LASEC
SECURITY AND CRYPTOGRAPHY LABORATORY

Family Name: ....

First Name: ....

Section: ....

Security and Cryptography

Fall semester 2007

Midterm Exam

November 1st, 2007

Duration: 105 minutes

Part 1 / 2

This document consists of 8 pages.

Instructions

Documents are *not* allowed apart from linguistic dictionaries.

Electronic devices are *not* allowed.

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 Attacks on a Simple Cipher

Let $C : \{0,1\}^n \times \{0,1\}^m \mapsto \{0,1\}^n$ be a n-bit block cipher with m-bit keys. C consists of 2 rounds of a Feistel scheme as depicted on Figure 1. The plaintext is denoted by $x \in \{0,1\}^n$ and the output ciphertext by $y \in \{0,1\}^n$.

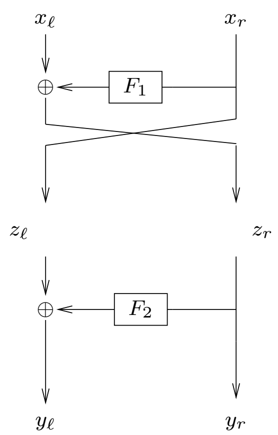

Figure 1: C: a 2-round Feistel scheme.

We use the notation $x_\ell, x_r \in \{0,1\}^{\frac{n}{2}}$ (resp. $y_\ell, y_r \in \{0,1\}^{\frac{n}{2}}$) for the plaintext (resp. ciphertext) on the left and right leaves, 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.

Now, we will define the round functions. Let the key $k \in \{0,1\}^n$, i.e. here $m = n$, and let $k_1, k_2 \in \{0,1\}^{\frac{n}{2}}$ be respectively the left and right part of k. We consider that the round function F_i with input α simply "xor" the input with the round key k_i, i.e. the output is

$$\beta = F_i(\alpha) = \alpha \oplus k_i.$$

2. Write y_ℓ and y_r in terms of x_ℓ, x_r, k_1, k_2.

3. Explain how it is possible to recover the key K using one plaintext-attack query, i.e. based on a plaintext-ciphertext pair (x, y).

Now, we use C from Figure 1 to build the cipher $2C$. $2C$ is built by concatenating two times C as decpited on Figure 2.

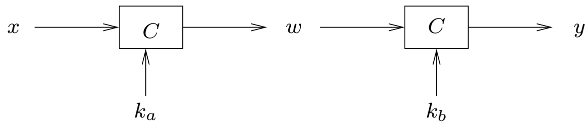

Figure 2: $2C$.

4. Considering C as a black-box, which well-known attack can be applied?

5. Write y_ℓ and y_r in terms of $x_\ell, x_r, k_{a1}, k_{a2}, k_{b1}, k_{b2}$.

6. Is a decryption attack now possible? Explain your answer.

7. Let y and y' be two ciphertexts. What can we say about $y \oplus y'$? What is the consequence?

2 Linear Algebra

1. Compute $17^{129} \bmod 19$.
   Give the details.

2. Compute the inverse of 7 in $\mathbb{Z}_{143}^*$, i.e. compute $7^{-1} \bmod 143$.
   Give the details.

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

Please be patient.