

Family Name:

First Name:

Section:

Security and Cryptography

Fall semester 2007-2008

Final Exam

January 24th, 2008

Duration: 225 minutes

Part 1 / 2

This document consists of 12 pages.

Instructions

Documents are *not* allowed apart from linguistic dictionaries.

Electronic devices are *not* allowed.

Answers must be written on the exercise sheet.

This part of the exam contains 3 *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 of each part and have all pages *stapled*.

1 CBCMAC

Let k , b , and n be some integers and let $\text{MAC} : \{0, 1\}^k \times (\{0, 1\}^b)^* \rightarrow \{0, 1\}^n$ be a message authentication code.

1. What is a MAC forgery attack against a message authentication code?
Discuss on security models.

2. Ideally, considering $k > n$ what complexity (in terms of b , k , and n) should have the best MAC forgery attack against MAC?

We let

$$\text{CBCMAC}(K, x_1, \dots, x_m) = C(K, x_m \oplus \text{CBCMAC}(K, x_1, \dots, x_{m-1}))$$

and

$$\text{CBCMAC}(K, \emptyset) = 0^b$$

where $C : \{0, 1\}^k \times \{0, 1\}^b \rightarrow \{0, 1\}^b$ is a block cipher, \emptyset is an empty input, and 0^b is a bit-string of b bits all equal to 0.

3. Give the only possible value for n (in terms of b or k).

4. Explain how to make a MAC forgery attack against CBCMAC with a probability of success of 1 by using 3 chosen messages (or less).

2 Modulo 33 Calculus

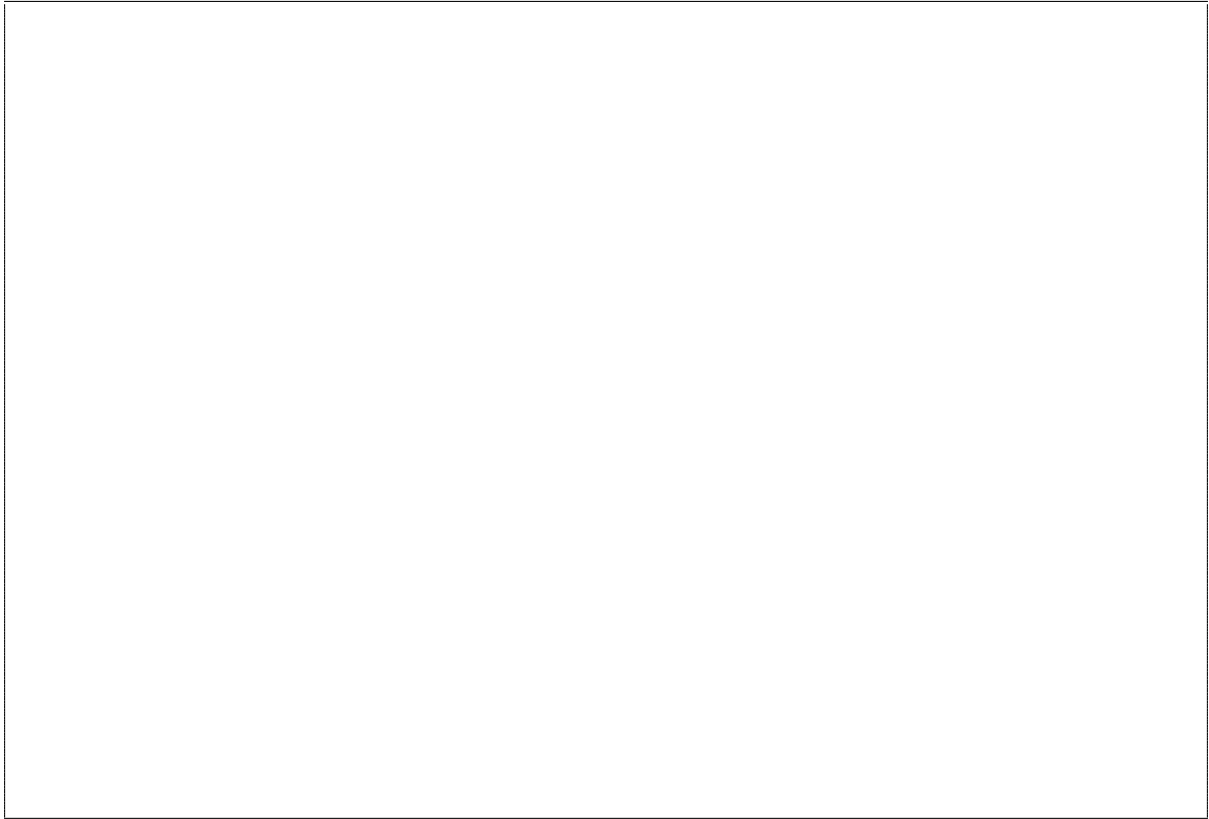
Let $d_{n-1} \dots d_1 d_0$ be the decimal expansion of an integer N , i.e. $d_i \in \{0, 1, \dots, 9\}$ and d_0 is the least significant digit of N .

Example: for $N = 789$ we have $d_0 = 9$, $d_1 = 8$, $d_2 = 7$.

1. Show that $N \equiv d_0 + d_1 + \dots + d_{n-1} \pmod{3}$.

2. Deduce an algorithm to reduce an integer modulo 3 by mental computing.

3. With the same notations, show that $N \equiv d_0 - d_1 + \cdots + (-1)^{n-1}d_{n-1} \pmod{11}$.



4. Deduce an algorithm to reduce an integer modulo 11 by mental computing.



Let a and b be arbitrary integers and let $N = 22a + 12b$.

5. Show that $N \equiv a \pmod{3}$ and $N \equiv b \pmod{11}$.



6. Show that N is the unique integer modulo 33 with the above properties.



7. By using the previous questions, compute $12341234^{56789} \bmod 33$.

3 RSA with Faulty Multiplier

Let p and q be two large ℓ -bit prime numbers such that :

$$q > 2^{\ell-1} + 2^{\ell-2} ,$$

$$p < 2^{\ell-1} + 2^{\ell-3} .$$

Let $N = p \cdot q$, e be such that $\gcd(e, (p-1)(q-1)) = 1$, and $d = e^{-1} \bmod ((p-1)(q-1))$.

We assume that an adversary can play with a black-box decryption device with the following properties:

- on query y , it returns $y^d \bmod N$;
- the internal RSA implementation uses the Chinese remainder acceleration; indeed, to decrypt an input y , it proceeds as follows:

$$\begin{array}{l} \text{first it computes} \end{array} \quad \begin{array}{l} y_p \leftarrow y \bmod p \\ d_p \leftarrow d \bmod (p-1) \\ x_p \leftarrow y_p^{d_p} \bmod p \end{array} \quad \text{and} \quad \begin{array}{l} y_q \leftarrow y \bmod q \\ d_q \leftarrow d \bmod (q-1) \\ x_q \leftarrow y_q^{d_q} \bmod q \end{array}$$

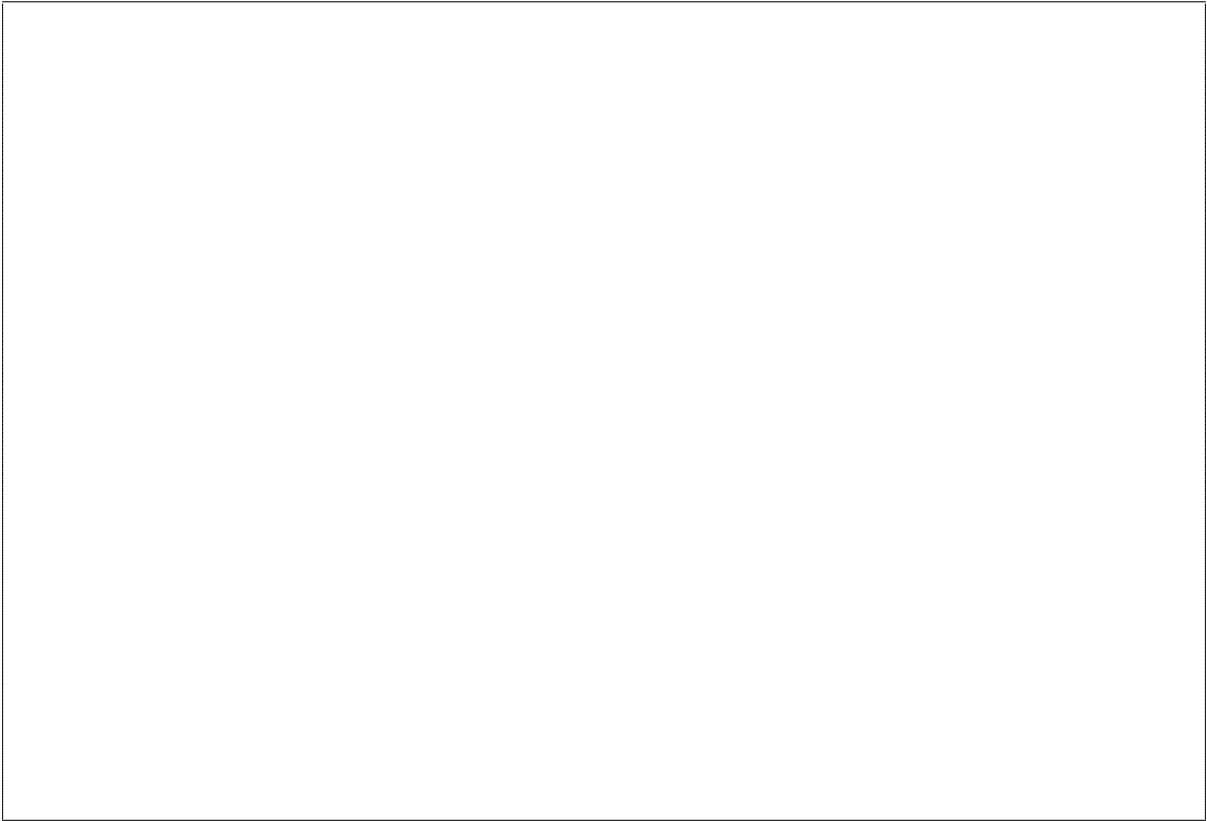
and then it reconstructs x by using some $x \leftarrow \text{CRT}(x_p, x_q)$ function;

- the internal microprocessor uses an optimized multiplier to multiply two 32-bit words together and return a 64-bit result;
- the multiplier has a bug inside such that when multiplying a special word α by a special word β leads to an incorrect result.

Let $y = y_{n-1} \parallel \dots \parallel y_1 \parallel y_0$ and $y^* = y_{n-1}^* \parallel \dots \parallel y_1^* \parallel y_0^*$ be numbers split into a sequence of 32-bit blocks, i.e. $y_i, y_i^* \in [0, 2^{32} - 1]$, $y = \sum_{i=0}^{n-1} y_i 2^{32i}$ and $y^* = \sum_{i=0}^{n-1} y_i^* 2^{32i}$.

1. Show how to implement a big number multiplier between y and y^* using a 32-bit multiplier.

2. Show that if y contains the blocks α and β , then the result of y^2 is likely to be wrong.



3. For any $y = 2^{\ell-1} + 2^{\ell-3} + u$ with $0 \leq u < 2^{\ell-3}$, show that we have $p < y < q$.

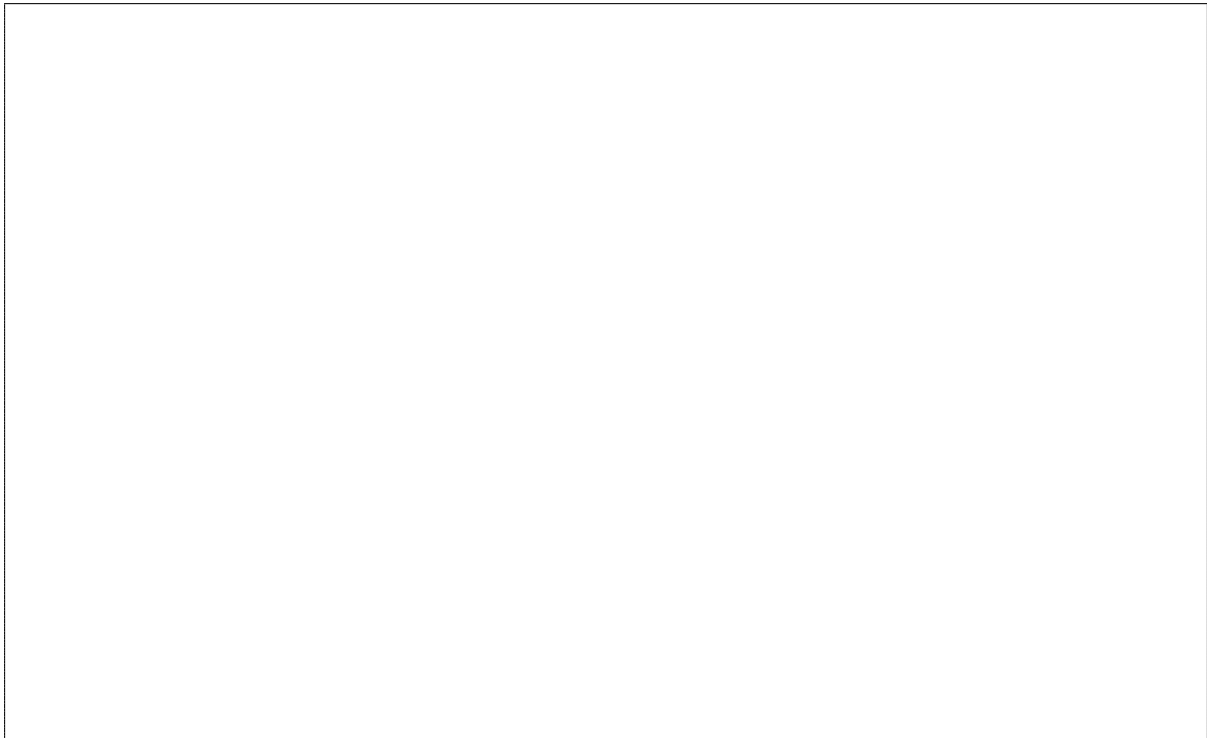


We consider an arbitrary string $y = 2^{\ell-1} + 2^{\ell-3} + u$ with $0 \leq u < 2^{\ell-3}$ such that when split into a sequence of 32-bit words, the words α and β are present in y . Let feed the decryption device with y and get the result z and let $y' = z^e \bmod N$.

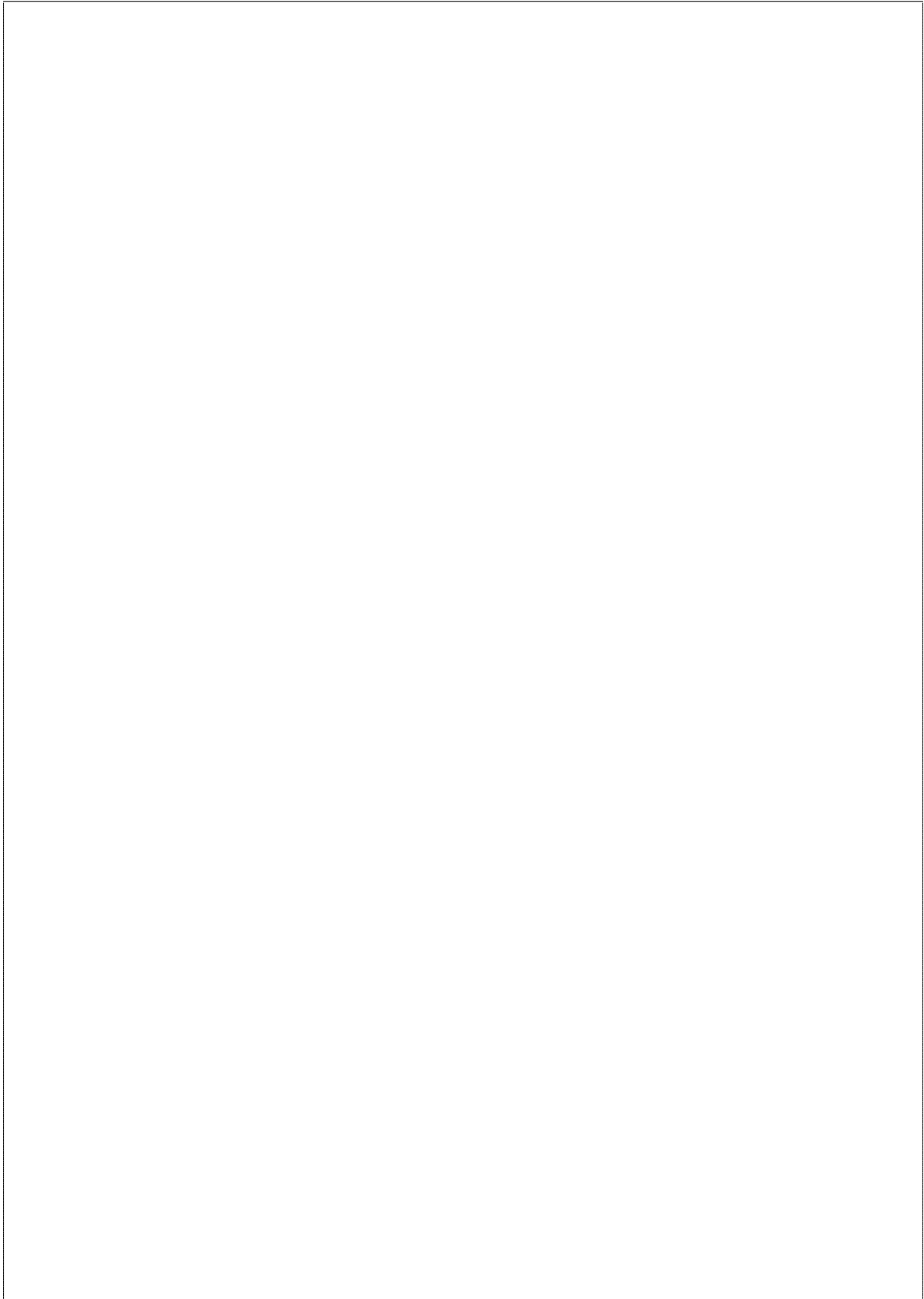
4. Show that $z \bmod q$ is likely to be incorrect in the sense that $y' \bmod q$ is not equal to $y \bmod q$.



5. Show that $z \bmod p$ is likely to be correct in the sense that $y' \bmod p$ is equal to $y \bmod p$.



6. From y' , y , and N show how to efficiently recover p and q .



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

Please be patient.