Tanner Krebs, Gerardo Lopez, William Thornton
Math 314
9/28/17

COSC/MATH - 314

Assignment 4

Problem 1 Using the Baby DES cryptosystem with 3 rounds, encrypt the plaintexts 110011000000, and 010101000000. Use the key K = 001100011. Show the outcome of each round. More precisely, for each of the two encryptions show:

L_0 R_0
L_1 R_1 , K_1
L_2 R_2 , K_2
and
L_3 R_3 , K_3

Separately (that is after presenting the above results), also show the work so that in case you did mistakes you can get partial credit.

Solution:

	$plaintext1$	$plaintext2$
	110011000000	010101000000
K_1	00110001	00110001
K_2	01100011	01100011
K_3	11000110	11000110
L_0	110011	010101
R_0	000000	000000
L_1	000000	000000
R_1	000011	100101
L_2	000011	100101
R_2	111100	000000
L_3	111100	000000
R_3	110011	100110

So after 3 rounds, the plaintext 1100 1100 0000 becomes the encrypted message, $R_3L_3 = 1100\ 1111\ 1100$
So after 3 rounds, the plaintext 0101 0100 0000 becomes the encrypted message, $R_3L_3 = 1001\ 1000\ 0000$

In order to get the above results, we need to note a couple of parameters.

XOR chart:

$\oplus$	0	1
0	0	1
1	1	0

and the S-boxes:

S_1	0	1	2	3	4	5	6	7
0	101	010	001	110	011	100	111	000
1	001	100	110	010	000	111	101	011

S_2	0	1	2	3	4	5	6	7
0	100	000	110	101	111	001	011	010
1	101	011	000	111	110	010	001	100

To start, we need to establish the Keys such that we get K_1, K_2, and K_3.

The 9 bits of the key are: 001 100 011

To get K_1 we use the 8 bits to the left so we get: 0011 0001

To get K_2 we rotate the key by 1 bit and use the 8 bits to the left, so we get: 0110 0011

To get K_3 we rotate the key again by 1 bit and use the 8 bits to the left, so we get: 1100 0110

Let's start with the first plaintext.

key: 001100011
message: 110011000000

Round 1 ($i = 0$)

$L_0 = 110\ 011$, $R_0 = 000\ 000$, and $K_1 = 0011\ 0001$
$E(R_0) = 0000\ 0000$
$E(R_0) \oplus K_1 = 0000\ 0000 \oplus 0011\ 0001 = 0011\ 0001$
$S_1(0011) = 110$
$S_2(0001) = 000$
$f(R_0, K_1) = 110\ 000$
$f(R_0, K_1) \oplus L_0 = 110\ 000 \oplus 110\ 011 = 000\ 011$
$L_i = R_{i-1} = L_1 = R_0 = 000\ 000$
$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) = L_0 \oplus f(R_0, K_1) = R_1 = 000\ 011$

Round 2 ($i = 1$)

$L_1 = 000\ 000$, $R_1 = 000\ 011$, and $K_2 = 0110\ 0011$
$E(R_1) = 0000\ 0011$
$E(R_1) \oplus K_2 = 0000\ 0011 \oplus 0110\ 0011 = 0110\ 0000$
$S_1(0110) = 111$
$S_2(0000) = 100$
$f(R_1, K_2) = 111\ 100$
$f(R_1, K_2) \oplus L_1 = 111\ 100 \oplus 000\ 000 = 111\ 100$
$L_i = R_{i-1} = L_2 = R_1 = 000\ 011$
$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) = L_1 \oplus f(R_1, K_2) = R_2 = 111\ 100$

Round 3 ($i = 2$)

$L_2 = 000\ 011$, $R_2 = 111\ 100$, and $K_3 = 1100\ 0110$
$E(R_2) = 1111\ 1100$
$E(R_2) \oplus K_3 = 1111\ 1100 \oplus 1100\ 0110 = 0011\ 1010$
$S_1(0011) = 110$
$S_2(1010) = 000$
$f(R_2, K_3) = 110\ 000$
$f(R_2, K_3) \oplus L_2 = 110\ 000 \oplus 000\ 011 = 110\ 011$
$L_i = R_{i-1} = L_3 = R_2 = 111\ 100$
$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) = L_2 \oplus f(R_2, K_3) = R_3 = 110\ 011$

So after 3 rounds, the plaintext 1100 1100 0000 becomes the encrypted message, $R_3L_3 = 1100\ 1111\ 1100$

Now let's do the second plaintext.

key: 001100011
message: 010101000000

Round 1 $(i = 0)$

$L_0 = 010\ 101$, $R_0 = 000\ 000$, and $K_1 = 0011\ 0001$
$E(R_0) = 0000\ 0000$
$E(R_0) \oplus K_1 = 0000\ 0000 \oplus 0011\ 0001 = 0011\ 0001$
$S_1(0011) = 110$
$S_2(0001) = 000$
$f(R_0, K_1) = 110\ 000$
$f(R_0, K_1) \oplus L_0 = 110\ 000 \oplus 010\ 101 = 100\ 101$
$L_i = R_{i-1} = L_1 = R_0 = 000\ 000$
$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) = L_0 \oplus f(R_0, K_1) = R_1 = 100\ 101$

Round 2 $(i = 1)$

$L_1 = 000\ 000$, $R_1 = 100\ 101$, and $K_2 = 0110\ 0011$
$E(R_1) = 1010\ 1001$
$E(R_1) \oplus K_2 = 1010\ 1001 \oplus 0110\ 0011 = 1100\ 1010$
$S_1(1100) = 000$
$S_2(1010) = 000$

$f(R_1, K_2) = 000\ 000$
$f(R_1, K_2) \oplus L_1 = 000\ 000 \oplus 000\ 000 = 000\ 000$
$L_i = R_{i-1} = L_2 = R_1 = 100\ 101$
$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) = L_1 \oplus f(R_1, K_2) = R_2 = 000\ 000$

Round 3 ($i = 2$)

$L_2 = 100\ 101$, $R_2 = 000\ 000$, and $K_3 = 1100\ 0110$
$E(R_2) = 0000\ 0000$
$E(R_2) \oplus K_3 = 0000\ 0000 \oplus 1100\ 0110 = 1100\ 0110$
$S_1(1100) = 000$
$S_2(0110) = 011$
$f(R_2, K_3) = 000\ 011$
$f(R_2, K_3) \oplus L_2 = 000\ 011 \oplus 100\ 101 = 100\ 110$
$L_i = R_{i-1} = L_3 = R_2 = 000\ 000$
$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) = L_2 \oplus f(R_2, K_3) = R_3 = 100\ 110$

So after 3 rounds, the plaintext 0101 0100 0000 becomes the encrypted message, $R_3L_3 = 1001\ 1000\ 0000$

Problem 2 In this part you are asked to execute the differential attack on Baby DES with 3 rounds that we discussed in class. For that use the above two plaintexts (i.e., 110011000000 and 010101000000) and the ciphertexts that you have obtained in part (1). Next run the differential attack using the method discussed in class. You should, of course, pretend that you do not know the key K. Show all the steps. Do all these for the left half and the right half and derive the possibilities for K_3.

You need to present the following:

- The 6-bit string denoted A in the description of the differential attack below.
- The 8-bit string E(L_3) + E(L_3*).
- The 16 pairs of inputs having the desired XOR (for the left half and the right half),

- The pairs that yield after the S-box substitutions the desired output (for the left half and the right half),
- List all the possibilities for K_3.
- List all the possibilities for K. If you worked correctly, the actual K should be on this list.

Organize your write-up neatly so that the grader can follow what you did.

Solution: