SECURITY AND CRYPTOGRAPHY LABORATORY

Family Name: ....

First Name: ....

Section: ....

Advanced Cryptography

Midterm Exam

April 15^{th}, 2008

Duration: 3 hours

This document consists of 12 pages.

Instructions

Electronic comunication devices and are *not* allowed.

Other electronic devices and all printed documents are permitted.

Answers must be written on the exercises sheet.

This exam contains 2 *independent* exercises.

Answers can be either in French or English.

Questions of any kind will certainly *not* be answered. Potential errors in these sheets are part of the exam.

You have to put your full name on the first page and have all pages *stapled*.

1 Attack on Modified TEA

The TEA block cipher is a 64-round feistel scheme operating on 64-bit message blocks with a 128-bit key.

In what follows,the plaintext is denoted by x and the ciphertext by y.

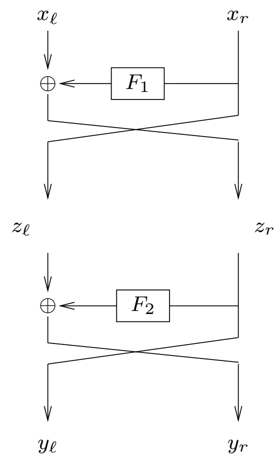

Figure 1: First 2 rounds of a Feistel scheme.

We use the notation x_ℓ, y_ℓ (resp. x_r, y_r) for the plaintext/ciphertext on the left (resp. right) leave, i.e., $x = x_\ell \| x_r$ and $y = y_\ell \| y_r$ where the operator "$\|$" denotes the concatenation.

1. Draw the inverse scheme for the Feistel scheme of Figure 1.

For each round i, a 32-bit subkey K_i is derived from the full key K. For the round i, the function F_i is then defined as:

$$F_i(\alpha) = (\alpha \ll 4) \oplus (\alpha \gg 5) \oplus \alpha \oplus K_i.$$

where $\ll 4$ denotes a shift to the left of 4 bits and $\gg 5$ denotes a shift to the right of 5 bits (the shifts are *not* rotations and insert bits 0).

2. Express z_ℓ, z_r in term of x_ℓ, x_r, K_1.

3. Express y_ℓ, y_r in term of x_ℓ, x_r, K_1, K_2.

4. Compute the differential coefficient $\mathrm{DP}^{F_i}(a, b)$ for any arbitrary a, b, i.

5. Using two queries, define an efficient distinguisher between 64-round TEA and the perfect cipher C^*. Compute its advantage.

2 Collisions on the AR Hash Function

The AR hash function has been proposed by *Algorithmic Resarch Ltd* and has been used in practice in the German banking world. AR hash is based on the DES and a variant of the CBC mode.

AR hash is more precisely defined as follows: the message m to be hashed is divided into b-bit blocks denoted by $m_1, m_2, \ldots, m_n$. For simplicity, we assume that the length of m is a multiple of the block size. We then define a series of b-bit blocks $B_{-1}, B_0, B_1, \ldots, B_n$ by:

$$B_{-1} = B_0 = 0 \text{ and } B_i = m_i \oplus \mathrm{DES}_K(m_i \oplus B_{i-1} \oplus B_{i-2}), i = 1 \ldots n$$

where K is an arbitrary DES key.

We define the function G as:

$$G(x, y, K) = \mathrm{DES}_K(x \oplus y) \oplus \mathrm{DES}_K(x) \oplus \mathrm{DES}_K(y) \oplus y$$

To hash the message m, two different DES keys K_1, K_2 are selected and the values c_1, c_2, c_3, c_4 are computed as:

$$c_1 = f_1(m, K_1), c_2 = f_2(m, K_1), c_3 = f_1(m, K_2), c_4 = f_2(m, K_2)$$

where $f_1(m, K), f_2(m, K)$ denote B_{n-1}, B_n, respectively. The hash value is finally obtained by the concatenation of $D(c_1, c_2, c_3, c_4, K_i), i = 1, 2$ with D:

$$D(c_1, c_2, c_3, c_4, K) = G(G(c_1, c_2, K), G(c_3, c_4, K), K)$$

1. Recall the plaintext length, the ciphertext length and the key length in DES. What is the size of the digest in the AR hash?

2. Recall the definition of a collision-resistant hash function. What is the complexity of a generic collision attack against the AR hash?

Let a and b be two messages with length multiple of the block length and let $a\|b$ denote their concatenation. From an arbitrary fixed DES key K and a message block m, we define the 3 functions C, D, E:

$$C(a\|m) = m \oplus f_1(a,K) \oplus f_2(a,K)\|\mathrm{DES}_K(m) \oplus f_1(a,K)\|\mathrm{DES}_K(m) \oplus f_2(a,K)$$
$$D(a\|m) = m \oplus f_1(a,K) \oplus f_2(a,K)\|m \oplus f_1(a,K)\|m \oplus f_2(a,K)$$
$$E(a\|m) = m \oplus f_1(a,K) \oplus f_2(a,K)\|m \oplus f_1(a,K)\|\mathrm{DES}_K^2(m) \oplus f_2(a,K)$$

3. Show that for arbitrary a, b, K, m, we have:

$$f_i(a\|b, K) = f_i(a\|C(a, m)\|b, K), i = 0, 1 \tag{1}$$

Hint: Look at the block B_{n-2}, the value produced just before $f_1(a\|C(a, m), K)\ldots$

Similarly, we can prove that

$$f_2(a, K) = f_2(a\|E(a, m), K). \tag{2}$$

Additionally, if K is a weak DES key,

$$f_i(a\|b, K) = f_i(a\|D(a, m)\|b, K), i = 1, 2. \tag{3}$$

Recall: A DES key K is weak iff $\mathrm{DES}_K(\mathrm{DES}_K(m)) = m$.

4. Show that for any c_1, c_2, K:

$$G(c_1, c_2, K) = G(c_1 \oplus c_2, c_2, K), G(c_1, 0, K) = \mathrm{DES}_K(0)$$
$$D(c_1, c_1, c_1, c_1, K) = (c_1, c_1), D(c_1, 0, c_2, 0) = 0$$

5. Deduce that G and D are not collision-resistant

5. Using equations 1, 2 and 3, show that for any m, K_2:

$$f_1(m \| \mathrm{DES}_{K_2} \| \mathrm{DES}_{K_2}, K_2) = 0$$
$$f_2(m \| \mathrm{DES}_{K_2} \| \mathrm{DES}_{K_2}, K_2) = 0$$

6. Using the two previous questions, show how it is possible to find a collision on the AR Hash.

   Hint: For a weak weak DES key there are 2^{32} fixpoints s.t. $\mathrm{DES}_K(m) = m$. Each fixpoint can be found in half a DES encryption.

   Consider K_1 a weak DES key and m a fixpoint...