A. CHEHAB

FACULTY OF ENGINEERING AND ARCHITECTURE
AMERICAN UNIVERSITY OF BEIRUT
FALL 2009-2010

MIDTERM SOLUTION

CRYPTOGRAPHY AND COMPUTER SECURITY (EECE 632)

November 25, 2009

NAME: _____ ID: _____

CLOSED BOOK (90 MINUTES)

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

Problem 1 (10 points)

Decipher the following ciphertext obtained by applying the Vigenere cipher with the key "MIDTERM". Ciphertext = "EPDDMIM". Note that the Vigenere tableau is attached to the exam.

Solution: SHAKIRA

Problem 2 (10 points)

Suppose we have 4 extra characters and we work mod 30 instead of 26 for affine ciphers. How many keys are possible? Solution: **8 x 30 = 240**

Problem 3 (10 points)

Encrypt the message "SIMPLE" using the Playfair cipher with the key "LEBANON"
Solution: RK PH EB

Problem 4 (10 points)

The ciphertext "MXT" was encrypted using the affine function 5x + 3 mod 26. Find the plaintext.

Solution: x = 21(y-3) ➔ HEY

Problem 5 (12 points)

The ciphertext TG was encrypted by a Hill cipher with matrix: $\begin{bmatrix} 15 & 14 \\ 2 & 3 \end{bmatrix}$. Find the plaintext.

Solution: Determinant = 17, inverse = 23, inverse matrix is $\begin{bmatrix} 17 & 16 \\ 6 & 7 \end{bmatrix}$ **➔ DA**

Problem 6 (12 points)

What is the inverse of {56} in GF(2^8). (The irreducible polynomial is $X^8 + X^4 + X^3 + X + 1$).

Solution: 87

Problem 7 (12 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.

L1 = 0 0 … 0 **Bit2 = 0; Bit17 = 0; Bit36 = 1; Bit56 = 1**

Problem 8 (14 points)

Using AES, we have in hexadecimal the plaintext {000102030405060708090A0B0C0D0E0F} and the key {12121212121212121212121212121212}. Note that 12(in hex) is actually 00010010

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

00	04	08	0C	12	16	1A	1E	C9	47	A2	72	C9	47	A2	72
01	05	09	0D	13	17	1B	1F	7D	F0	AF	C0	F0	AF	C0	7D
02	06	0A	0E	10	14	18	1C	CA	FA	AD	9C	AD	9C	CA	FA
03	07	0B	0F	11	15	19	1D	82	59	D4	A4	A4	82	59	D4

Problem 9 (10 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 when the 128-bit key consist of a string of consecutive ones and zeros in binary starting from a 1. Show the results in hexadecimal. (The key expansion algorithm is attached to the exam)

AA	AA	AA	AA
AA	AA	AA	AA
AA	AA	AA	AA
AA	AA	AA	AA

07	AD	07	AD
06	AC	06	AC
06	AC	06	AC
06	AC	06	AC

Previous:

1. Find plaintext using key (YIUAES) and ciphertext (MIDTER)
2. The affine cipher question we got in the assignment
3. Playfair key (BEIRUT) encrypt dayrol
4. Find plaintext of UCR using affine cipher (a=9 and b=2)
5. Decrypt YI using Hill cipher with H=[15 13; 2 3]
6. Find multiplicative inverse of {76} in GF(2^8)
7. Problem 3.13 in the book
8. A question about AES similar to assignment but without mixColumn
9. A question about key expansion (similar to the assignment)