Eastern Mediterranean University
Computer Engineering Department
CMSE-353 Security of Software Systems
Midterm Exam

Three A4 sheets of handwritten paper may be used for your help. Photocopies, printouts, etc. are not allowed! Electronic devices are not allowed

Duration: 110 Minutes **April 10, 2017**

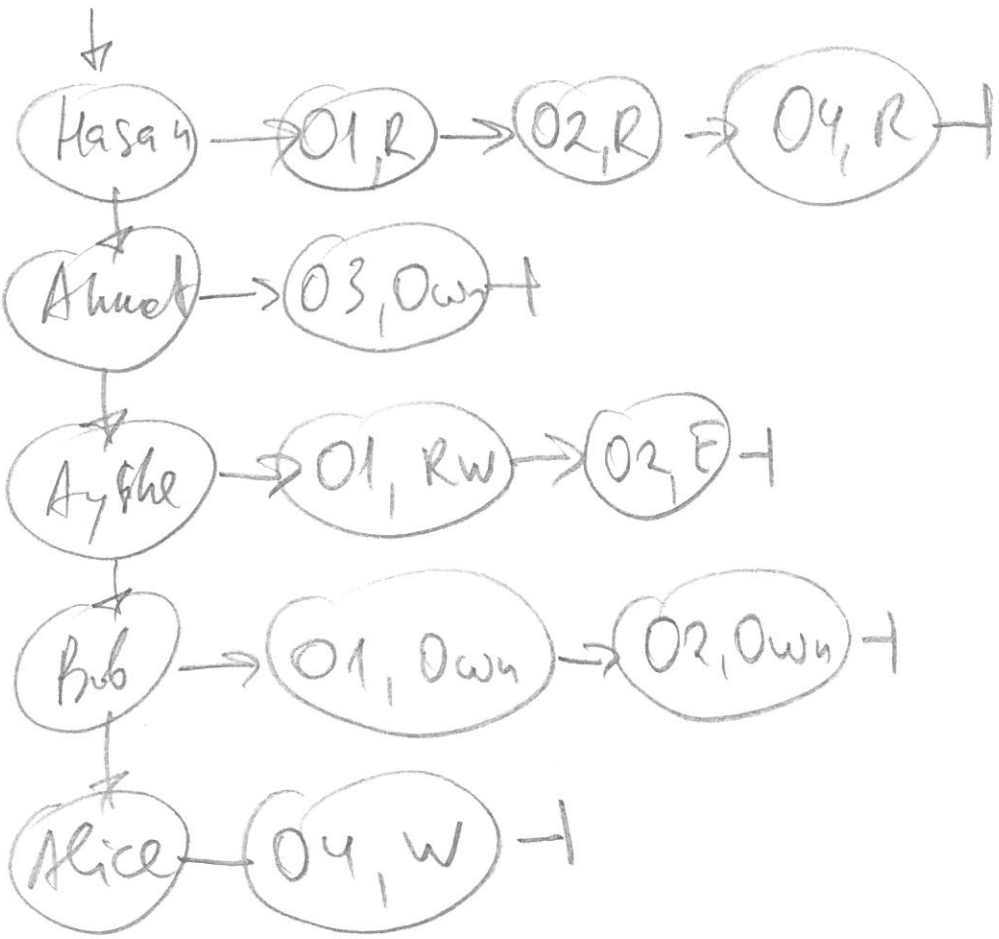
StdId_____ **Std Name**_____

Instructor Alexander Chefranov

Totally 6 questions, 9 pages

1.	2.	3.	4.	5.	6.	Total
10	15	15	20	20	20	100

Q1. (10 points). Consider a system with the users Hasan, Ahmet, Ayshe, Bob, and Alice, objects O1, O2, O3, O4. Hasan can read O1, O2, and O4, Ahmet is an owner of O3, Ayshe can read and write O1 and execute O2, Bob is an owner of O1 and O2, and Alice can write O4. Construct a Capability List to keep the privileges described.



Q2. (15 points). Explain Social engineering methods

- Pretexting (5 points)

Impersonating of a valid user when calling to a service provider for a password change

- Baiting (5 points)

Attracting people by something so that they themselves install some software together with malicious codes about which they do not know

- Quid pro quo (5 points)

Use of people's gratitude for doing some-thing useful for them to get from them their secret data

Q3. (15 points). Encrypt and decrypt back the following English language message "Hello, World!" using substitution cipher with a key phrase: "The head of a key US congressional investigation has temporarily stepped down". Construct a substitution table. Give necessary explanations.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
T	H	E	A	D	O	F	K	Y	U	I	S	C	N	G	R	I	L	V	M	P

20	21	22	23	24	25
u	v	w	x	y	z
W	B	J	Q	X	Z

H	E	L	L	O	W	O	R	L	D
D	C	C	R	J	R	V	C	I	A

Encrypt

Decrypt

Q4. (20 points). Using Hill cipher with size 2 block, encrypt and decrypt back the **first** block of the following message "How are you?" preserving blanks, dots, and question marks. What numerical codes of the symbols you use? Construct an appropriate key matrix. What conditions must be satisfied by the key matrix? What modulo value shall be used? Show that the matrix you construct satisfies the conditions. Calculate inverse of the key matrix. Give necessary explanations.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

v	w	x	y	z	␣	.	?
21	22	23	24	25	26	27	28

$n = 29$

$K = \begin{vmatrix} 3 & 3 \\ 1 & 2 \end{vmatrix}$, $\det K = 3 \neq 0 \bmod 29$

$\gcd(3, 29) = 1$

$(\det K)^{-1} = 3^{-1} \bmod 29 = 10$

X	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
3x	3	6	9	12	15	18	21	24	27	1																

$K^{-1}_{ij} = (-1)^{i+j} D_{ji} (\det K)^{-1}$; $K_{11} = (-1)^2 \cdot 2 \cdot 10 \bmod 29 = 20$

$K^{-1}_{21} = (-1)^{2+1} D_{12} \cdot 10 \bmod 29 = -1 \cdot 10 = -10 = 19$

$K^{-1}_{12} = (-1)^{1+2} D_{21} \cdot 10 \bmod 29 = -3 \cdot 10 = -1 = 28$

$K^{-1}_{22} = (-1)^{2+2} D_{22} \cdot 10 \bmod 29 = 3 \cdot 10 = 1$

$K \cdot K^{-1} = \begin{pmatrix} 3 & 3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 20 & 28 \\ 19 & 1 \end{pmatrix} = \begin{pmatrix} 60+57 & 84+3 \\ 20+38 & 28+2 \end{pmatrix} = \begin{pmatrix} 117 & 87 \\ 58 & 30 \end{pmatrix}$

$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$C = K \cdot P = \begin{pmatrix} 3 & 3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 7 \\ 14 \end{pmatrix} = \begin{pmatrix} 21+42 \\ 7+28 \end{pmatrix} = \begin{pmatrix} 63 \\ 35 \end{pmatrix} \bmod 29 = \begin{pmatrix} 5 \\ 6 \end{pmatrix}$

$P = (HO) =$

$= (7, 14)$; $C = (FG)$;

$P = K^{-1} C = \begin{pmatrix} 20 & 28 \\ 19 & 1 \end{pmatrix} \begin{pmatrix} 5 \\ 6 \end{pmatrix} = \begin{pmatrix} 100+168 \\ 95+6 \end{pmatrix} =$

$= \begin{pmatrix} 268 \\ 101 \end{pmatrix} \bmod 29 = \begin{pmatrix} 7 \\ 14 \end{pmatrix} = (HO)$

Q5. (20 points)..DES round key generation procedure is described in the text below and Figure 3.8 from the Lecture notes:

"KEY GENERATION

Input key has 64 bits. But each 8th bit is not used: bits 8,16,24,32,40,48,56,64 are not further used. The 56-bit key is first subjected to permutation Permuted Choice 1:

Permuted Choice 1 (PC-1)
57 49 41 33 25 17 9
1 58 50 42 34 26 18
10 2 59 51 43 35 27
19 11 3 60 52 44 36
63 55 47 39 31 23 15
7 62 54 46 38 30 22
14 6 61 53 45 37 29
21 13 5 28 20 12 4

The resulting 56-bit key is then treated as two 28-bit quantities, labeled C0 and D0. At each round, C_{i-1} and D_{i-1} are separately subjected to a circular left shift, or rotation, of 1 or 2 bits as governed by the following:

Schedule of Left Shifts															
Round number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

These shifted values serve as input to the next round. They also serve as input to Permuted Choice 2, which produces a 48-bit output that serves as input to the function $F(R_{i-1}, K_i)$.

Permuted Choice 2 (PC-2)
14 17 11 24 1 5 3 28
15 6 21 10 23 19 12 4
26 8 16 7 27 20 13 2
41 52 31 37 47 55 30 40
51 45 33 48 44 49 39 56
34 53 46 42 50 36 29 32

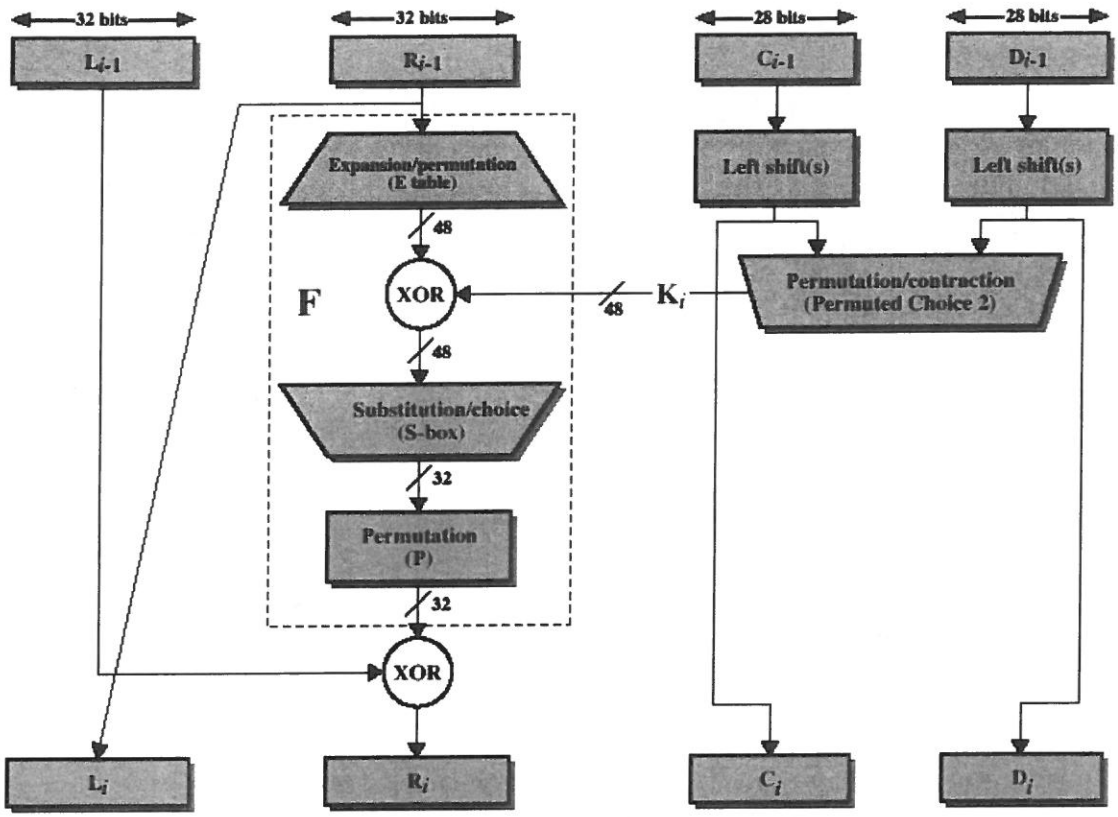
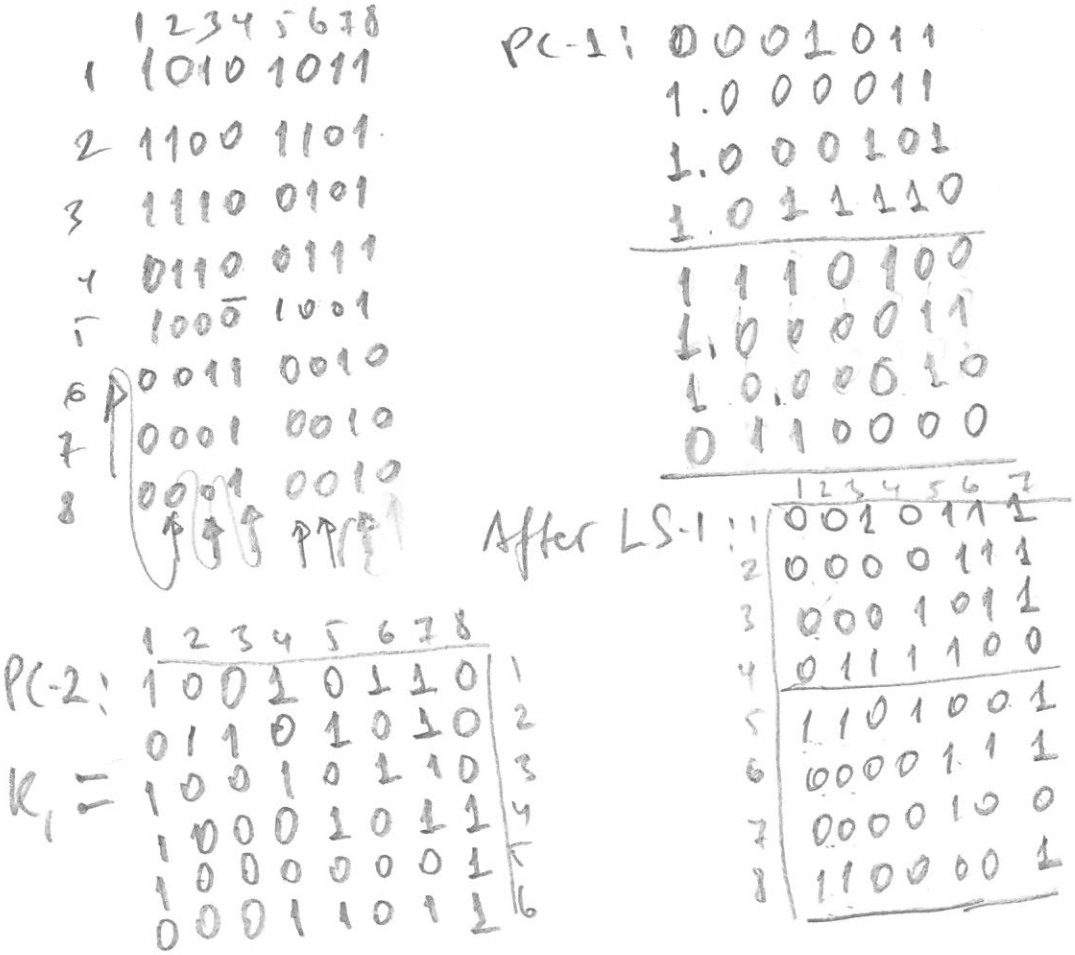


Figure 3.8 Single Round of DES Algorithm

"

A master 64-bit key, *K*, specified by a user in hexadecimal form is as follows, K=0xabcde56789321212. Get the first round-key, K_1. Give necessary explanations



Q6. (20 points). Assume that 48-bit result of XOR with the round-key, Ki, in Figure 3.8, is as follows, Res=0xabdc56f80abc, in hexadecimal. What are the 4 bits output by S-box S3.
Expansion/permutation table from Figure 3.8

Expansion/Permutation (E table)		
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

1 1010 | S1
2 1011 S2
3 1101
4 1100 S3
5 0101
6 0110
7 1111
8 1000
9 0000
10 1010
11 1011
12 1100

Figure 3.9 illustrating work of S-boxes

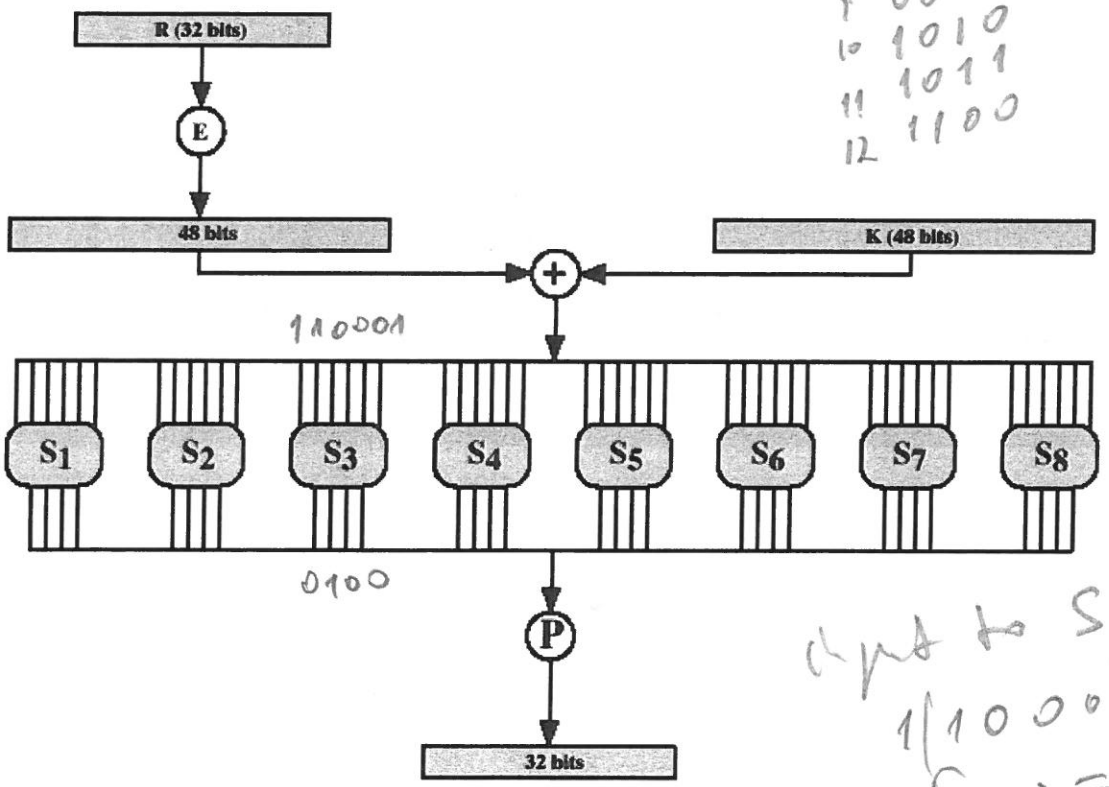


Figure 3.9 Calculation of F(R, K)

and Table 3.3 showing each S-box

input to S3 is
1 1000 1
row = 3
column = 8
output of S3 =
$= 4_{10} = 0100_2$

Table 3.3 Definition of DES S-Boxes

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
	0	1	2	3	4	5	6	7	8							
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11