



ÉCOLE POLYTECHNIQUE  
FÉDÉRALE DE LAUSANNE

Family Name: .....

First Name: .....

Section: .....

# Advanced Cryptography

Final Exam

July 18<sup>th</sup>, 2006

Start at 9:15, End at 12:00

This document consists of 12 pages.

## Instructions

Electronic devices are *not* allowed.

Answers must be written on the exercises sheet.

This exam contains 1 exercise.

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*.

## An RSA Variant with Public Exponent 3

In this problem, we consider a special variant of RSA with public exponent  $e$  that is *not* coprime with  $\varphi(N)$ . For simplicity, we focus on  $e = 3$ . More precisely, key generation works as follows:

- pick  $r_1$  of  $\frac{s}{2}$  bits at random until  $p = 9r_1 - 2$  is prime
- pick  $r_2$  of  $\frac{s}{2}$  bits at random until  $q = 3r_2 - 1$  is prime
- take  $N = pq$ ,  $e = 3$
- public key is  $(N, e)$ , secret key is  $(p, q)$

### Cubic Residuosity

1. Let  $x \in \mathbf{Z}_q^*$ .

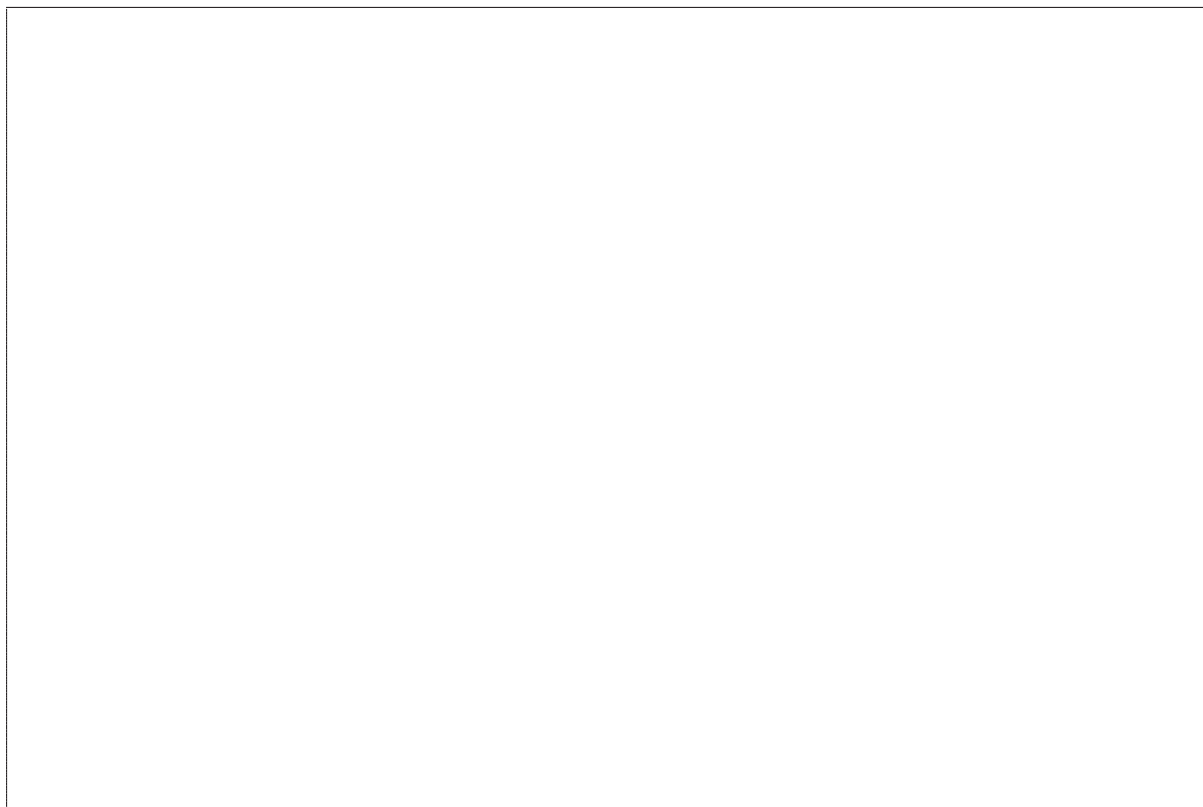
How many cubic roots can we have?

How to compute cubic roots in  $\mathbf{Z}_q^*$ ?

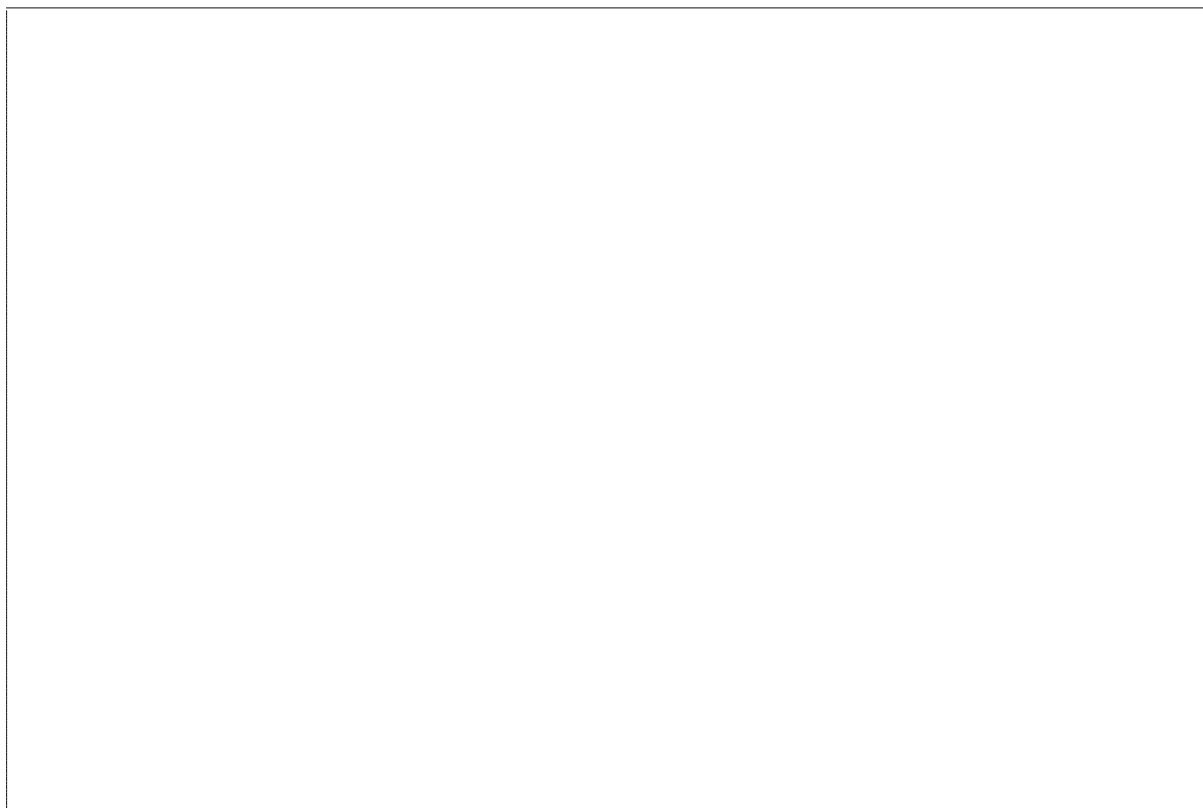
2. Let  $x \in \mathbf{Z}_p^*$ .

Show that  $(x^3)^{\frac{p+2}{9}}$  is a cubic root of  $x^3$ .

3. Given  $x \in \mathbf{Z}_p^*$ , how many cubic roots can we have in  $\mathbf{Z}_p^*$ ?



4. By using the Jacobi symbol and its computation rules, prove that  $-3$  is a quadratic residue in  $\mathbf{Z}_p^*$ .



5. Let  $j = \frac{\theta-1}{2} \pmod p$  where  $\theta$  is a square root of  $-3$ .  
Show that  $j^3 \pmod p = 1$ .

6. Deduce all cubic roots of 1 in  $\mathbf{Z}_p^*$ .

7. Deduce a way to compute all cubic roots of cubic residues in  $\mathbf{Z}_p^*$ .



8. By using the Chinese Remainder Theorem, tell how many cubic roots cubic residues have in  $\mathbf{Z}_N^*$  and how to compute them.



We now denote  $\text{Root}(y, p, q)$  the function mapping any  $y \in \mathbf{Z}_N^*$  to the set of all its cubic roots using the secret key. This function will be used throughout this problem.

### Complexity of Cubic Roots

1. If  $x, y \in \mathbf{Z}_N^*$  are such that  $x \not\equiv y \pmod{N}$  and  $x^3 \equiv y^3 \pmod{N}$ , show that  $\gcd(x - y, N) = q$ .

2. Deduce that an oracle who can extract one cubic root from a cubic residue in  $\mathbf{Z}_N^*$  can be used to factor  $N$ .

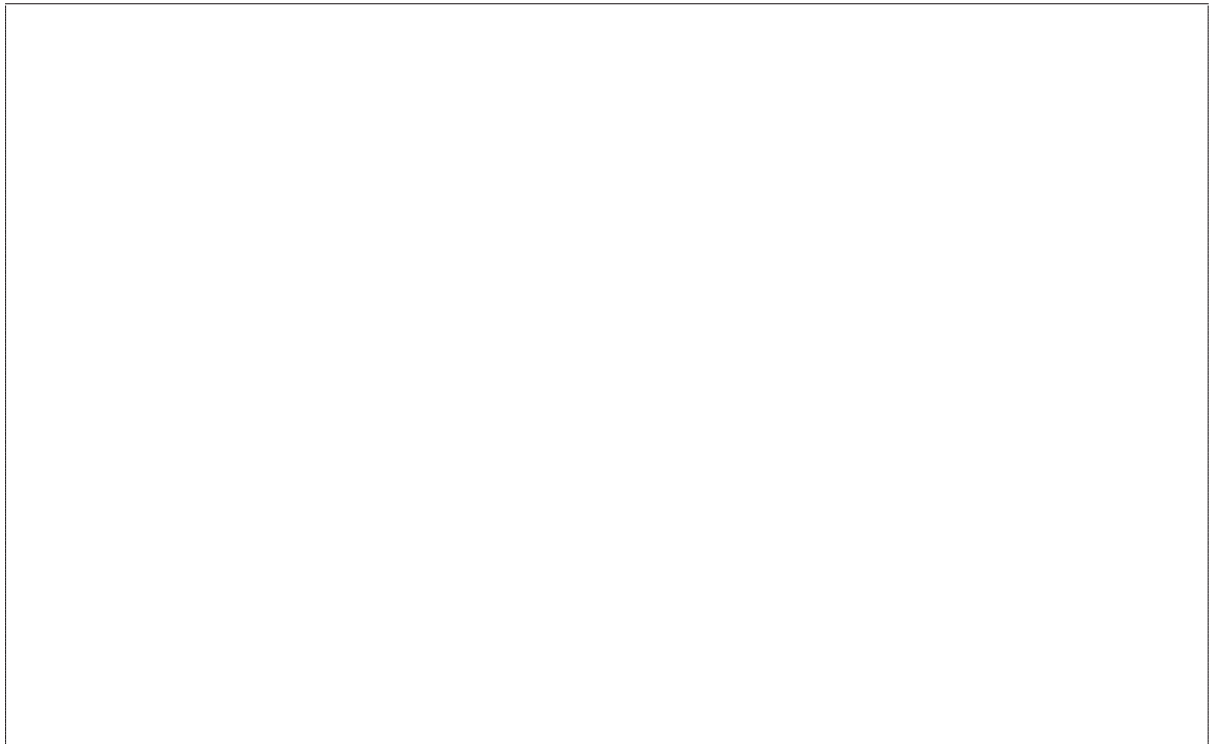
## Raw Encryption and Decryption

We consider the message space  $\mathbf{Z}_N^*$ . Encryption is made as in RSA, by raising to the power  $e$  modulo  $N$ .

1. Show that decryption is ambiguous.



2. Devise a chosen ciphertext attack.



## Encryption and Decryption on a Reduced Space

Let  $n$  be such that  $2^n \ll N$ . Let  $F$  be a random injection from  $\{0,1\}^n$  to  $\mathbf{Z}_N^*$  which is easy to invert. We now consider the message space  $\{0,1\}^n$ . We define the encryption of  $x$  by  $F(x)^e \bmod N$ .

1. How can we decrypt now?

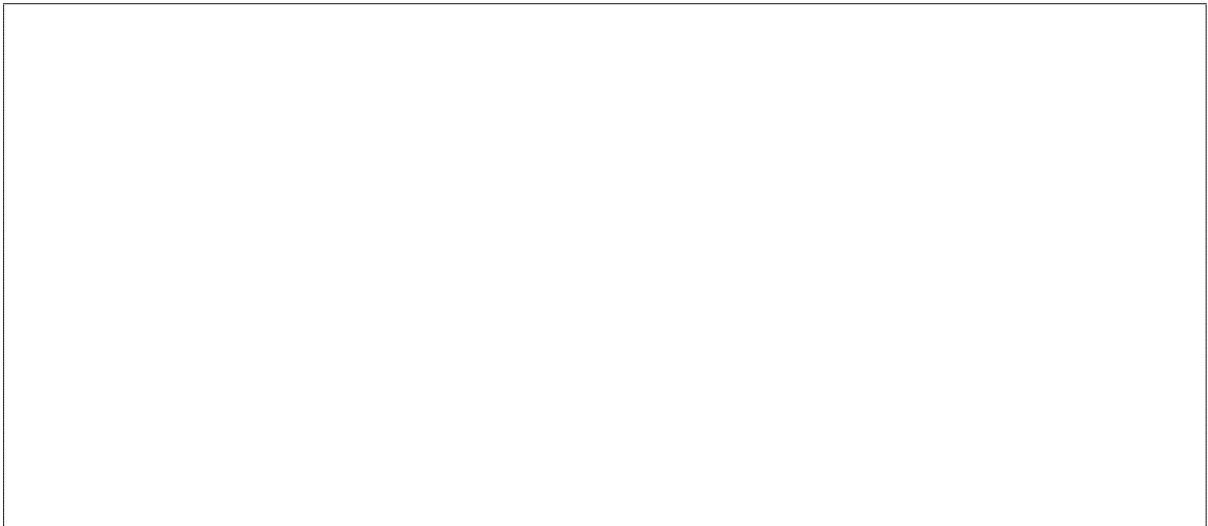
2. What is the probability (over the choice of  $F$ ) that there exists  $x$  such that decrypting the encryption of  $x$  does not produce  $x$ ?



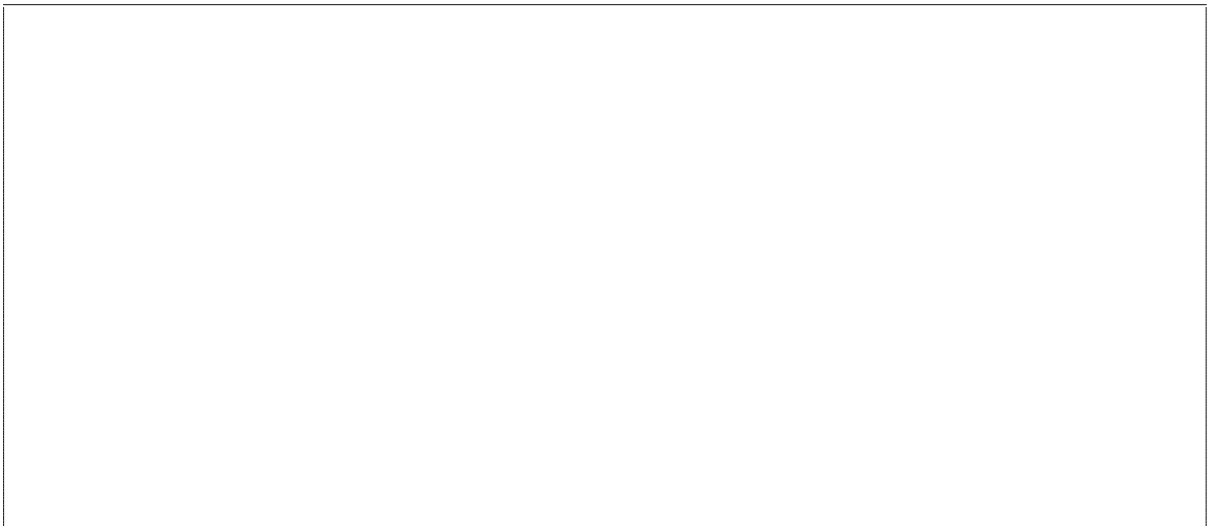
3. Show that key recovery is equivalent to factoring numbers like  $N$ .



4. What can we now say about the decryption problem?



5. Give at least one Boolean function on the plaintext that is not a hard core bit.



## Probabilistic Variant

Let  $n$  and  $k$  be integers such that  $k < n$ . We now consider that the message space is a binary code of length  $n$  and dimension  $k$ . We consider a symmetric encryption scheme over the plaintext/ciphertext space  $\{0, 1\}^n$  and keyspace  $\mathcal{K}$  defined by **SymEnc** and **SymDec** algorithms. Let  $H$  be a random function from  $\mathbf{Z}_N^*$  to  $\mathcal{K}$ . To encrypt a codeword  $x$ , we first pick a random  $r \in \mathbf{Z}_N^*$  and we compute  $y = \text{SymEnc}_{H(r)}(x)$  and  $z = r^e \bmod N$ . The ciphertext is  $(y, z)$ .

1. How to decrypt?

2. Assuming that the symmetric encryption is ideal and that  $\mathcal{K}$  is large enough, what is the probability that decryption is ambiguous?

3. Recall what is an adversary against the semantic security.

4. Assume that we have an adversary  $\mathcal{A}$  playing the semantic security game against our new cryptosystem. We assume that the symmetric encryption scheme is an ideal cipher, that is,  $H(r)$  fully specifies a random permutation over  $\{0, 1\}^n$ . We further assume that function  $H$  is only available through an oracle  $\mathcal{O}$ , that is, nobody can reliably compute  $H(r)$  without querying the oracle  $\mathcal{O}$  with  $r$  to get  $H(r)$  in return. This way,  $\mathcal{A}$  may query the oracle  $\mathcal{O}$  while playing the semantic security game.

- (a) Show that if  $\mathcal{A}$  does not query  $\mathcal{O}$  with the  $r$  chosen by the challenger, the advantage of  $\mathcal{A}$  in the semantic game is zero.

- (b) By simulating  $\mathcal{O}$  and several parts of the semantic game, deduce that if the advantage of  $\mathcal{A}$  is  $\varepsilon$ , we can transform  $\mathcal{A}$  in an algorithm which given  $z = r^3 \pmod N$  for a random  $r$  can deduce  $r$  or other cubic roots of  $z$  with probability  $\varepsilon$ .

(c) Deduce that if the advantage of  $\mathcal{A}$  is  $\varepsilon$ , we can factor  $N$  with probability  $\varepsilon$ .

(d) Deduce that if factoring  $N$  is hard, if the symmetric encryption is ideal, and if  $H$  is a random oracle, this cryptosystem is semantically secure.