Cryptography HW 1

Shizhi Gu
661544785

1. **For the simplified DES, consider Sbox S_0 and show how DiffCrypto attack would work.**

First, create a plaintext pair (P, P*) such that (P XOR P*) = A. Then possible XORs are

Ouput: 0 1 2 3
Occurs: 6 2 6 2

A -> 1 has 2 occurrences. These input pairs are dual: (α, β) and (β, α).

I wrote a Python script to construct the S0 differential distribution table. Then I discover these inputs as 3, 9

X1 = 3 = 0011, X2 = 9 = 1001
3 XOR 9 = 1010 = A

Y1 = S0(3) = 0010, Y2 = S0(9) = 0011
Y1 XOR Y2 = 1

Also, I list all the possible input values for S0 box with input XOR A:
A -> 0 [8, 2, 4, 14]
A -> 1 [9, 3]
A -> 2 [1, 11]
A -> 3 [0, 5, 6, 7, 10, 12, 13, 15]

Suppose we know two inputs to S0 as 1 and B which XORs to A, and the output XOR as 0.

Since S1I = S1E XOR S1K
We have S1K = S1I XOR S1E
Which gives:

8 XOR 1 = 9	8 XOR B = 3
2 XOR 1 = 3	2 XOR B = 9
4 XOR 1 = 5	4 XOR B = F
E XOR 1 = F	E XOR B = 5

Thus, possible keys are {9, 3, 5, F}

Furthermore, suppose we know two inputs to S0 as 9 and 3 which XORs to A, and the output XOR as 2

1 XOR 9 = 9
11 XOR 9 = C
6 XOR 9 = F
7 XOR 9 = E
A XOR 9 = 3
C XOR 9 = 5

D XOR 9 = 4
F XOR 9 = 6

Thus, possible keys are {9, C, E, 4, 6, 3, 5, F}

We can see that, there are four K values in the intersection. Therefore, we need to go back to the first step and generate additional data.

The process is the same as what I showed above.

At last, we can get a single key value in intersections, and this single key value is the correct key.

2. Consider the crypto system below and compute H(K|C)

Pc(1) = 1/3 * 1/2 + 1/2 * 1/4 = 1/6 + 1/8 = 7/24

Pc(2) = 1/3 * 1/4 + 1/6 * 1/2 + 1/2 * 1/2 = 1/12 + 1/12 + 1/4 = 5/12

Pc(3) = 1/3 * 1/4 + 1/6 * 1/4 = 1/12 + 1/24 = 1/8

Pc(4) = 1/6 * 1/4 + 1/2 * 1/4 = 1/24 + 1/8 = 1/6

H(P) = -((1/3) * log_2(1/3) + (1/6) * log_2(1/6) + (1/2) * log_2(1/2)) ≈ 1.46

H(K) = -((1/2) * log_2(1/2) + (1/4) * log_2(1/4) + (1/4) * log_2(1/4)) = 1.5

H(C) = -((7/24) * log_2(7/24) + (5/12) * log_2(5/12) + (1/8) * log_2(1/8) + (1/6) * log_2(1/6)) ≈ 1.85

H(K|C) = H(K) + H(P) - H(C) = 1.5 + 1.46 - 1.85 = 1.11