Cryptography and Security — Midterm Exam

Serge Vaudenay

6.12.2013

- duration: 3h00
- no document is allowed except one two-sided sheet
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will *not* answer any technical question during the exam
- the answers to each exercise must be provided on separate sheets
- readability and style of writing will be part of the grade
- do not forget to put your name on every sheet!

1 Ambiguous Power

We let $n = pq$ be the product of two different prime numbers p and q. We assume that $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are odd and coprime.

Q.1 Show that there exists $z \in \mathbf{N}$ such that $z \equiv 3 \pmod p$ and $z \equiv 5 \pmod q$ and give a method to compute it.

Q.2 Explain how to find some exponent $e \in \mathbf{N}$ such that for every $x \in \mathbf{Z}_n^*$, we have $x^e \equiv x^3 \pmod p$ and $x^e \equiv x^5 \pmod q$.
NOTE: we do expect a complete mathematical proof for this question.

Q.3 Application: find such e for $p = 7$ and $q = 11$.

Q.4 More generally, under which condition on $e_p \in \mathbf{N}$ and $e_q \in \mathbf{N}$ does some $e \in \mathbf{N}$ exist such that $x^e \equiv x^{e_p} \pmod p$ and $x^e \equiv x^{e_q} \pmod q$ for all $x \in \mathbf{Z}_n^*$?

Q.5 Could this be interesting to compute two RSA encryptions in parallel (with public keys (n_1, e_1) and (n_2, e_2)) in one exponentiation instead of two?

2 Cubic Roots

Let p be an odd prime number.

Q.1 In this question only, we assume that $p \bmod 3 = 2$. Show that every $x \in \mathbf{Z}_p^*$ has exactly one cubic root and propose a method to compute it.

Q.2 (From now on, we assume that $p \bmod 3 = 1$.) Show that -1 is a quadratic residue in $\mathbf{Z}_p$ if and only if $p \bmod 4 = 1$.
HINT: invoke Legendre.

Q.3 (We recall that $p \bmod 3 = 1$.) By considering two cases, compute the Legendre symbol $(3/p)$.
HINT: we recall the rules to compute the Jacobi symbol:
- $\left(\frac{a}{b}\right) = \left(\frac{a \bmod b}{b}\right)$ for b odd,
- $\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right)$ for c odd,
- $\left(\frac{2}{a}\right) = 1$ if $a \equiv \pm 1 \pmod 8$ and $\left(\frac{2}{a}\right) = -1$ if $a \equiv \pm 3 \pmod 8$ for a odd,

- $\left(\frac{a}{b}\right) = -\left(\frac{b}{a}\right)$ if $a \equiv b \equiv 3 \pmod 4$ and $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$ otherwise for a and b odd.

Q.4 (We recall that $p \bmod 3 = 1$.) Show that -3 is a quadratic residue.

Q.5 (We recall that $p \bmod 3 = 1$.) Set j a square root of -3.
Show that $\frac{-1+j}{2}$ is a cubic root of 1. What are the two others?

Q.6 (We recall that $p \bmod 3 = 1$.) Show that for all $x \in \mathbf{Z}_p^*$, x has either 0 or 3 cubic roots.

Q.7 If $p \bmod 9 = 7$, show that if x is a cubic residue, then $x^{\frac{p+2}{9}} \bmod p$ is a cubic root of x.
By using j from Q.5, express the two others.

Q.8 Propose a variant to RSA in which we would use $e = 3$ but with e and $\varphi(n)$ not coprime.

3 Elliptic Curves with Projective Coordinates

In this exercise, we consider a prime number $p > 3$. Given $a, b \in \mathbf{Z}_p$ such that $\Delta = -16(4a^3 + 27b^2) \neq 0$, we consider an elliptic curve

$$E_{a,b} = \{\mathcal{O}\} \cup \{(x,y) \in \mathbf{Z}_p^2; y^2 = x^3 + ax + b\}$$

We recall that for $P = (x_p, y_p) \in E_{a,b}$, we define $-P = (x_P, -y_P)$ and that for $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ such that $Q \neq -P$, we define $P + Q = R$ with $R = (x_R, y_R)$ computed by

$$\lambda = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} & \text{if } x_P \neq x_Q \\ \frac{3x_P^2 + a}{2y_P} & \text{if } x_P = x_Q \end{cases}$$
$$x_R = \lambda^2 - x_P - x_Q$$
$$y_R = (x_P - x_R)\lambda - y_P$$

The definition of $-P$ and of $P + Q$ is straightforward in other cases of $P, Q \in E_{a,b}$.

In this exercise, we let T_{mul} be the time complexity of one full-size multiplication in $\mathbf{Z}_p$ and T_{inv} be the time complexity of one inversion in $\mathbf{Z}_p^*$. We assume that the cost of addition and of multiplication by 2 or 3 can be neglected. We also assume that the cost of a square is the same as T_{mul}. The exercises is based on the fact that $T_{\mathsf{inv}} > T_{\mathsf{mul}}$.

Q.1 Using the recalled formulas, what is the cost of computing $P+Q$ in the $P, Q \in E_{a,b} - \{\mathcal{O}\}$ and $Q \neq -P$ case?

Q.2 We define
$$E'_{a,b} = \{(x,y,z) \in \mathbf{Z}_p^3; y^2 z = x^3 + axz^2 + bz^3\} - \{(0,0,0)\}$$
and a mapping $f : E'_{a,b} \to E_{a,b}$ by $f(x,y,z) = (\frac{x}{z}, \frac{y}{z})$ for $z \neq 0$ and $f(x,y,z) = \mathcal{O}$ otherwise. We propose to *represent* points of $E_{a,b}$ by one preimage by f. Under which condition do two elements of $E'_{a,b}$ represent the same point in $E_{a,b}$?

Q.3 With the same notations, given $P, Q \in E'_{a,b}$, we define $R = P + Q$ by

$$u = y_Q z_P - y_P z_Q$$
$$v = x_Q z_P - x_P z_Q$$
$$x_R = v(z_Q(z_P u^2 - 2x_P v^2) - v^3)$$
$$y_R = z_Q(3x_P u v^2 - y_P v^3 - z_P u^3) + u v^3$$
$$z_R = v^3 z_P z_Q$$

Show that $f(P+Q) = f(P) + f(Q)$ in the $P \neq Q$ case.
HINT: first observe $\lambda = \frac{u}{v}$, then compute $\frac{x_R}{z_R}$ and $\frac{y_R}{z_R}$.

Q.4 With the same notations and the proposed representation of points in $E_{a,b}$, what is now the cost of computing $P + Q$?
For which ratio $T_{\mathsf{inv}}/T_{\mathsf{mul}}$ is this competitive in the $P \neq Q$ and $P + Q \neq \mathcal{O}$ case?
HINT: think of reusing some intermediate results.

Q.5 If we do cryptographic operations involving a secret and using the proposed representation method of points, the element of $E'_{a,b}$ may leak some information about the computation. Propose a way to randomize the representation so that it does not leak more than the point itself.