ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Family Name: .....

First Name: .....

Section: .....

Advanced Cryptography

Midterm Exam

May 19th, 2006

Duration: 2 hours 30 minutes

This document consists of 12 pages.

Instructions

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 *each* page and you have to do it *now*.

1 Attack on a simple Feistel Scheme

Let C be the block cipher that consists of the 2-round Feistel scheme of Figure 1. The plaintext is denoted by x and the output ciphertext by y.

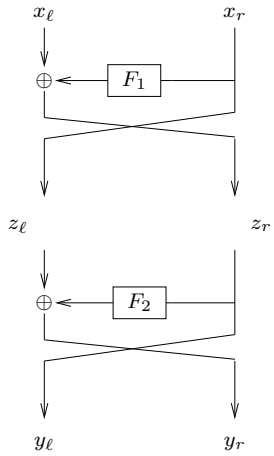

Figure 1: 2-round Feistel scheme.

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.

We consider that the functions F_i simply performs a xor between the input and a subkey. We denote by k_1 the subkey of the first round, and by K_2 the subkey of the second round. Consequently, we have $F_i(\alpha) = \alpha \oplus k_i$.

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 $\mathrm{DP}^C(a, b)$ for any fixed (unknown) a, b.

5. Consider $x_\ell, y_\ell, k_i \in \{0,1\}$. Compute $[C]^1$ the distribution matrix of C at order 1.

6. Is the cipher C a markov cipher? Justify your answer.

7. Does C provide perfect secrecy if it is used only once? Justify your answer.

8. Using two queries, define an efficient distinguisher between C and the perfect cipher C^*. Compute its advantage.

2 GCM: the Galois Counter authenticated encryption Mode

We consider 128-bit strings as elements of the Galois field GF(2^{128}) so that the addition corresponds to the bitwise XOR operation denoted "$\oplus$" and the multiplication is denoted by "$\cdot$". We assume we have a conventional choice for the representation of the Galois field.

We consider a keyed hash function which, given a bitstring X of bitlength multiple of 128 and a 128-bit key H defines

$$\mathsf{GHASH}_H(X) = X_1 \cdot H^m \oplus \cdots \oplus X_m \cdot H$$

where $X = X_1 || \cdots || X_m$ is the decomposition of X into m blocks of 128 bits.

1. Assuming that H is uniformly distributed, show that for any m, GHASH_H is a $m2^{-128}$-XOR-universal hash function from the set of bitstrings of length up to $128m$ to the set of 128-bit strings.

   Recall: an ε-XOR-universal hash function h_K is a family of functions depending on some parameter K such that for any different x and y and any δ, we have

   $$\Pr_K[h_K(x) \oplus h_K(y) = \delta] \leq \varepsilon$$

   when K is uniformly distributed.

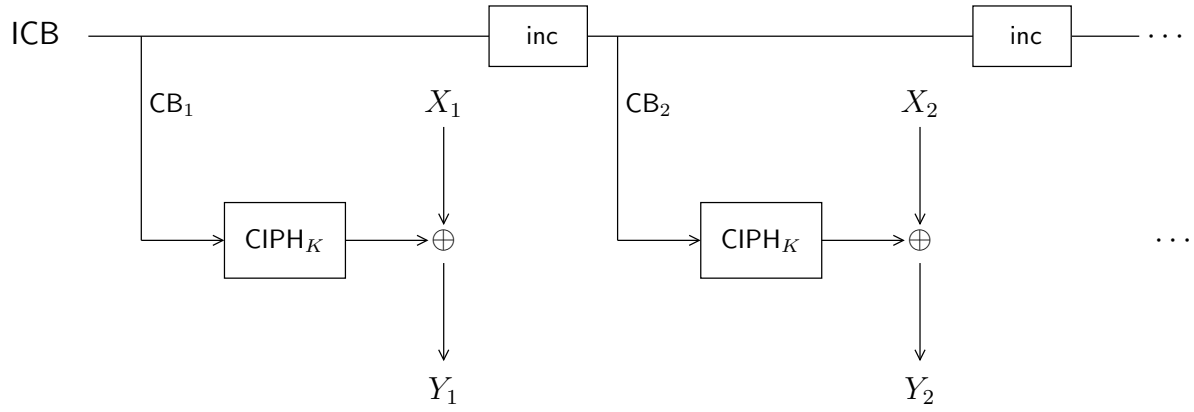

Figure 2: $\mathsf{GCTR}_K(ICB, X)$

Given a 128-bit string X, we define X_H of 96 bits and X_L of 32 bits such that

$$X = X_H \| X_L.$$

The function $\mathsf{inc}(X)$ is defined as follows:

$$\mathsf{inc}(X) = X_H \| X'_L$$

where $X'_L = X_L + 1 \bmod 2^{32}$ and X_L is considered as an integer.

We consider a block cipher with 128-bit blocks which, given a block x and a key K defines a ciphertext block $\mathsf{CIPH}_K(x)$. We define $\mathsf{GCTR}_K(\mathsf{ICB}, X)$ (see Figure 2), the encryption of an arbitrary nonempty bitstring X by key K in CTR mode with initial counter block ICB by

$$\mathsf{GCTR}_K(\mathsf{ICB}, X) = Y_1 || \cdots || Y_{n-1} || Y_n$$

with

$$Y_i = X_i \oplus \mathsf{CIPH}_K(\mathsf{CB}_i), \qquad X = X_1 || \cdots || X_{n-1} || X_n$$

and

$$\mathsf{CB}_i = \mathsf{inc}(\mathsf{CB}_{i-1}), \qquad \mathsf{CB}_1 = \mathsf{ICB}$$

where X_i are 128-bit blocks and X_n is a nonempty string of length at most 128.
When X is of length 0, $\mathsf{GCTR}_K(\mathsf{ICB}, X)$ is the empty string.

2. Show that the length of the ciphertext and the length of the plaintext are the same.

3. Let ICB and ICB' be two possible values for the initial counter block.
   The ith counter block of ICB *(resp.* ICB'*) is denoted* CB_i *(resp.* CB'_i*).*
   Let X and X' be two arbitrary plaintexts of length (in blocks) less than 2^{32}.
   The ith block of X *(resp.* X'*) is denoted* X_i *(resp.* X'_i*).*
   Let Y and Y' be the ciphertexts, i.e. $Y = \mathsf{GCTR}_K(\mathsf{ICB}, X)$ and $Y' = \mathsf{GCTR}_K(\mathsf{ICB}', X')$.
   The ith block of Y *(resp.* Y'*) is denoted* Y_i *(resp.* Y'_i*).*

   What can happen if there exists i, j such that $\mathsf{CB}_i = \mathsf{CB}'_j$?

We now assume that all ICB values are pairwise different and such that the 32 least significant bits consist of a fixed block b. Namely, we have $\mathsf{ICB} = \mathsf{IV}||b$ where IV is a nounce.

4. Show that for all i, j we have $\mathsf{CB}_i \neq \mathsf{CB}'_j$.

5. Assuming there exists i, j such that $Y_i = Y'_j$, deduce some mutual information on X_i and X'_j.

6. We assume a model where an adversary can submit chosen plaintexts and receive a fresh ICB together with the corresponding ciphertext in return. Deduce a distinguisher which can submit a total number within the order of magnitude of 2^{64} blocks of plaintext and have an advantage within the order of magnitude of $\frac{1}{2}$.

We define two algorithms

authenticated encryption: $\mathsf{ENC}_K(P, A, \mathsf{IV}) = (C, T)$
given a plaintext P, and additional authenticated data A, and an initialization vector IV (to be used as a nounce), computes a ciphertext C and a t-bit tag T

authenticated decryption: $\mathsf{DEC}_K(\mathsf{IV}, A, C, T) = P$ (or fail)
given the initial vector, the additional authenticated data A, the ciphertext C, and the tag T, authenticates A and C and recovers the plaintext P or tell that A and C are not authenticated.

For simplicity, we assume that the length of C is multiple of 8 and that IV is of 96 bits.

Given a bitstring x of length at most 128, we define $\mathsf{pad}(x)$ the string x concatenated with enough zero bits to reach a full block length.

The authenticated encryption is defined by first letting H be the encrypted block by CIPH_K of the all-zero block, letting $J_0 = \mathsf{IV}||b$, letting $C = \mathsf{GCTR}_K(\mathsf{inc}(J_0), P)$, letting $S = \mathsf{GHASH}_H(\mathsf{pad}(A)||\mathsf{pad}(C)||\ell_A||\ell_C)$ where ℓ_A and ℓ_C are the bitlength of A and C respectively, and letting T be the t most significant bits of $\mathsf{GCTR}_K(J_0, S)$.

7. Define the authenticated decryption algorithm.

8. We define $\mathsf{GMAC}_K(A, \mathsf{IV}) = T$ for T such that there exists C such that $\mathsf{ENC}_K(\emptyset, A, \mathsf{IV}) = (C, T)$ where $\emptyset$ denotes a string of length zero.

   What kind of cryptographic primitive do we obtain?

9. Let H be as defined in the authenticated encryption. Let IV^i, $i = 1, \ldots, n$ be n arbitrary pairwise different initial vectors. They define J_0^i, $i = 1, \ldots, n$.

   Assuming that CIPH_K behaves like a perfect random function when K is random, show that for any pairwise different $h, j_1, \ldots, j_n$ we have $\Pr[H = h, J_0^i = j_i; i = 1, \ldots, n] = 2^{-128(n+1)}$.

10. Write how T is obtained depending on t, H, J_0, and A by using only the pad and GHASH functions.

11. We assume a model where the adversary can choose values for A and get a fresh IV and a 128-bit $T = \mathsf{GMAC}_K(A, \mathsf{IV})$ in return (i.e. $t = 128$). The goal of the adversary is to output an A that was not submitted together with any IV and the right value for $\mathsf{GMAC}_K(A, \mathsf{IV})$.

    Assuming that CIPH_K behaves like a perfect random function when K is random, show that the success probability of the adversary limited to n queries is upper bounded by $(m + 1)2^{-128}$.

    Hint: consider the case where the adversary outputs a fresh IV and the case where she reuses a received one. In the former case, show that the probability of success is bounded by 2^{-128}. In the latter case, show that it is bounded by $m2^{-128}$ where m is the maximum length in blocks of a value A.

Note: this exercise is inspired by publication NIST SP 800-38D, April 2006.