Introduction to Cryptography

TEK 4500 (Fall 2020)
Problem Set 2

Problem 1.
Read Chapter 3 and Chapter 4 (Sections 4.8–4.10 can be skipped) in [BR].

Problem 2. [Problem 6.8 in [Ros]]
Suppose F is a secure PRF with input length in, but we want to use it to construct a PRF G with longer input length. Below are some approaches that don't work ("$\|$" denotes string concatenation, e.g. $101\|01 = 10101$). For each one, describe a successful distinguishing attack and compute its PRF-advantage (i.e., what is $\mathbf{Adv}_G^{\mathsf{prf}}(\mathcal{A})$, where $\mathcal{A}$ is the adversary that runs your attack?):

a) $G(K, X\|X') = F(K, X)\|F(K, X')$, where X and X' are each in bits long.

b) $G(K, X\|X') = F(K, X) \oplus F(K, X')$, where X and X' are each in bits long.

c) $G(K, X\|X') = F(K, X) \oplus F(K, X \oplus X')$, where X and X' are each in bits long.

d) $G(K, X\|X') = F(K, 0\|X) \oplus F(K, 1\|X')$, where X and X' are each $in - 1$ bits long.

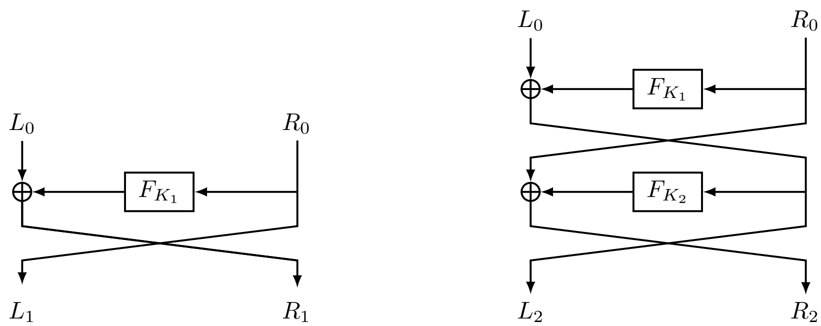
Problem 3.
Suppose $F : \{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ is a secure PRF. For each of the following constructions of a *new* PRF from F, decide whether it is also a secure PRF. If you think it's not, describe an attack, else, indicate why the new construction is also secure.

a) $G(K, X) = \begin{cases} 0^{128}, & \text{if } K = 0^{128} \\ F_K(X), & \text{otherwise} \end{cases}$

b) $G(K, X) = \begin{cases} 0^{128}, & \text{if } X = 0^{128} \\ F_K(X), & \text{otherwise} \end{cases}$

c) $G(K, X) = F(K, X) \oplus 1^{128}$

d) $G(K, X) = F(K, X) \oplus C$, where $C \in \{0,1\}^{128}$ is a *fixed* and *public* (and thus known to the adversary) hard-coded string of some arbitrary value.



(**a**) One-round. (**b**) Two-rounds.

Figure 1: Feistel network.

Problem 4.

Let $E^{(1)} : \{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ denote the block cipher defined by the one-round Feistel network shown in Figure 1a, where $F : \{0,1\}^{128} \times \{0,1\}^{64} \to \{0,1\}^{64}$ is the internal round function. Show that $E^{(1)}$ is *not* a secure PRF by demonstrating an attack. What is the PRF-advantage of your attack? That is, what is $\mathbf{Adv}^{\mathsf{prf}}_{E^{(1)}}(\mathcal{A})$, where $\mathcal{A}$ is the adversary that runs your attack?

Hint: What is $E^{(1)}(K_1, 0^{128})$?

Problem 5.

Let $E^{(2)} : \{0,1\}^{256} \times \{0,1\}^{128} \to \{0,1\}^{128}$ denote the block cipher defined by the two-round Feistel network shown in Figure 1b, where $F : \{0,1\}^{128} \times \{0,1\}^{64} \to \{0,1\}^{64}$ is the internal round function (the first 128 bits of E's key is being used as the key to F in the first round, and the last 128 bits in the second round). Show that $E^{(2)}$ is *not* a secure PRF by demonstrating an attack. What is the PRF-advantage of your attack? That is, what is $\mathbf{Adv}^{\mathsf{prf}}_{E^{(2)}}(\mathcal{A})$, where $\mathcal{A}$ is the adversary that runs your attack?

Hint: it is possible to obtain a very high PRF-advantage by making two oracle queries in the PRF experiment $\mathbf{Exp}^{\mathsf{prf}}_{E^{(2)}}(\mathcal{A})$.

Problem 6.

Suppose DES was only using a *single* round and suppose you have access to two plaintext-ciphertext pairs (X, Y), (X', Y') (in particular, $Y = (L_1, R_1)$, where $L_1 = R_0$ and $R_1 = L_0 \oplus F_{K_1}(R_0)$; similarly for Y'). Explain how you can recover the *key* K_1 of this one-round version of DES.

Hint 1: Unlike in Problem 4, you should now exploit the *concrete* round function $F : \{0,1\}^{48} \times \{0,1\}^{32} \rightarrow \{0,1\}^{32}$ used inside DES. Look up the details in [PP] or on Wikipedia if you have to.

Hint 2: Some trial-and-error of candidate keys is necessary. However, it should be possible to obtain K_1 by trying about $4^{48/6} = 2^{16}$ candidate keys. Notice that this is much less than the possibly 2^{48} keys you would have to try by brute-force.

Problem 7.

A crucial component of the DES and AES round functions is the S-boxes, which are the only non-linear parts of DES and AES. Recall that a function F is linear if $F(A+B) = F(A) + F(B)$ for all inputs A, B. In this exercise you are asked to validate that the first S-box of DES, S_1, is indeed non-linear by computing the output values for a set of input values. In particular, show that $S_1(X_1) \oplus S_1(X_2) \neq S_1(X_1 \oplus X_2)$ for:

a) $X_1 = 000000, X_2 = 000001$

b) $X_1 = 111111, X_2 = 100000$

c) $X_1 = 101010, X_2 = 010101$

Extra: Write a script (e.g. in Python) that checks whether S_1 is non-linear for *all* inputs. Do the same for other DES S-boxes and the AES S-box. Values for the DES and AES S-boxes can be found online, e.g., here (DES) and here (AES).

References

[BR] Mihir Bellare and Phillip Rogaway. *Introduction to Modern Cryptography*. `https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf`.

[PP] Christof Paar and Jan Pelzl. *Understanding Cryptography - A Textbook for Students and Practitioners*. Springer, 2010.

[Ros] Mike Rosulek. *The Joy of Cryptography*, (draft Feb 6, 2020). `https://web.engr.oregonstate.edu/~rosulekm/crypto/crypto.pdf`.