of when encryptour keys. ipher A and the on, decrypt the control of the control	gives the ciphting the plaint following money in the plaint follow	nertext C / vith one odes of vith key K:	5+5
	0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1110 1110	1111 0001 1010 0111 1000 1100 1011 0000 1110 1001 1001 1101 0101 1101 0101	0000 0010 0101 1010 1010 1110 0111 1111 0011 1110 0011 1100 1101 1100	10 0101 1001 0111 0010 1100 1101 1110 1100 0000 0100 0110 1111	0001 0111 1000 1010 1010 1010 1011 1011 1001 1001 1001 1000 1100	table be produced of the formula of	elow. The table of when encryptour keys. ipher A and the on, decrypt the control of the control	gives the ciphting the plaint following money in the plaint follow	nertext C / vith one odes of vith key K:	5+5
04	0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1011 1010 1100 1101 1110	1111 0001 1010 0111 1000 1100 1011 0000 1110 1001 0100 0110 0101 1101 0010 0011	0000 0010 0101 1010 1010 1110 0111 1111 0001 1110 0110 1100 1101 1000 1011	10 0101 1001 1001 1100 1110 0110 1110 0001 1101 1100 0000 0100 0110 1111 0011	0001 0111 1000 1111 0101 1010 0110 1110 1110 1101 1101 1101 0010 0000 1100 0011	table be produced of the five section of the	elow. The table of when encryptour keys. ipher A and the on, decrypt the on 1101 0100 11 00 ses assume any ter: mode decryptic B E Counter C	gives the cipiting the plaint following mo ciphertext C w 00 0100 initial values	nertext C / vith one odes of vith key K:	
04	0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1110 1110 1110 1111	1111 0001 1010 0111 1000 1100 1101 0000 1110 1001 0100 0110 0101 1101 0010 0011	0000 0010 0101 1010 1010 1110 0011 1110 0011 1100 1101 1000 1011 1000 1011	10 0101 1001 0110 0110 1100 1110 0001 1101 1100 0000 0100 0110 1111 0011 1101 1010	0001 0111 1000 1111 0101 1010 0100 1110 0110 1101 1101 0010 0000 1100 0001	table be produced of the full Using coperation operation C In all cases as a Counter C Counter C CBC mo C C C C C C C C	elow. The table of when encryptour keys. ipher A and the on, decrypt the of 1101 0100 11 00 ses assume any ter: mode decryptic \mathbb{E}_{k_i} Counded decryption: \mathbb{E}_{k_i} Counded decryption: \mathbb{E}_{k_i} Counded decryption:	gives the cipiting the plaint following mo ciphertext C w 00 0100 initial values	nertext C / vith one odes of vith key K:	5+5
04	0000 0001 0010 0010 0101 0110 0110 1000 1001 1000 1001 1110 1110 11110 11111	1111 0001 1010 0111 1000 1100 1101 0000 1110 1001 0100 0110 0101 0101 0010 0011 the meet-in-th given in Prev.	0000 0010 0101 0101 1010 1011 0011 1110 0001 0011 1100 1101 1100 1101 1000 1011 1000 1011	10 0101 1001 0110 0110 1100 1100 1101 1101 1100 0000 0110 0110 1111 0011 1101 ttack works	0001 0111 1000 1111 0101 1010 1100 110	table be produced of the full case operation of the full case of the	elow. The table of when encryptour keys. ipher A and the on, decrypt the on 1101 0100 11 00 ses assume any ter: mode decryptic B E Counter C	gives the cipiting the plaint following mo ciphertext C w 00 0100 initial values	nertext C / vith one odes of vith key K:	
1	0000 0001 0010 0011 0100 0101 0111 1000 1001 1010 1110 1110 1111 1111 Show how cipher A is	1111 0001 1010 0111 1000 1100 1101 0000 1110 1001 0100 0110 0101 0101 0010 0011 the meet-in-th given in Prev (plaintext, cip)	0000 0010 0101 1010 1010 1110 0011 1110 0011 1100 1010 1010 1010 1000 1011 1000 1011 1000 1011	10 0101 1001 0010 1100 1100 1101 1101	0001 0111 1000 1111 0101 1010 1101 1101 1001 0010 0000 1100 0000 1100 0011 by applying attack to fin	table be produced of the full case operation of the full case of the	elow. The table of when encryptour keys. ipher A and the on, decrypt the of 1101 0100 11 00 ses assume any ter: mode decryption: $C(C_i) \oplus C_i$ Double- A , when sed if the attack	gives the cipiting the plaint following mo ciphertext C w 00 0100 initial values	nertext C / vith one odes of vith key K:	
4 1	0000 0001 0010 0010 0101 0110 0111 1000 1001 1010 1110 1111 1110 1111 Show how cipher A is knows the	1111 0001 1010 1011 1000 1100 1011 0000 1110 0100 0110 0101 1101 0010 0011 the meet-in-the given in Prev (plaintext, ciparly the steps	0000 0010 0101 1010 1010 1110 0011 1110 0011 1100 1010 1010 1010 1000 1011 re-middle al	10 0101 1001 0110 1100 1100 1101 1101 1000 0000 0110 0110 1111 0011 1010 0010 01	0001 0111 1000 1111 0101 1010 1100 110	table be produced of the five services of the services of t	elow. The table of when encryptour keys. ipher A and the on, decrypt the of 1101 0100 11 00 ses assume any ter: mode decryptic E_k (Counded decryption: E_k (Counded decryption: E_k (Counded decryption: E_k (Ci) E_k (C	gives the cipiting the plaint following modification of the cipital values on: Column	text P with one odes of with key K:	
4	0000 0001 0010 0101 0110 0110 1011 1000 1001 1010 1111 1110 1111 1110 1111 1111 Show how cipher A is knows the Explain cle	1111 0001 1010 1011 1000 1100 1011 0000 1110 0100 0110 0101 1101 0010 0011 the meet-in-the given in Prev (plaintext, ciparly the steps	0000 0010 0101 1010 1010 1110 0011 1110 0011 1100 1010 1010 1010 1000 1011 re-middle al	10 0101 1001 0110 1100 1100 1101 1101 1000 0000 0110 0110 1111 0011 1010 0010 01	0001 0111 1000 1111 0101 1010 1010 1101 1101 1001 0010 0000 1100 0011 by applying attack to fin 111) (0100, and how the	table be produced of the five services of the services of t	elow. The table of when encryptour keys. ipher A and the on, decrypt the of 1101 0100 11 00 ses assume any ter: mode decryption: $C(C_i) \oplus C_i$ Double- A , when sed if the attack	gives the cipiting the plaint following modification of the cipital values on: Column	text P with one odes of with key K:	
4	0000 0001 0010 0101 0110 0110 1011 1000 1001 1010 1110 1111 1110 1111 1111 Show how cipher A is knows the Explain cle Hint: first	1111 0001 1010 0111 1000 1100 1101 0100 1110 0100 0110 0101 0101 0010 0011 the meet-in-th given in Prev (plaintext, cip, arly the steps apply brute fo	0000 0010 0101 0101 1110 0111 1110 0001 0011 1100 1101 0110 1000 1011 re-middle al	10 0101 1001 0110 1100 1100 1101 1101 1000 0000 0110 0110 1111 0011 1010 0010 01	0001 0111 1000 1111 0101 1010 0100 1101 1101 1001 0000 0000 1100 0011 by applying attack to fin 111) (0100, and how the sand estimated to	table be produced of the full case operation of the full case of the full c	elow. The table of when encryptour keys. ipher A and the on, decrypt the of 1101 0100 11 00 ses assume any ter: mode decryptic E_k Counded decryption:	gives the cipiting the plaint following modification of the cipital values on: Column	text P with one odes of with key K:	
4 1	0000 0001 0010 0100 0101 0110 0110 1001 1001 1100 1110 1111 1110 1111 1111 Show how cipher A is knows the Explain cle Hint: first pair	the meet-in-th given in Prev (plaintext, cipsarply brute fo	0000 0010 0101 0101 1110 0111 0011 1110 0011 1100 1101 1000 1011 ne-middle alious Questichertext) pair applied by the confirst	10 0101 1001 0111 0010 1100 1101 1110 0001 1101 1000 0000 0100 0110 1111 0011 1010 ttack works on. Use the rs: (1110, 0 the attacker known pair	0001 0111 1000 1111 0101 1010 1010 101	table be produced of the five contents of the key until 101) of the key is ideate keys, the optes, use 8	elow. The table of when encryptour keys. ipher A and the on, decrypt the control of the control	gives the cipiting the plaint following mo ciphertext C w 00 0100 initial values on: tter re ker already ated keys on s	econd known	5
4	0000 0001 0010 0100 0101 0110 0110 1001 1001 1100 1110 1111 1110 1111 1111 Show how cipher A is knows the Explain cle Hint: first pair	the meet-in-th given in Prev (plaintext, cipsarply brute fo	0000 0010 0101 0101 1110 0111 0011 1110 0011 1100 1101 1000 1011 ne-middle alious Questichertext) pair applied by the confirst	10 0101 1001 0111 0010 1100 1101 1110 0001 1101 1000 0000 0100 0110 1111 0011 1010 ttack works on. Use the rs: (1110, 0 the attacker known pair	0001 0111 1000 1111 0101 1010 1010 101	table be produced of the five contents of the key until 101) of the key is ideate keys, the optes, use 8	elow. The table of when encryptour keys. ipher A and the on, decrypt the of 1101 0100 11 00 ses assume any ter: mode decryptic E_k Counded decryption:	gives the cipiting the plaint following mo ciphertext C w 00 0100 initial values on: tter re ker already ated keys on s	econd known	
4 1 1 1 1 1 1 1 1 1	0000 0001 0010 0100 0101 1000 1001 1100 1101 1100 1101 1110 1111 1110 1111 1111 Show how cipher A is knows the Explain cle Hint: first pair Consider the s, the state	the meet-in-th given in Prev (plaintext, cipsarply brute fo	0000 0010 0101 0101 1110 0111 0001 000	10 0101 1001 0111 0010 1100 1101 1110 0001 1101 1000 0000 0100 0110 1111 0011 1010 ttack works on. Use the rs: (1110, 0 the attacker known pair	0001 0111 1000 1111 0101 1010 1010 101	table be produced of the five contents of the key until 101) of the key is ideate keys, the optes, use 8	elow. The table of when encryptour keys. ipher A and the on, decrypt the control of the control	gives the cipiting the plaint following mo ciphertext C w 00 0100 initial values on: tter re ker already ated keys on s	econd known	5
4 1 1 1 I I I I I I I I I I I I I I I I	0000 0001 0010 0100 0101 1000 1001 1100 1101 1110 1111 1110 11111 11111 1111 1111 11111 1111 1111 1111 1111	the meet-in-th given in Prevention Sapply brute for S is 8 and be represent.	0000 0010 1010 1010 1010 1111 0001 1111 0001 1100 1100 1101 1000 1011 1000 1001 1001 1000 1000 1	10 0101 1001 1110 0010 1110 0010 0000 0100 0110 1111 1010 1010 1111 1010 1010 1011 1011 1011 1011 1011 1011 1011 1011 1011 1011 1011 1011 1010 1011 101	0001 0111 1000 1111 0101 1010 0100 1101 1101 1001 0000 1100 0010 0000 1100 0011 by applying attack to fin 111) (0100, and how the sand estimate the full 256 te on 3-bits of the sand state to the full 256 te on 3-bits of the sand state to the full 256 te on 3-bits of the sand state to the full 256 te on 3-bits of the sand state to the full 256 te on 3-bits of the sand state to the sand s	table be produced of the five contents of the key until 101) to key is ide keys, the contents of plaintext	elow. The table of when encryptour keys. ipher A and the on, decrypt the control of the control	gives the cipiting the plaint following mo ciphertext C w 00 0100 initial values on: tter re ker already ated keys on s	econd known	5
14	Show how cipher A is knows the Explain cle Hint: first bair]	the meet-in-th given in Prev (plaintext, cips apply brute fo	0000 0010 0101 1010 1011 1111 0001 1001 1110 0111 1100 1101 1000 1011 0110 1000 1011 0100 1011	ttack works on. Use the rs: (1110,0 the attacker known pair	0001 0111 0000 1111 0100 1110 0110 011	table be produced of the fill Using coperation operation operation of the fill Using coperation operation	elow. The table of when encryptour keys. ipher A and the on, decrypt the control of the attack of the control of th	gives the cipiting the plaint following mo ciphertext C w 00 0100 initial values on: tter re ker already ated keys on s	econd known	5

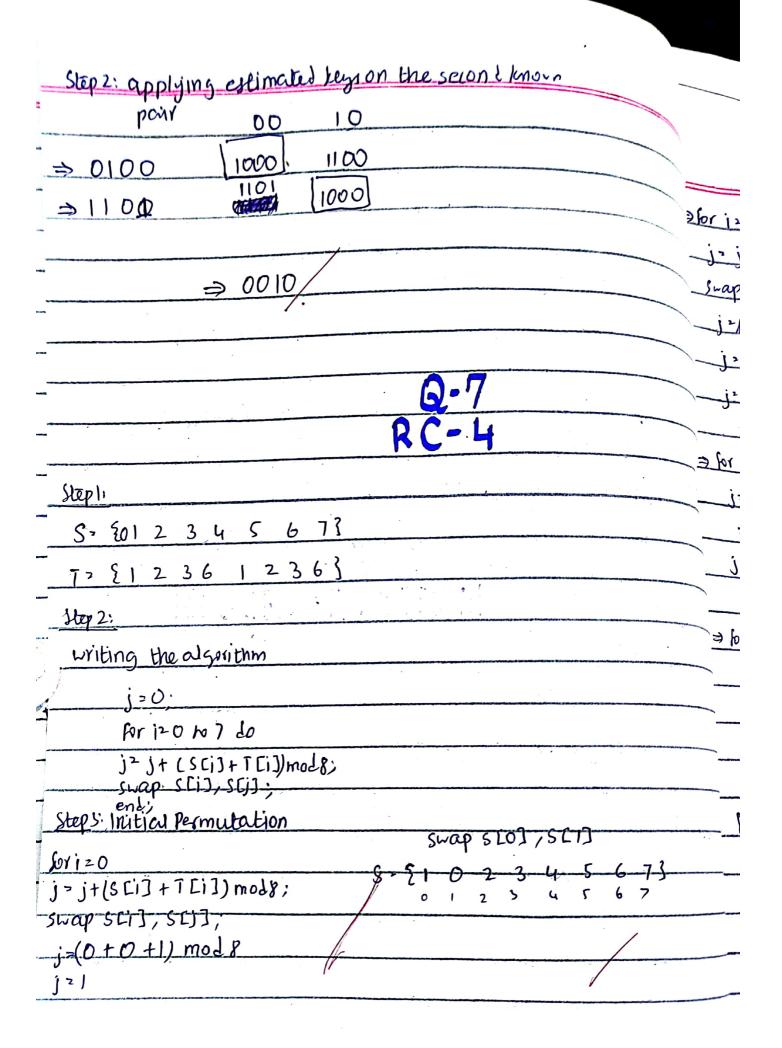
Name: Muhammad Usman Roll No: 2020-4-55 Subject: Information Securits SECURITY SERVICES The saurity services desired in computer networks are mentioned as 1. Availabilits: The system must be available to the users 24/7. bolow: 2 considertialits: The messages or conversations sent between the uses shall remain 3. Integrits: The data Hansferred on the system shall not be changed. 4 Access control: The control to the different users shall be limited based on their pusitions. * Brute Force Attack: Brute force attack is a nul and trial method used by the hacters to crack passions or find hidden rebsites. It's a very fruitful methods. In most cases, scripts containing different combinations are used in brute force method to clack assuolds.

Q4 EULERS THEOREM

	The state of the s
760 mod 47	Blocky
a 4(n) > 1 mod n	
a ((47) 2 1 mod n = a ((47))2 1 mod 47	-
760 mod 47 ~ ((26)1). 714) mod 47	· Part 2:
1.7 14 mod 47	Block 1:
128 mod 47 = 34 AM	
Hence Proved 1	Dicder.
Q5	
BLOCK CIPHER	and the same of th
	-
* Part A:	
Block 12 E (0000, 00) -1111	-
Pl= (1 xor IIII)	
20010	
Black 2 = 2 (000) 700) 20001	
2 (2 many xor 000)	-
20101/	· · · · · · · · · · · · · · · · · · ·
Block 3 ~ E (0010,00) 2)010	AND
+ (5 x0) (016	The second secon
· 0110	

Block 4 = E 10011,00) =01111	
Pu = (4 x0x0111 = 0011	
=> 0010-01-0-110-0011-AM	
	(5
# Part 2:	01 - 0101
Block 1: D(1101,00), 1101	Block 3: > (1100,00) ~ 0101
1101 XOF 0000 = 1101	IN
Bloder: 0(0100,00), 1010	Medity: 0 (\$100 \s) = 1010 \s
TOLO KOR HOL 2 OILL	1010 x02 1186 2 0110
201 0110 01	3
3 1101 0111 0001 0110 AM	1+5
	1-6
MCET	IN THE MIDDLE
MEE	11 Ine l'IIPPL
Step 1: Applying bruteforce on the know	713 poul 3
(ULD DIII)	
API ACT	
(0100,1101)	
00	01 10 11
1110 0010	1000 0011 1100
0111 [001]	0110 0010 0001
•	
00 10 ->	
10 00 ->	and any management of the first of the second secon
10 00	





	5-af 5513, 55 33	Thosage.
	j-j+ 15[1]+T[1]) mod 8; 5. 2132045673	'-2023
	The state of the s	'2023 '4Y, LAHOL
		en Ma
	j. 3 mod ?	
	1.3	The state of the s
	J	ature
	= for j22 swap \$[23,560]	The transfer of the state of th
	12 × 2 + 3) MOI	Sharananananan S
	2 8 mol 8 S2 2234 0456.71	ಕಾರ್ಪ್ ಕರ್ಷೇಶ್ ಹೆಡೆದಾರ್ಯ ಸಾಕ್ಷಿಣ ನಿರ್ದೇಶವು
	j.0	ESTERATORISME WHITE ARREST SHEET SHE
		70
	⇒ for 1=3	
	j= (0+B+6) mol 8 swap \$[3], \$E()	
	4 . 0	ggi kannsanda ili palikan magamin alamanda mansis ya kinsana nyisi sama a
	j= 8 mod 8 92 {2 3 1 6 45 573	
	J ² 6	
ar ya a ka anan a ka anan a ka a a a a a a a		
	for 124	
	j= (6+4+6) mod 8 swap s[4], 5[3]	
5-6-73	0, 19 11 12 12 1	}
s 6 7	j= 16 mods 32 (2) 45 4 7	
/	123	

swap SCBI SCOT for 105 j. (3+5+1) mod 8 82 82 3 5 4 6 (3)73 1, 2 swap SEG7, SE47 for is 6 12 5 5 4 (3) 1 6 73). (6+3+3) mod P 12 4 for 127 J2 (4+7+6) mo28 j = 17 mod 8 122