A. CHEHAB

FACULTY OF ENGINEERING AND ARCHITECTURE
AMERICAN UNIVERSITY OF BEIRUT
SPRING 2014-2015
MIDTERM

CRYPTOGRAPHY AND NETWORK SECURITY (EECE 455/632)

NAME: ID:

CLOSED BOOK (90 MINUTES)

WRITE YOUR **NAME** AND **ID NUMBER** IN THE SPACE PROVIDED ABOVE.

PROVIDE YOUR **ANSWERS** IN THE SPACE PROVIDED ON THE QUESTION SHEET.

THE **SCRATCH** BOOKLET **WILL NOT** BE CONSIDERED IN GRADING.

Problem	Total Points	Scored Points
1	8	
2	8	
3	8	
4	10	
5	10	
6	10	
7	12	
8	8	
9	10	
10	8	
11	8	
TOTAL	100	

Problem 1 [8 points]

We are using the *Vigenere* cipher with the key "**MIDTERM**". Note that the *Vigenere* Tableau is attached to the exam.

a) Encrypt the plaintext word "**VERY**". **Ciphertext =** _____

b) Decrypt the ciphertext word "**TIUW**". **Plaintext =** _____

Problem 2 [8 points]

Encrypt the message "**APPLES**" using the *Playfair* cipher with the key "**MIDTERM**".

Ciphertext = _____

Problem 3 [8 points]

The most two frequent letters of the English alphabet are '**E**' and then '**T**'. We used an affine cipher (***C = aP + b mod 26***). It turned out, after encryption, that the two frequent letters became '**M**' and then '**O**'. Break the affine cipher by computing the key (a, b). (*Remember 'A' = 0, ..., 'Z' = 25. You can solve this by trial and error, but show muscle and use Euclid to find the inverse of a number!*)

a = _____ **b =** _____

Problem 4 [10 points]

The ciphertext "**CHUH**" was encrypted using the *affine cipher:* ***7x + 5 mod 26***. Find the plaintext. (*Don't forget: Letter 'A' = 0, 'B' = 1, ..., 'Z' = 25, and remember how useful Euclid is*)

Plaintext =

Problem 5 [10 points]

Decrypt "**DLJX**" using the Hill cipher with the key: $\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$. **Plaintext:** _____

Problem 6 (10 points)

What is the inverse of **{59}** in **GF(2^8)**. (The irreducible polynomial is: $X^8 + X^4 + X^3 + X + 1$). Express your answer as a **polynomial** and as a **Hexadecimal** number.

{59^{-1}} as *polynomial* = _____; as *Hex* = _____

Problem 7 (10 points)

Compute the bits number 2, 17, 36, and 56 of the output L_1R_1 of the first round of DES, assuming that the input message block consists of **all zeros**, and the key consists of **all ones**. Note that the DES S-Boxes and the Permutation function (P) are attached to the exam.

BIT 2	BIT 17	BIT 36	BIT 56

Problem 8 (10 points)

a. Let X' be the bitwise complement of X. When using DES, if we have that $Y = E(K, X)$, then if we complement the text and we complement the key, what would be the result of encryption. In other words what would be *E(K', X')*? *(Note: only trace one round)*

E(K', X') = __ ____

b. The brute force attack on DES requires searching a key space of 2^{56}. Does the result of a) change that and why?

Yes / No. Why: __

_ _____

Problem 9 [8 points]

Compute the first and second 4x4 Round Key Matrices (W[0,3] and W[4,7]) produced by the key expansion procedure of AES, which is attached to the test, when all original key bytes are in [**45**] **(in Hexadecimal**, i.e. **[0100 0101] in binary). Show ALL results as "States" in Hexadecimal**.

W[0]	W[1]	W[2]	W[3]

W[4]	W[5]	W[6]	W[7]

Problem 10 (10 points)

Using AES, we have in *Hexadecimal* the plaintext {12121212 23232323 45454545 56565656} and the key {77777777777777777777777777777777}. Note that 77(in hex) is actually 0111 0111

a. Show the original content of the state displayed as a 4x4 matrix (below).

b. Show the value of the state after initial AddRoundKey

c. Show the value of the state after SubBytes. (The S-Box is attached to the exam)

d. Show the value of the state after ShiftRows

Original State				After Round Key			

After Substitution				After Shift Rows			

Problem 11 [8 points]

Compute the polynomial product below in GF(2^8) with $m(x) = x^8+x^4+x^3+x+1$

$$P(x) = (x^6+x^5+x^2+x+1) \times (x^6+x^2+x)$$

P P(x) as *polynomial* = _____

P(x) as *Hex* = _____

	Plaintext																								
	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

(a) S-box

	y															
x	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

```
KeyExpansion( byte key[16], word w[44])
{   word temp;
    for(i=0; i<4; i++)
        w[i] = (key[4*i], key[4*i+1], key[4*i+2], key[4*i+3]);
    for(i=4; i<44; i++)
    {   temp = w[i-1];
        if(i mod 4 == 0)
            temp = SubWord(RotWord(temp)) xor Rcon[i/4];
        word[i] = temp xor w[i-4];
    }
}
```

j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

(c) Expansion Permutation (E)

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

(d) Permutation Function (P)

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

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

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