Cryptography and Security Course (Cryptography Part)

Midterm Solution

Preliminaries and Brute Force Attacks

1. The block-cipher DES is based on a Feistel scheme.

2. The decryption is depicted in Figure 1.

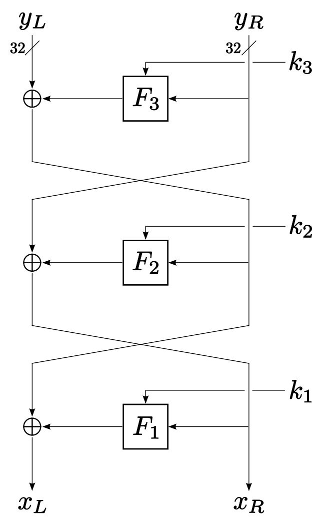

Figure 1: Inversion of a 3-round Feistel scheme.

3. An exhaustive key search on a set of size N has an average complexity of $\frac{N+1}{2}$ encryptions. Since $N = 2^{96}$, we get

$$\frac{2^{96}+1}{2} \approx 2^{95}.$$

4. Obviously, we know that at least one key (the right one) is displayed. It remains to estimate the probability that any wrong key is displayed. Let $(x_1, y_1), \ldots, (x_t, y_t)$ be the given witnesses. We idealize Ψ by the uniform random permutation C^*. So, we get

$$\Pr[\mathsf{C}^*(x_i) = y_i \text{ for } i = 1, \ldots, t] \approx 2^{-64t},$$

which shows that the number of wrong keys which are displayed in average is given by

$$\frac{2^{96}-1}{2^{64t}} \approx 2^{96-64t}.$$

Thus, the total number of keys which are displayed in average is $1 + 2^{96-64t}$. From this, one deduce that $t \geq 2$ ensures with large probability that no wrong key is displayed.

5. We can perform a meet-in-the-middle attack after the first round. Let (x, y) be a given plaintext-ciphertext pair. We denote the *ith* round of Ψ by R_i for $i = 1, 2, 3$. We construct a table composed of the pairs $(k_1, R_1(k_1, x))$ for all possible subkeys $k_1 \in \{0,1\}^{32}$. Then, for any k_2 and k_3 in $\{0,1\}^{32}$, we compute $R_2^{-1}(k_2, R_3^{-1}(k_3, y))$ and checks whether this value can be found in the above table. If this the case, the corresponding key (k_1, k_2, k_3) is a key candidate. We obtain about 2^{32} candidates and using a second plaintext-ciphertext pair should allow to eliminate the wrong ones. This meet-in-the-middle attack requires 2^{32} blocks of 64 bits ($= 2^{35}$ MB) and a complexity equivalent to about 2^{64} Ψ encryptions.

6. This observation allows us to make an exhaustive search on the subkeys k_1 and k_2 using a couple of pairs (x, y_R), where x is any plaintext and y_R denotes the 32 rightmost bits of the corresponding ciphertext. Once, these subkeys are known, one can peel-off the two first layers and find k_3 by exhaustive search.

A Known-Plaintext Attack

7. First, we observe that $y_R = y'_R$ leads to $F_3(y_R) = F_3(y'_R)$. From this, we deduce

$$y_L \oplus F_1(x_R) \oplus x_L = y'_L \oplus F_1(x'_R) \oplus x'_L \tag{1}$$

8. We are looking for a collision on a set of size 2^{32} elements. Birthday paradox tells us that approximately $\sqrt{2^{32}} = 2^{16}$ plaintext-ciphertext pairs are sufficient.

9. We first collect some plaintext-ciphertext pairs until we get a collision on the 32 rightmost bits of two ciphertexts. Let us denote the corresponding plaintexts by (x_L, x_R) and (x'_L, x'_R). Then, the subkey k_1 can be found by exhaustive search by testing the equality (1). Namely, a candidate for k_1 is detected when this equality holds.

10. We find k_1 as in the previous question. Then, y_R only depends on k_2, which allows to make an exhaustive search on the subkey k_2. Finally, k_3 can be also retrieved by an exhaustive search. The computational complexity is reduced to about $3 \cdot 2^{32}$ Ψ encryptions. Finding the above collision requires 2^{16} blocks of 32 bits which is equivalent to 2^{18} MB of memory.

4-round Feistel Scheme with Weak Round Functions

11. Since all round functions are affine, we note that any round is an affine transformation over $\{0,1\}^{64}$, which shows that the 4-round Feistel scheme is an affine transformations well. Since the subkeys are only involved in the additive part of the round functions, we can write this cipher as

$$y = A \cdot x \oplus f(k_1, k_2, k_3, k_4),$$

for a matrix $A \in \{0,1\}^{64\times 64}$, a function f, and any plaintext-ciphertext pair (x, y). Using the fact that the key is only involved in the additive part, we can decipher any ciphertext y' by computing

$$A^{-1}(y \oplus y') \oplus x.$$

Note that A is invertible since the Feistel scheme is invertible as well.