LASEC

SECURITY AND CRYPTOGRAPHY LABORATORY

Family Name:..........................

First Name:...........................

Section:..............................

Security and Cryptography

Midterm Exam (Solutions)

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

Duration: 1 hour 45 min

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.

   Since $13 \times 17 = 221$ *we have* $p = 13$ *and* $q = 17$*.*

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

   We have $a \bmod p = 53 \bmod 13 = 1$*. Since* p *is a prime number the only square roots of* $+1$ *are* $+1$ *and* -1*. That is,* $x \bmod p$ *is either 1 or 12.*

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

   We have $a \bmod q = 2$*. We have* $a^{\frac{q-1}{2}} = 2^8 \pmod{17}$*. This is* $(-1)^4 \bmod 16$ *which is 1, so* a *is a quadratic residue. To find a square root, we can try by exhaustive search as* q *is pretty small. The list of squares modulo 17 is* $1, 4, 9, 16, 8, 2, \ldots$ *so 6 is a quare root of 1. The second square root is* $-6 = 11 \pmod{17}$*.*

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

   We compute $170 \bmod p = 1$ *and* $170 \bmod q = 0$

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

   Clearly, $(1 - 170) \bmod p = 0$ *and* $(1 - 170) \bmod q = 1$

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

Clearly, $(u\alpha + v\beta) \bmod p = u \bmod p$ *and* $(u\alpha + v\beta) \bmod q = v \bmod q$

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

We use the Chinese remainder theorem. We have $x^2 \bmod n = a \iff x^2 \bmod p = a \bmod p$ *and* $x^2 \bmod q = a \bmod q$*. The right hand side suggests 4 solutions such that* $x \bmod p \in \{1, 12\}$ *and* $x \bmod q \in \{6, 11\}$*. Using the previous question we compute* x *by*

$$\begin{aligned}
1 \times \alpha + 6 \times \beta &= 170 \times (1 - 6) + 6 \\
1 \times \alpha - 6 \times \beta &= 170 \times (1 + 6) - 6 \\
-1 \times \alpha + 6 \times \beta &= 170 \times (-1 - 6) + 6 \\
-1 \times \alpha - 6 \times \beta &= 170 \times (-1 + 6) - 6
\end{aligned}$$

We do the computation modulo 221 and obtain $x \in \{40, 79, 142, 181\}$.

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.

> *Since p and q are large, they are larger than 3. Since they are prime, they are not divisible by 3.*

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

> *e is a valid exponent iff it is coprime with $\varphi(n) = (p-1)(q-1)$.*

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

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

> *If $e = 3$ is a valid exponent, then $(p-1)(q-1)$ is coprime with 3, which means that it is not divisible by 3. Therefore, neither $p-1$ nor $q-1$ can be divisible by 3.*

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

> *Due to the previous questions, $p \bmod 3$ is neither 0 nor 1 so it must be 2. The same holds for q.*

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

> *We have $n = p \times q = 2^2 = 1 \pmod 3$.*

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

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

> *This directly comes from $10 \bmod 3 = 1$.*

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

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

> *From the previous question we have $n \bmod 3 = (1+1+1+2+1+2+0+0+0) \bmod 3 = 2$ which is not equal to 1. So, either n is not a product of two primes or 3 is not a valid exponent. In any case, $(n, 3)$ is not a valid RSA public key.*

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 $\mathbf{Z}_2$.

   We have $P(0) = 1$ and $P(1) = 1$ so it has no root in $\mathbf{Z}_2$.

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

   Having a factor of degree 1 is equivalent to having a root. So, P has no factor of degree 1.

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

   We have x^2, x^2+1, x^2+x, x^2+x+1. We can check that all have roots, except x^2+x+1. So, only x^2+x+1 remains as a candidate for being irreducible. Since it has degree 2, having no factor of degree 1 is enough to guaranty irreducibility. Hence, $Q(x) = x^2+x+1$ is the only irreducible polynomial of degree 2.

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

   We have $P(x) = x^4 + x + 1 = (x^2 + x) \times Q(x) + 1$ so $P(x)$ is not divisible by $Q(x)$.

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

   $P(x)$ has degree 4 and no factor of degree 1. Thus, either it has two irreducible factors of degree 2 or it is irreducible. Since $Q(x)$ is the only irreducible polynomial of degree 2 and is not a factor of $P(x)$, $P(x)$ must be 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?

We have $6 = 2^2 + 2^1$ *so it represents* $x^2 + x$. *We have* $A = 2^3 + 2^1$ *so it represents* $x^3 + x$. *Thus, the sum is* $x^3 + x^2$ *which is represented by* $2^3 + 2^2 = C$: $6 \boxplus A = C$.

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

Since 1 represents 1, the multiplication by 1 is trivial: $6 \boxtimes 1 = 6$.

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

Since 2 represents x, *the multiplication by 2 can be done by shifting bits (if no carry). 6 represents* $x^2 + x$ *which is shifted to* $x^3 + x^2$, *represented by* C: $6 \boxtimes 2 = C$.

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

We can check that $3 = 2 \boxplus 1$ *(indeed). We have* $6 \boxtimes 3 = (6 \boxtimes 2) \boxplus (6 \boxtimes 1) = C \boxplus 6 = A$.

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

We have $x^4 + x + 1 = x \times (x^3 + 1) + 1$ *so* $0 = (2 \boxtimes 9) \boxplus 1$ *which can also writes* $2 \boxtimes 9 = 1$: *9 is the inverse of 2.*