	Department of Computer Science UET Lahore, New Campus		Semester: Spring-2023
EXAM: Mid Term	CS 364-Information Security	Time Limit: 100 minutes	Total Marks: 35 Marks Obtained:

Name: Muhammad Usman Regd. No. 2020-SE-35 Section: ______

CLO1 [5]	4	CLO4 [30]	27.9

Q. No.	Questions	MARKS
1. CLO 1	List the key security services desired in computer networks. For each service, explain what the service means. confidentiality, integrity, Authenticity, availability, access control	3
2. CLO1	Define following. (attempt any one) 1. Unconditionally secure and computationally secure encryption scheme. 2. Brute Force Attack 3. Confusion and Diffusion	2
3. CLO4 6.9	1. In the DES algorithm the round key is ________ bit and the Round Input is __________bits. a) 48, 32 b) 64,32 c) 56, 24 d) 32, 32 2. In the DES algorithm the 64 bit key input is shortened to 56 bits by ignoring every 4th bit. a) True b) False 3. The DES Algorithm Cipher System consists of ___________rounds each with a round key a) 12 b) 18 c) 9 d) 16 4. The number of unique substitution boxes in DES after the 48 bit XOR operation are a) 8 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^{9} 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 8. 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	7

c) Transitions
d) Permutations

10. In AES the 4×4 bytes matrix key is transformed into a keys of size ________ bytes
a) 32
b) 64
c) 54
d) 44

11. On comparing AES with DES, which of the following functions from DES does not have an equivalent AES function?
a) f function
b) permutation p
c) swapping of halves
d) xor of subkey with function f

12. On performing the Mix Columns transformation for the sequence of bytes "77 89 AB CD" we get output
a) {01 55 EE 4A}
b) {0A 44 EF 4A}
c) {08 55 FF 3A}
d) {09 44 DD 4A}

13. Conversion of the Plaintext WILLIAMSTALLINGS to a state matrix leads to? →

W	I	T	
I	A	A	N
L	M	L	G
L	S	L	S

14. What is the Shifted Row transformation for the matrix bellow?

~~50~~	D7	AF	FE
FE	72	2B	D7
6B	77	A4	6B
AD	01	F0	63

FE	72	2B	D7
6B	77	A4	6B
AD	01	F0	63
30	D7	AF	FE

4. CLO4 — 3

1. Show that $7^{60} \equiv 34$ (mod 47. OR
2. Find multiplicative inverse using Fermat's little theorem 5 mod 19.

5. CLO4 — 5+5

P \ K	C: 00	01	10	11
0000	1111	0000	0101	0001
0001	0001	0010	1001	0111
0010	1010	0101	0111	1000
0011	0111	1010	0010	1111
0100	1000	1001	1100	0101
0101	1100	1110	1011	1010
0110	1011	0111	1110	0100
0111	0000	1111	0001	1110
1000	1110	0001	1101	0110
1001	1001	0011	1000	1011
1010	0100	1100	0000	1101
1011	0110	1101	0100	1001
1100	0101	0100	0110	0010
1101	1101	0110	1111	0000
1110	0010	1000	0011	1100
1111	0011	1011	1010	0011

Consider a block cipher, called *A*, shown in the table below. The table gives the ciphertext *C* produced when encrypting the plaintext *P* with one of the four keys.
Using cipher *A* and the following modes of operation, decrypt the ciphertext *C* with key *K*:

C	1101 0100 1100 0100
K	00

In all cases assume any initial values are 0.
a) Counter:
b) CBC:
Counter mode decryption:
$P_i = C_i \oplus E_{k_i}$ (Counter)
CBC mode decryption:
$C_0 = IV$
$P_i = D_K(C_i) \oplus C_{i-1}$

6. CLO4 — 5

Show how the meet-in-the-middle attack works by applying it against *Double-A*, where cipher *A* is given in Previous Question. Use the attack to find the key used if the attacker already knows the (plaintext, ciphertext) pairs: (1110, 0111) (0100, 1101)
Explain clearly the steps applied by the attacker and how the key is identified.
[Hint: first apply brute force on first known pairs and estimate keys, then apply estimated keys on second known pair]

7. CLO4 — 5

Consider the stream cipher RC4, but instead of the full 256 bytes, use 8 x 3-bits. That is, the state vector S is 8 x 3-bits. We will operate on 3-bits of plaintext at a time since S can take the values 0 to 7, which can be represented as 3 bits.
Assume a 4 x 3-bit key of K = [1 2 3 6]. And a plaintext P = [1 2 2 2]
Perfrom the first step (initial permutation) of RC4 and find out the state vector S.

Name: Muhammad Usman
Roll No: 2020-4E-55
Subject: Information security

Q-1
SECURITY SERVICES

The security services desired in computer networks are mentioned as below:-

1. Availability: The system must be available to the users 24/7.
2. Confidentiality: The messages or conversations sent between the users shall remain confidential.
3. Integrity: The data transferred on the system shall not be changed.
4. Access control: The control to the different users shall be limited based on their positions.

Q-2
DEFINITION

* **Brute Force Attack:**

Brute force attack is a hit-and trial method used by the hackers to crack passwords or find hidden websites. Its a very fruitful method. In most cases, scripts containing different combinations are used in brute force method to crack password.

Q4
EULERS THEOREM

$7^{60} \bmod 47$

$a^{\varphi(n)} = 1 \bmod n$

$a^{\varphi(47)} = 1 \bmod n \Rightarrow a^{\varphi(47)} = 1 \bmod 47$

$7^{60} \bmod 47 = ((7^{46})^{1} \cdot 7^{14}) \bmod 47$

$1 \cdot 7^{14} \bmod 47$

$128 \bmod 47 = 34$ Ans.

Hence Proved!

Q5
BLOCK CIPHER

Part A:

Block 1 = E(0000, 00) = 1111

P1 = (1 XOR 1111)

= 0010

Block 2 = ~~E(0001, 00) = 0001~~

= C2 ~~0110~~ XOR 0001

= 0101

Block 3 = E(0010, 00) = 1010

= C3 XOR 1010

= 0110

Block 4

⇒

Part 2:

Block 1:

Block 2:

Block 4 = E (0011, 00) = 0111

P4 = (4 XOR 0111 = 0011

⇒ ~~0010 0101 0110 0011~~ Ans

5

\# Part 2:

IV = 0000

Block 1: D(1101, 00) = 1101

1101 XOR 0000 = 1101

Block 3: D (1100, 00) = 0101

0101 XOR 0100 = 0001

Block 2: D(0100, 00) = 1010

~~1010 XOR 1101~~ = 0111

Block 4: D (0100, 00) = 1010

1010 XOR 1100 = 0110

⇒ 1101 0111 0001 0110 Ans.

Q-6
MEET IN THE MIDDLE

Step 1: Applying brute force on the known pairs

(1110, 0111) → P1, → C1

(0100, 1101) → P1, → C1

	00	01	10	11
1110	$\boxed{0010}$	1000	$\boxed{0011}$	1100
0111	$\boxed{0011}$	0110	$\boxed{0010}$	0001

00 10 →

10 00 →

Step 2: applying estimated keys on the second known pair

	00	10
⇒ 0100	$\boxed{1000}$	1100
⇒ 1100	1101	$\boxed{1000}$

⇒ 0010

Q-7
RC-4

Step 1:

S = {0 1 2 3 4 5 6 7}

T = {1 2 3 6 1 2 3 6}

Step 2:

writing the algorithm

j = 0;
for i = 0 to 7 do
j = j + (S[i] + T[i]) mod 8;
swap S[i], S[j];
end;

Step 3: Initial Permutation

for i = 0
j = j + (S[i] + T[i]) mod 8;
swap S[i], S[j];
j = (0 + 0 + 1) mod 8
j = 1

swap S[0], S[1]

S = {1 0 2 3 4 5 6 7}
0 1 2 3 4 5 6 7

⇒ for i =
j = j
swap
j =
j =
j =
⇒ for
j
j
⇒ fo

second known

, S[7]

4 5 6 7}

4 5 6 7

⇒ for i = 1

j = j + (S[i] + T[i]) mod 8;

swap S[i], S[j];

j = [redacted] (1 + 0 + 2) mod 8

j = 3 mod 8

j = 3

swap S[1], S[3]

S = {1 3 2 0 4 5 6 7}

0 1 2 3 4 5 6 7

⇒ for i = 2

j = (3 + 2 + 3) mod 8

= 8 mod 8

j = 0

swap S[2], S[0]

S = {2 3 1 0 4 5 6 7}

0 1 2 3 4 5 6 7

⇒ for i = 3

j = (0 + 0 + 6) mod 8

j = 6 mod 8

j = 6

swap S[3], S[6]

S = {2 3 1 6 4 5 3 7}

0 1 2 3 4 5 6 7

for i = 4

j = (6 + 4 + 6) mod 8

j = 16 mod 8

j = 3

swap S[4], S[3]

S = {2 3 1 4 6 5 3 7}

0 1 2 3 4 5 6 7

for i = 5

j = (3 + 5 + 2) mod 8

j = 2

swap S[5], S[2]

S = { 2 3 5 4 6 1 3 7 }

0 1 2 3 4 5 6 7

for i = 6

j = (6 + 3 + 3) mod 8

j = 4

swap S[6], S[4]

{ 2 3 5 4 3 1 6 7 }

for i = 7

j = (4 + 7 + 6) mod 8

j = 17 mod 8

j = 2

swap S[7], S[2]

{ 2 2 3 7 4 3 1 6 5 }