Cryptography & Network Security I - Fall 2018

Homework 1 Part 2

Charles Schmitter

September 24, 2018

Q1. For the simplified DES, consider Sbox S_0 and show how DiffCrypto attack would work.

A.

With the simplified DES, at the step where Sbox S_0 is used, there exists $S0_E$ which is the expanded 4-bit input (expanded to 8-bits) and the 8-bit subkey $S0_K$. These two values are XORed with one another to produce the input to Sbox S_0 as well as Sbox S_1. Since we are required to only look at Sbox S_0, we will only look at the first 4 bits of this XORed value (these first 4 bits are the bits that go on to Sbox S_0.

For a differential cryptanalysis attack to work, we must first construct the differential distribution table for S_0. Once constructed, we can consider a particular input XOR to evaluate. We will take a look at the input XOR value of F. The following pairs of values XOR to F:

$$(15, 0); (10, 5); (12, 3); (9, 6); (14, 1); (7, 8); (2, 13); (4, 11)$$

After putting each pair through Sbox S_0, we find the following mappings of pairs to output XORs:

- $(9, 6) \to 1$
- $(4, 11) \to 2$
- $(15, 0); (10, 5); (12, 3); (14, 1); (7, 8); (2, 13) \to 3$

With this in mind, suppose we have two inputs to S_0: 12 and 3 (which XOR to F) and the output XOR 1. We also know the following:

$$S0_K = S0_I \oplus S0_E$$

With all of this known, we can then find:

- $12 \oplus 9 = 5$
- $12 \oplus 6 = 10$
- $3 \oplus 9 = 10$
- $3 \oplus 6 = 5$

We therefore know potential keys are in the set:

$$\{5, 10\}$$

We can do this process again. Suppose we have two inputs to S_0: 10 and 5 (which again XOR to F) and the output XOR 2. We can then similarly find:

- $10 \oplus 4 = 14$
- $10 \oplus 11 = 1$
- $5 \oplus 4 = 1$
- $5 \oplus 11 = 14$

We then end up with the result set:

$$\{1, 14\}$$

We take this result set and take the intersection of this set with the result set of the last findings. We then have a set of potential keys:

$$\{1, 5, 10, 14\}$$

We can repeat this DiffCrypto process with different input XORs and different output XORs, eventually determining what the key is precisely. This is how a DiffCrypto attack would work, with Sbox S_0 being used as an example.

Q2. Consider the crypto system and compute $H(K|C)$.

A.

To compute $H(K|C)$, we can use the the theorem: $H(K|C) = H(K) + H(P) - H(C)$. We will start with computing $H(P)$, the entropy of the plaintext component:

$$H(P) = -\sum_{i=1}^{n} p_i * log_2 * p_i$$

where n is the number of plaintexts and p_i is the probability of each plaintext. So:

$$H(P) = -[\tfrac{1}{3}log_2\tfrac{1}{3} + \tfrac{1}{6}log_2\tfrac{1}{6} + \tfrac{1}{2}log_2\tfrac{1}{2}] = 1.459$$

Next, we will similarly compute the entropy of the key component:

$$H(K) = -\sum_{i=1}^{n} p_i * log_2 * p_i$$

where n is the number of keys and p_i is the probability of each key. So:

$$H(K) = -[\tfrac{1}{2}log_2\tfrac{1}{2} + \tfrac{1}{4}log_2\tfrac{1}{4} + \tfrac{1}{4}log_2\tfrac{1}{4}] = 1.5$$

Finally, we will compute the entropy of the ciphertext component. To compute the probability of each ciphertext, we will use:

$$P_C(y) = \sum P_K(k) * P_P(d_k(y)) \text{ where } \{k : y \in C(k)\}$$

Below are the probabilties computed for each ciphertext in the set $\{1, 2, 3, 4\}$:

- $P_C(1) = \frac{7}{24}$

- $P_C(2) = \frac{5}{12}$
- $P_C(3) = \frac{3}{24}$
- $P_C(4) = \frac{1}{6}$

Now we can use the entropy formula as used in computing $H(P)$ and $H(K)$:

$$H(C) = -[\frac{7}{24}log_2\frac{7}{24} + \frac{5}{12}log_2\frac{5}{12} + \frac{3}{24}log_2\frac{3}{24} + \frac{1}{6}log_2\frac{1}{6}] = 1.851$$

We will finalize this problem by using the theorem as stated at the start of the solution:

$$H(K|C) = H(K) + H(P) - H(C) = 1.459 + 1.5 - 1.851 = 1.108$$