Introduction to Cryptography: Homework 4

October 6, 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 18, 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. **Multi-target attacks and scheme recognition.** In this exercise, we are going to analyze the scheme in Figure 1. Moreover, we will perform a multi-target attack on several instantiations of this scheme.

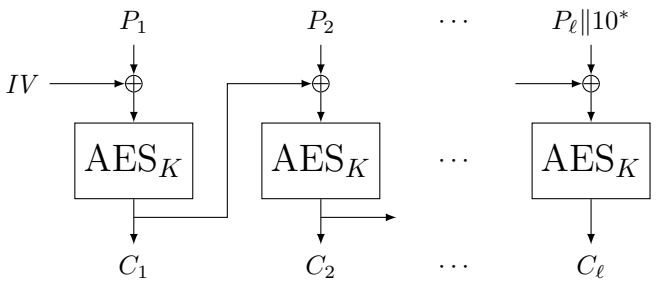

Figure 1: The scheme up for analyzing.

Assume that the instantiation of AES uses 10 rounds.

(a) What type of encryption is this?

(b) What is the ideal counterpart of the used internal?

(c) What is the length of the key used in this scheme?

Suppose we as the attacker have located 100 devices on which this scheme is used, and we can make queries to the device to receive the ciphertexts. Each of the devices has a different key that is used to perform encryption.

Every query we make consists of choosing a specific plaintext and receiving the corresponding ciphertext. Since the padding that is used here is reversible, you may disregard issues with padding.

(d) Assume upon being presented a plaintext, a device randomly generates an IV that it, together with the ciphertext, presents at the output. Explain why this prevents a multi-target attack. [Hint: The IV randomizes your plaintext value, what can you compare?]

Because of what is written in the previous subquestion, we now assume that the devices precompute random IVs such that there is always one ready before a query is made. That is, after outputting (IV, C) for a given plaintext, the device immediately generates a new random IV. Furthermore, assume that we have a way to read this random IV from the device before making a query.

(e) Explain that we can now make queries with certain P_i to all devices, such that $P_i \oplus \mathrm{IV}_i = P_j \oplus \mathrm{IV}_j$ for all devices.

(f) Explain how to perform a multi-target attack against these devices. [Give the queries you make, both online and offline, and how you decide to have found the correct key.]

(g) What is the probability of finding at least one of the 100 secret keys with one guess?

(h) What is the upper bound on the security strength of this scheme against this multi-target attack?

2. **Meet-in-the-middle attack on Triple-DES.** In this exercise, we are going to perform a meet-in-the-middle attack on Triple-DES, and see what effect this has on the security strength.

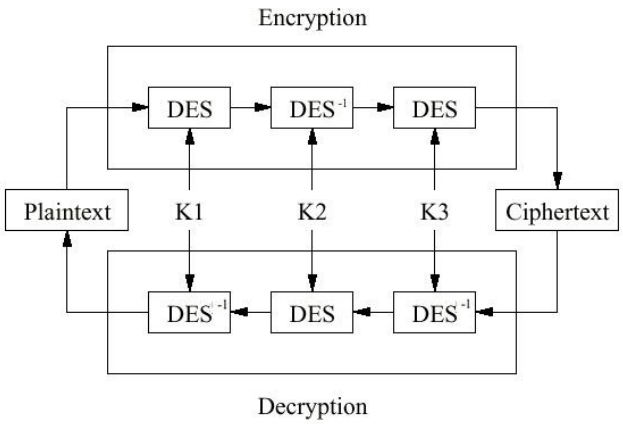

Figure 2: Triple-DES.

As seen in Figure 2, to encrypt a plaintext using Triple-DES, one performs:

$$\mathrm{DES}_{K_3}(\mathrm{DES}^{-1}_{K_2}(\mathrm{DES}_{K_1}(P))) = C$$

In the lecture, there was discussion on the various instantiations of Triple-DES, depending on whether all keys are distinct, all keys are the same, or $K_1 = K_3$. (See slide 23 of slides_4_blockciphers.)

(a) Give an upper bound on the security strength for each of the Triple-DES instantiations referenced above, considering only exhaustive key search. I.e.,

i. $K_1 = K_2 = K_3$;

ii. $K_1 = K_3$ and K_2 independent of K_1;

iii. K_1, K_2, K_3 all independent.

(b) Explain why the case that $K_1 = K_2$, but K_3 independent of K_1 is equivalent to one of the other instantiations of Triple-DES. Make sure to mention to which instantiation it is equivalent.

(c) Explain how to do a meet-in-the-middle attack on Triple-DES with three distinct keys. You may use three online queries that result in plaintext-ciphertext pairs $(P_0, C_0), (P_1, C_1)$ and (P_2, C_2). [You get three pairs as you will turn out to need two pairs to verify your result in order to get a probability close to 1.]

(d) Give an upper bound on the security strength on Triple-DES with three distinct keys, taking into account the meet-in-the-middle attack.

(e) To obtain a higher security strength, someone proposes to use Quadruple-DES with four independent keys. Is this more secure? If yes, how much more? If no, why not?

3. **CBC colliding ciphertexts.** Consider the CBC-mode for block ciphers in slide 11 of slides_5_blockciphermodes. If for some $i < j$, we have $C_i = C_j$, then some information about the plaintexts can be obtained.

(a) Show that $P_j = C_{i-1} \oplus P_i \oplus C_{j-1}$.

(b) Suppose that for a 10-block plaintext $P_1, \ldots, P_{10}$, the resulting ciphertext under encrypting with initialization vector IV is

$$(C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9, C_{10}) = (S_1, S_2, S_3, S_1, S_2, S_4, S_5, S_6, S_2, S_4)$$

(The S_i are just taken as placeholders for certain strings, so you can see which are equal.) You, as an adversary, can perform three online queries to the inverse of the underlying block cipher. Which ciphertext blocks should you query to obtain as much information regarding the plaintext as possible? [Hint: Use (a).]

Hand in assignments

1. **(60 points) Using the complementation property in DES.** In the lecture, we saw that DES satisfies the complementation property:

$$\mathrm{DES}_{\overline{K}}(\overline{P}) = \overline{C} \iff \mathrm{DES}_K(P) = C$$

In this exercise, you will show how you can use this property to do an "adapted exhaustive key search" and reduce the upper bound on the security strength from DES. That is, for some specific encryption device using DES, you are going to find its key K with the "adapted exhaustive key search".

   (a) Give descriptions of the plaintexts for which you make online queries. 8 pt

   (b) Use the complementation property on those queries and give the descriptions of the resulting plaintext-ciphertext pairs. 12 pt

   (c) Give a set of keys $\mathcal{K}$ for which you will make offline queries. 12 pt

   (d) Show how you can determine the correct key when performing your "adapted exhaustive key search". 20 pt

   (e) Compute the security strength of DES, considering this adapted exhaustive key search. 8 pt

2. **(40 points) Modes of operation and error during transit.** Alice and Bob have a shared AES key. Alice wants to send a plaintext of 900 bits long to Bob, using their AES key as a means to confidentially get this plaintext message across.

   Assume that the plaintext message m is encrypted using AES in ECB, CBC, OFB or CTR mode, assume that CBC and OFB have random IV and CTR a diversifier.

   (a) What is the length of the ciphertext? Distinguish between different modes. 20 pt

      i. ECB;
      ii. CBC;
      iii. OFB;
      iv. CTR.

   Assume that the corresponding ciphertext C gets disturbed in transfer to Bob. The bit c_{300} is therefore flipped, yielding C' as the bit string that Bob receives. Bob decrypts the message to obtain m'. In this exercise, you should assume that whenever one input bit to AES is flipped, the output of AES differs in half of the bits.

   (b) In which bits does m' differ from m? Also give the number of bits where m' differs from m. Distinguish between different modes. 20 pt

      i. ECB;
      ii. CBC;
      iii. OFB;
      iv. CTR.