SECURITY AND CRYPTOGRAPHY LABORATORY

Family Name: ....

First Name: ....

Section: ....

Security and Cryptography

Midterm Exam

October 30$^{\text{th}}$, 2008

Duration: 1 hour 45 min

This document consists of 12 pages.

Instructions

Documents are *not* allowed apart from linguistic dictionaries.

Electronic devices (including *calculators*) are *not* allowed.

Answers must be written on the exercises sheet.

This 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 and have all pages *stapled*.

1 Square roots of 53 modulo 221

The purpose of this exercise is to solve in $\mathbf{Z}_n$ the equation

$$x^2 \equiv a \pmod{n}$$

with $n = 221$ and $a = 53$.

1. Let $n = pq$ be the factorization of n into prime numbers where p is the smallest one. Compute p and q.

2. Solve in $\mathbf{Z}_p$ the equation $x^2 \equiv a$.

3. Solve in $\mathbf{Z}_q$ the equation $x^2 \equiv a$.

4. Reduce $\alpha = 170$ modulo p and modulo q.

5. Reduce $\beta = 1 - \alpha$ modulo p and modulo q.

6. Given arbitrary u and v, reduce $u\alpha + v\beta$ modulo p and q.

7. List all roots in $\mathbf{Z}_n$ of the equation $x^2 \equiv a$.

2 RSA with exponent 3

In this exercise we consider an RSA modulus $n = pq$ where p and q are large prime numbers (here, by "large" we mean at least equal to 5). We consider a valid RSA exponent e for RSA.

1. Show that neither $p \mod 3$ nor $q \mod 3$ can be equal to 0.

2. Under which condition e is a valid exponent for a modulus n?

From now on, we will assume that $e = 3$.

3. Show that neither $p - 1$ nor $q - 1$ can be multiples of 3.

4. Deduce that $p \bmod 3 = q \bmod 3 = 2$.

5. What is the value of $n \bmod 3$?

6. For any digits $d_0, \ldots, d_{\ell-1}$, show that

$$\left(\sum_{i=0}^{\ell-1} d_i 10^i\right) \bmod 3 = \left(\sum_{i=0}^{\ell-1} (d_i \bmod 3)\right) \bmod 3$$

7. Show that $e = 3$ is not a valid RSA exponent for the following RSA modulus:

$$n = 777\,575\,993$$

3 Computation in $\mathsf{GF}(16)$

Let us consider the polynomial $P(x) = x^4 + x + 1$ in $\mathbf{Z}_2[x]$.

1. Show that P has no root in $\mathbf{Z}_2$.

2. Deduce that P has no factor of degree 1 in $\mathbf{Z}_2[x]$.

3. Enumerate all polynomials of degree 2 in $\mathbf{Z}_2[x]$ and identify the one $Q(x)$ which is irreducible.

4. Show that $Q(x)$ does not divide $P(x)$.

5. Deduce that $P(X)$ is irreducible.

6. We define

$$\mathsf{GF}(16) \leftrightarrow \{0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F\}$$

where an hexadecimal $u = \alpha 2^0 + \beta \times 2^1 + \gamma \times 2^2 + \delta \times 2^3$ with $\alpha, \beta, \gamma, \delta \in \{0,1\}$ is considered to represent the polynomial

$$\alpha + \beta x + \gamma x^2 + \delta x^3 \text{ in } \mathsf{GF}(16)$$

Those polynomials in $\mathbf{Z}_2[x]$ are taken modulo $P(x)$.

(a) What is the $\mathsf{GF}(16)$-sum of 6 and A?

(b) What is the $\mathsf{GF}(16)$-multiplication of 6 and 1?

(c) What is the $\mathsf{GF}(16)$-multiplication of 6 and 2?

(d) What is the $\mathsf{GF}(16)$-multiplication of 6 and 3?

(e) What is the $\mathsf{GF}(16)$-inverse of 2?

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

Please be patient.