Introduction to Cryptography - Exercise session 5

Prof. Sebastian Faust

November 21, 2018

In the first part of this exercise, we recall the new topics covered during the lecture: modes of operation ECB, CBC and CTR, and the blockcipher DES. The second part of this sheet contains more interesting exercises.

PART 1

Exercise 1 (Modes of operation)

Recall the three modes of operation discussed during the lecture, i.e. ECB mode, CBC mode and CTR mode.

(a) Let F be a blockcipher with n-bit key and block length. For each of the modes write down/draw how a message $m_1, \ldots, m_\ell \in \{0,1\}^{\ell \times n}$ would be encrypted using F. For each mode, explain how decryption work.

(b) For each of the modes, explain the effect of a single-bit error in the ciphertext.

Exercise 2 (DES)

Let F be a block cipher with n-bit key and ℓ-bit block length. Then the new block cipher F' with key of length $2n$ can be defined as

$$F'_{k_1,k_2}(x) := F_{k_2}(F_{k_1}(x)),$$

where k_1, k_2 are independent keys. For the case when $F = \mathsf{DES}$, we call $F' = 2\mathsf{DES}$. The above construction can be generalized to triple encryption as follows:

$$F''_{k_1,k_2,k_3}(x) := F_{k_3}(F^{-1}_{k_2}(F_{k_1}(x))).$$

If $F = \mathsf{DES}$, then the blockcipher F'' is called $3\mathsf{DES}$. The reason why the second invocation of F is reversed is for backward compatibility.

(a) Show how to design DES from $3\mathsf{DES}$.

(b) Show how to design $2\mathsf{DES}$ from $3\mathsf{DES}$.

(c) Assume that F is a strong PRP. Informally argue, why the above construction of F'' is as good as if the second invocation of F would not be reversed, i.e. $F_{k_3}(F_{k_2}(F_{k_1}(x)))$.

PART 2

Exercise 3 (CBC mode)

Consider a stateful variant of the CBC-mode encryption Π where the sender simply increments the $IV \in \{0,1\}^n$ by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is not CPA-secure.

Exercise 4 (Meet-in-the-middle attack)

Let F be a block cipher with n-bit key and ℓ-bit block length. Consider a block cipher F' with key of length $2n$ defined as

$$F'_{k_1,k_2}(x) := F_{k_2}(F_{k_1}(x)),$$

where k_1, k_2 are independent n-bit keys.

(a) Design an adversary that given only one valid (plaintext, ciphertext) pair (x, y), i.e.

$$y = F'_{k_1^*,k_2^*}(x),$$

can find a set S consisting of all key pairs (k_1, k_2) such that $y = F'_{k_1,k_2}(x)$ and whose time complexity is asymptotically smaller that the time complexity of the bruteforce attack (which is $\mathcal{O}(2^{2n})$). Hint: Make use of the name of this exercise.

(b) What is the space complexity of the above algorithm?

(c) Assume that the adversary knows two pliantext, ciphertext pairs (x_1, y_1) and (x_2, y_2) for $x_1 \neq x_2$, i.e. $y_1 = F'_{k_1^*,k_2^*}(x_1)$ and $y_2 = F'_{k_1^*,k_2^*}(x_2)$. Does this additional knowledge help the attacker? Explain your answer.

HOMEWORK

Exercise 5 (Chained CBC)

Is the chained CBC mode scheme defined below CPA-secure? If not, illustrate with an attack.

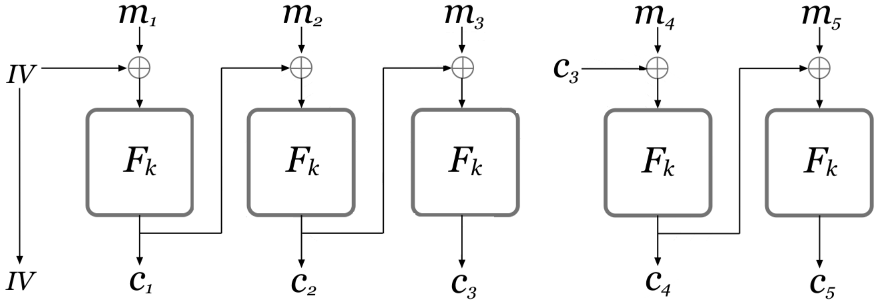

Figure 1: Chained CBC