Introduction to Cryptography: Homework 3

September 29, 2021

Requirements about the delivery of this assignment:

- Submit a pdf-document via Brightspace;
- Any additional files (e.g., Python scripts) can be added as well;
- Make sure that you write both name and student number on all documents (not only in the file name).

Deadline: Monday, October 11, 17:00 sharp!

Grading: You can score a total of 100 points for the hand-in assignments. To get full points, please **explain all answers clearly**.

Exercises:

1. **Feistel structure inverse.** Consider the following two-round Feistel structure:

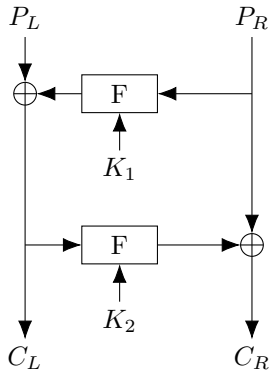


Figure 1: Two round Feistel structure.

Let $\mathrm{F}\colon \{0,1\}^\ell \to \{0,1\}^\ell$ be an arbitrary function. In the lecture, it was explained that the inverse of a Feistel structure is just the same structure, but with the round keys in the reversed order. We will verify that this is indeed the case.

(a) One can express C_L as $C_L = P_L \oplus \mathrm{F}(K_1, P_R)$. Express C_R in terms of $P_L, P_R, \mathrm{F}, K_1$ and K_2 in a similar fashion.

(b) Assume we evaluate the function on $C_R \| C_L$ with keys K_1, K_2 swapped. Write the output as $Q_L \| Q_R$. Express Q_L and Q_R in terms of $C_L, C_R, \mathrm{F}, K_1$ and K_2.

(c) Show that $Q_L = P_R$.

(d) Show that $Q_R = P_L$.

2. **Insecurity of Feistel structure.** Consider a two-round Feistel structure as in Figure 2.

Let $\mathrm{F}_{K_1}\colon \{0,1\}^\ell \to \{0,1\}^\ell$ and $\mathrm{F}_{K_2}\colon \{0,1\}^\ell \to \{0,1\}^\ell$ be functions that are infeasible to distinguish from a random function. Assume we have access to a device that allows us to encrypt messages. The goal of this exercise is to recover the plaintext for a given ciphertext $C_L \| C_R$.

(a) Recall the formulas for C_L and C_R in terms of $\mathrm{F}, K_1, K_2, P_L$ and P_R. [Note that they are those of Exercise 1a.]

(b) We encrypt $0^\ell \| 0^\ell$ on the device and obtain $a \| b$. Express a and b using the formulas from part (a).

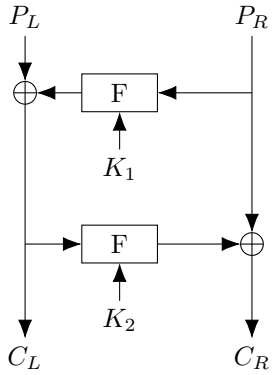


Figure 2: Two-round Feistel structure.

(c) We encrypt $(C_L \oplus \mathrm{F}_{K_1}(0^\ell))\|0^\ell$ on the device and obtain $c\|d$. Explain why we can compute $C_L \oplus \mathrm{F}_{K_1}(0^\ell)$.

(d) Express c and d using the formulas from (a).

(e) Using the result from (d), show how to obtain P_R.

(f) Find a final encryption to make, so that you can obtain P_L. [Hint: You can now use P_R.]

3. **PRP-security of 2-round Feistel structure.** In this exercise, we consider a two-round Feistel structure, like in Figure 2 again.

   Let the keys K_1, K_2 be 32 bits long, and let for both keys K_1, K_2, the map $\mathrm{F}_{K_i} : \{0,1\}^{32} \to \{0,1\}^{32}$ be infeasible to distinguish from a random function.

   (a) Based only on exhaustive key search, what is an upper bound on the security strength of this cipher?

   (b) Give a distinguisher $\mathcal{D}$ that distinguishes the two-round Feistel structure from a random permutation. [You do not have to compute the advantage yet.]

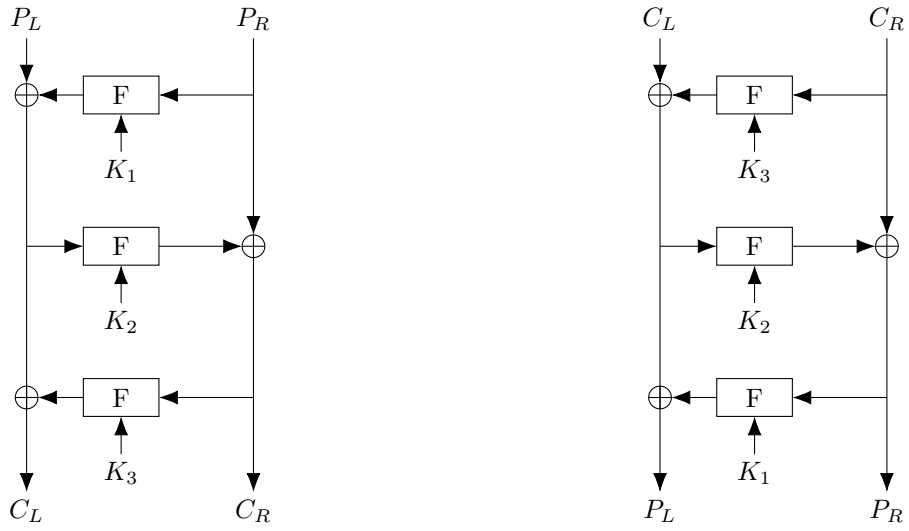
   (c) Give the probability that you guess that you are talking to a 2-round Feistel structure when you are actually talking to a random permutation.

   (d) Compute the advantage of your distinguisher $\mathcal{D}$.

   (e) Given your attack to show the 2-round Feistel structure is not PRP-secure, what is the new upper bound on the security strength?

Hand in assignments:

1. **(80 points) SPRP-security of the Feistel structure.** In this exercise, we are going to show that a Feistel structure with up to 3 rounds is not SPRP secure.



(a) Encryption (b) Decryption

Figure 3: Three-round Feistel structure.

Assume that the functions $\mathrm{F}_{K_i}\colon \{0,1\}^\ell \to \{0,1\}^\ell$ are infeasible to distinguish from a random function for $i \in \{1,2,3\}$.

We try to distinguish between this three-round Feistel structure (see Figure 3) and a random permutation $\mathcal{RP}$.

To do this, we perform the following steps:

i. Decrypt $0^\ell \| 0^\ell$ and call the result $a \| b$;

ii. Encrypt $0^\ell \| b$ and call the result $c \| d$;

iii. Decrypt $(a \oplus c) \| d$ and call the result $e \| f$.

We say that we are interacting with the Feistel structure if $f = b \oplus d$, and we are interacting with the random permutation if this is not the case.

For (a)–(f), we assume that we interact with the Feistel structure.

(a) Give formulas for C_L and C_R in terms of F_{K_i}, P_L and P_R like in Exercise 1(a) when encrypting with this three-round Feistel structure. 10 pt

(b) Give formulas for P_L and P_R in terms of F_{K_i}, C_L and C_R when decrypting with this 3-round Feistel structure. 10 pt

(c) Give formulas for a and b. 10 pt

(d) Give formulas for c and d. 10 pt

(e) Give formulas for e and f. 15 pt

(f) Show that indeed $f = b \oplus d$. [Hint: What is $a \oplus c$?] 15 pt

(g) The probability that $f = b \oplus d$ when we are interacting with the random permutation is $\frac{2^\ell - 2}{2^{2\ell} - 2}$, $\frac{2^\ell - 1}{2^{2\ell} - 2}$ or $\frac{2^\ell}{2^{2\ell} - 2}$, depending on a case distinction. (You do not need to show/prove this!) For large enough ℓ, this can be approximated by $\frac{1}{2^\ell}$. Compute the advantage of this distinguisher, using this approximation. 5 pt

(h) Compute the security strength of the three-round Feistel structure. 5 pt

2. **(20 points) PRP-security of 1-round Feistel structure.** In this exercise, we consider a one-round Feistel structure. Let again $F_{K_1}: \{0,1\}^\ell \to \{0,1\}^\ell$ be infeasible to distinguish from a random function. You will show that the one-round Feistel structure is not PRP-secure.

   (a) What is the ideal version of the Feistel structure that your distinguisher will compare it with? 2 pt

   (b) Give your distinguisher $\mathcal{D}$. [Give the queries your distinguisher makes and what conclusion it takes. Furthermore, explain why this will work.] 5 pt

   (c) Give the probability that your distinguisher is actually talking to the ideal version, but the distinguisher decides that it is talking to the 1-round Feistel structure. 4 pt

   (d) What is the advantage of your distinguisher? 4 pt

   (e) Give an upper bound for the security strength of a 1-round Feistel structure. 3 pt

   (f) Is the Feistel structure SPRP-secure? 2 pt