ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Family Name: ______________________

First Name: ______________________

Section: ______________________

Cryptography and Security Course (Cryptography Part)

Midterm Exam

December 15th, 2006

This document consists of 7 pages.

Instructions

Books and lecture notes are *not allowed.*

Electronic devices are *not allowed.*

Answers must be written on the exercises sheet.

Answers can be written either in French or in English.

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

We consider a 3-round Feistel scheme Ψ as depicted in Figure 1 with a 64-bit block size and a 96-bit key k. From the key $k \in \{0,1\}^{96}$, we derive three subkeys of 32 bits each, which are defined such that $k = k_1 \| k_2 \| k_3$. The ith round function F_i only depends on the subkey k_i for $i = 1, 2, 3$, i.e., F_i is of the form $f^i_{k_i}$. For a given plaintext $x \in \{0,1\}^{64}$, we will denote the corresponding ciphertext $\Psi(x)$ by y. The 32 leftmost bits of x (resp. y) will be denoted x_L (resp. y_L) and the 32 rightmost bits will be denoted x_R (resp. y_R).

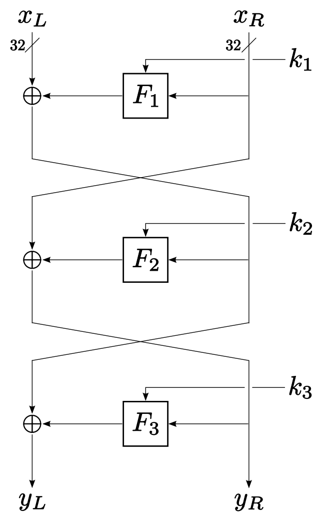

Figure 1: 3-round Feistel scheme.

Preliminaries and Brute Force Attacks

1. Give the name of a block-cipher based on a Feistel scheme.

2. Draw the scheme corresponding to the decryption of the cipher Ψ.

3. What is the average complexity of an exhaustive key search against Ψ using a stop test oracle?

4. We want to implement a stop test oracle using t known plaintext-ciphertext pairs as witnesses. By doing an exhaustive search based on the t witnesses, depending on t, how many possible keys are displayed on average? (Hint: separate the right key and the wrong key cases.) How large t must be so that the average number of wrong keys is close to 0?

5. Show how you can decrease the complexity of the previous attack by performing a "meet-in-the-middle" attack. Describe it precisely and evaluate the computational complexity as well as the required memory.

6. Observe that y_R does not depend on the subkey k_3. Using this observation, derive an attack to retrieve k with a complexity within the order of magnitude of 2^{64} Ψ encryptions and almost no memory using a few known plaintext-ciphertext pairs. (Hint: find first a procedure to recover k_1 and k_2.)

A Known-Plaintext Attack

7. Show that if we find two different plaintexts $x = (x_L, x_R)$ and $x' = (x'_L, x'_R)$ with corresponding ciphertexts $y = (y_L, y_R)$ and $y' = (y'_L, y'_R)$ such that $y_R = y'_R$, we can deduce a relation involving k_1 and $x_L, x'_L, x_R, x'_R, y_L, y'_L$.

8. How many known plaintext-ciphertext pairs do we need approximately to get two pairs such that $y_R = y'_R$? (Hint: use the birthday paradox.)

9. Derive a known-plaintext attack to retrieve k_1.

10. Derive a known-plaintext attack to retrieve k. Describe it carefully and evaluate the computational complexity and required memory.

4-round Feistel Scheme with Weak Round Functions

From now on, we consider a 4-round Feistel scheme and a 128-bit key $k = k_1 \| k_2 \| k_3 \| k_4$ such that the round functions F_i are of the form $f^i_{k_i}$ for $i = 1, \ldots, 4$.
We select the round functions $f^i_{k_i}$ to be some affine functions. More precisely, we choose some matrices $A_i \in \{0, 1\}^{32 \times 32}$ and define the round functions as follows

$$f^i_{k_i}(u) := A_i \cdot u \oplus k_i,$$

for $i = 1, \ldots, 4$.

11. Describe a very efficient attack which allows to decrypt any ciphertext from a single given plaintext-ciphertext pair. (We do not have access to an encryption or a decryption oracle.)

**Any attempt to look at
the content of these pages
before the signal
will be severely punished.**

Please be patient.