Family Name: ....

First Name: ....

Section: ....

Advanced Cryptography

Midterm Exam

May 22^{th}, 2007

Duration: 3 hours 45 minutes

This document consists of 11 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 the first page and have all pages *stapled*.

1 Substitution-Permutation Networks

We consider a block cipher $C : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ based on a substitution-permutation network (SPN). C is defined on n-bit plaintext x and k-bit key K and outputs an n-bit ciphertext y. C consists of $r-1$ rounds as described on Figure 1 followed by a round depicted on Figure 2.

Each round i uses a subkey K_i except for the last round which uses two subkeys K_r and K_{r+1}. All subkeys are derived from K.

Each round uses b substitution boxes (s-boxes) $S_1, \ldots, S_b$ in parallel over W and a bijective mapping $L : W^b \to W^b$ where $W = \{0,1\}^{\frac{n}{b}}$. We say that L is linear in the sense that $L(x+y) = L(x) + L(y)$ for any x and y.

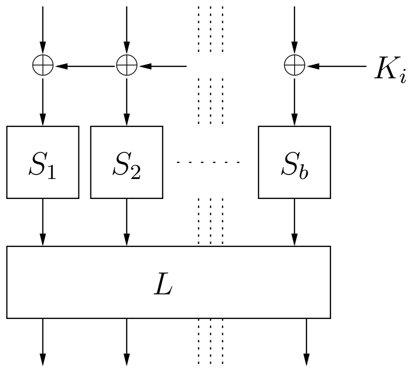

Figure 1: The i^{th} round of C for $1 \leq i < r$.

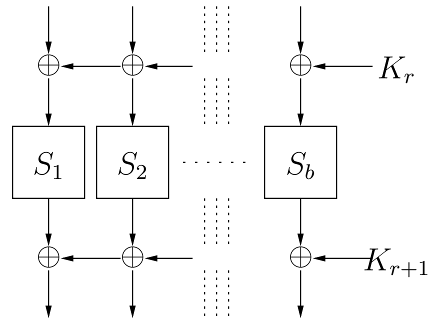

Figure 2: The last round of C.

1. What are the respective values of n, k, and b for the AES?

2. Which AES subroutine plays the role of L?

We define the *branch number* B of a linear mapping $f : W^b \leftarrow W^b$ by

$$B = \min_{x \neq 0} \left[\mathsf{hw}(x) + \mathsf{hw}\left(f(x)\right) \right]$$

where the $\mathsf{hw}(x)$ is the hamming weight *per element*, i.e. the number of non-zero W-element of the vector x (of b elements).

3. Show that $2 \leq B \leq b+1$.

4. Recall the definition of a multipermutation for f.

5. Show that a linear multipermutation from W^b to W^b is equivalent to a linear mapping with branch number equal to $b+1$.

6. What is the branch number B of L in the case of the AES?
   Hint: The 4x4 matrix in MixColumns defines a multipermutation.

Let X and X' be two *distinct* inputs of C and let $\Delta X = (\Delta X_1, \ldots, \Delta X_b) = X \oplus X'$. We say that the s-box S_i in round j is *active* if its input value is different from the $C_K(X)$ to the $C_K(X')$ calculations.

7. Let X and X' be two *distinct* inputs of C. Give ℓ, the minimum number of active s-boxes in terms of the branch number B when $r = 1$ and when $r = 2$.
   Deduce the value ℓ for the general case in terms of B and r.

We define the coefficient $\mathsf{DP}^S_{\max}$ of the s-boxes by

$$\mathsf{DP}^S_{\max} = \max_{\alpha \neq 0, \beta, i} \mathsf{DP}^{S_i}(\alpha, \beta)$$

A differential caracteristic of C is a tuple $\Omega = (\Delta_1, \Delta_2, \ldots, \Delta_{r+1})$ where Δ_i is the input difference at the round i for $1 \leq i \leq r$ and Δ_{r+1} is the output difference of C. We assume $\Delta_1 \neq 0$. We define

$$\mathsf{P}(\Omega) = \mathsf{DP}^{C_1}(\Delta_1, \Delta_2) \cdot \mathsf{DP}^{C_2}(\Delta_2, \Delta_3) \cdot \ldots \cdot \mathsf{DP}^{C_r}(\Delta_r, \Delta_{r+1}).$$

Let $\mathsf{P}_{\max} = \max_\Omega \mathsf{P}(\Omega)$.

8. Show that
$$\mathsf{P}_{\max} \leq \left(\mathsf{DP}^S_{\max}\right)^\ell$$
where ℓ is defined in question 7.

9. It can be shown that $\mathsf{DP}^S_{\max} = 2^{-6}$ for the AES. What is the value of $\mathsf{P}_{\max}$ for the AES when $r = 4, 6, 8$?

For simplicity, we consider that the AES is made of r *identical* rounds. In other words, the last round is equal to the previous ones.

10. Denote by G the two first rounds of AES "glued" together. What is the branch number of G?

11. Give a new bound on the maximal probability of a differential caracteristic $\mathsf{P}_{\max}$ of the AES on r rounds when r is even.

12. As before, $\mathsf{DP}^{S}_{\max} = 2^{-6}$ for the AES. What is the value of $\mathsf{P}_{\max}$ for the AES $r = 4, 6, 8$?

2 Finding Collisions

Let $\mathcal{D}$ be some finite set and $f : \mathcal{D} \to \mathcal{D}$ be a function defined on this set. Our objective is to find a collision on f, i.e., a pair $(x, y) \in \mathcal{D}^2$ such that $f(x) = f(y)$ and $x \neq y$. Given an initial element $x_0 \in \mathcal{D}$, define the sequence $\{x_i\}_{i \geq 0}$ by $x_i = f(x_{i-1})$.

1. Explain why the sequence *eventually* becomes periodic.

There must exist λ and μ such that $x_0, \ldots, x_{\mu+\lambda-1}$ are all distinct but $x_i = x_{i+\lambda}$ for all $i \geq \mu$. The elements $x_0, \ldots, x_{\mu-1}$ form the *tail* of the sequence, the elements $x_\mu, \ldots, x_{\mu+\lambda-1}$ constitute the *cycle* of the sequence. This is represented on Figure 3. Obviously, the pair $(x_{\mu-1}, x_{\mu+\lambda-1})$ is a collision for f.

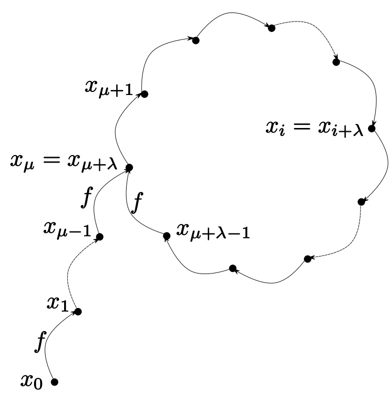

Figure 3: The tail and the cycle of the $\{x_i\}$ sequence.

2. We assume in this question that the exact value of λ is known (we will see later how to compute this value). Give the value of θ for which Algorithm 1 outputs a collision for f. Give, in terms of λ and μ, the total number of evaluations of the function f in this algorithm.

```
x ← x_0
y ← x_0
for i = 1, ..., θ do
    x ← f(x)
end
loop
    x' ← f(x)
    y' ← f(y)
    if x' = y' then return (x, y)
    x ← x'
    y ← y'
end
```

Algorithm 1: Finding a Collision on f when λ is known (for a given x_0).

From the previous question we know that, for a given x_0, the knowledge of λ is sufficient to efficiently find a collision on f. We now consider the problem of finding this value λ. For this we consider Algorithm 2, which outputs λ with probability p (when f is sampled uniformly at random) or loops forever.

```
x ← x_0
y ← x_0
i, j ← 0
loop
    x ← f(x)
    i ← i + 1
    if x = y then return i − j
    if x < y then y ← x and j ← i
end
```

Algorithm 2: Finding λ for a given x_0.

3. Explain in which case Algorithm 2 terminates and which case it does not. Deduce the value of p in terms of λ and μ.

4. Consider the case where Algorithm 2 terminates. Show that on average it performs $\mu + \frac{3}{2}\lambda$ evaluations of the function f.

Denoting N the cardinality of $\mathcal{D}$, it can be shown that on average $\mu = \lambda = \sqrt{\pi N/8}$.

5. Using the results of the previous questions, show that on average one needs $8 \cdot \sqrt{\pi N/8}$ evaluations of f to find a collision using algorithms 1 and 2. What can you say about the memory requirements of this method?

We now want to improve the running time of the previous method by using a *partitioning technique* in Algorithm 2. We replace Algorithm 2 by Algorithm 3. We denote p' the probability that Algorithm 3 outputs λ (so that this algorithm loops forever with probability $1 - p'$).

$x \leftarrow x_0$
$y_0, y_1, \ldots, y_{k-1} \leftarrow \infty$
$y_{x \bmod k} \leftarrow x$
$i, j_0, j_1, \ldots, j_{k-1} \leftarrow 0$
loop
  $x \leftarrow f(x)$
  $i \leftarrow i + 1$
  if $x = y_{x \bmod k}$ **then** return $i - j_{x \bmod k}$
  if $x < y_{x \bmod k}$ **then** $y_{x \bmod k} \leftarrow x$ and $j_{x \bmod k} \leftarrow i$
end

Algorithm 3: Finding λ for a given x_0 using k partitions.

6. Explain in which case Algorithm 3 terminates and which case it does not. Deduce the value of p' in terms of λ, μ, and k.

7. Let S denote the number of partitions for which the minimum lies on the cycle. Consider the case where Algorithm 3 terminates (so that $\Pr[S = 0] = 0$). Assuming (for simplicity) that $\mu = \lambda$, compute $\Pr[S = u]$ for $0 < k \leq u$.

8. Consider the case where Algorithm 3 terminates and assume that $\mu = \lambda$. Using the previous question, show that on average it performs $\mu + \lambda + \frac{\lambda}{k+1}(2 - \frac{k}{2^k-1})$ evaluations of the function f.

9. Assume that $1 \ll k \ll \sqrt{N}$ and that $\mu \approx \lambda \approx \sqrt{\pi N/8}$. Using the previous questions, show that on average one needs $5 \cdot \sqrt{\pi N/8}$ evaluations of f to find a collision using algorithms 1 and 3. What can you say about the memory requirements of this method?