Cryptography and Security — Midterm Exam
Solution

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!

The exam grade follows a linear scale in which each question has the same weight.

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.

> *Since p and q are different prime numbers, they are coprime. So, we can use the Chinese remainder theorem. Let $\alpha = q(q^{-1} \bmod p)$ and $\beta = p(p^{-1} \bmod q)$. The number $z = 3\alpha + 5\beta$ is such that $z \bmod p = 3$ and $z \bmod q = 5$.*

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.

> *Since $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are odd and coprime, 2, $\frac{p-1}{2}$, and $\frac{q-1}{2}$ are coprime. So, we can use the Chinese remainder theorem and find e such that $e \bmod 2 = 1$, $e \bmod \frac{p-1}{2} = 3$ and $e \bmod \frac{q-1}{2} = 5$. Clearly, e and 3 are equal modulo 2 and modulo $\frac{p-1}{2}$, so they are equal modulo $p-1$. Similarly, e and 5 are equal modulo 2 and modulo $\frac{q-1}{2}$, so they are equal modulo $q-1$. So, $x^e \equiv x^{e \bmod (p-1)} \equiv x^3 \pmod p$ and $x^e \equiv x^{e \bmod (q-1)} \equiv x^5 \pmod q$.*

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

> *Let $\alpha = 15$, $\beta = 10$, and $\gamma = 6$. We take $e = \alpha + 0\beta + 0\gamma = 15$ and obtain $e \bmod 2 = 1$, $e \bmod 3 = 3 \bmod 3$, and $e \bmod 5 = 5 \bmod 5$. We can check that $e \bmod 6 = 3$ and $e \bmod 10 = 5$.*

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 $x \in \mathbf{Z}_n^*$?

For such e to exist, it is necessary that $e \equiv e_p \pmod{p-1}$ and $e \equiv e_q \pmod{q-1}$. Since both $p-1$ and $q-1$ are even, it is necessary that $e \equiv e_p \pmod 2$ and $e \equiv e_q \pmod 2$. So, it is necessary that $e_p \equiv e_q \pmod 2$.
This condition is also sufficient: if $e_p \equiv e_q \pmod 2$, we construct using the Chinese remainder theorem e such that $e \equiv e_p \pmod 2$ (so, we also have $e \equiv e_q \pmod 2$), $e \equiv e_p \pmod{\frac{p-1}{2}}$, and $e \equiv e_q \pmod{\frac{q-1}{2}}$. Since $e \equiv e_p \pmod 2$ and $e \equiv e_p \pmod{\frac{p-1}{2}}$, we deduce $e \equiv e_p \pmod{p-1}$. So, $x^e \equiv x^{e_p} \pmod p$. Similarly, we have $e \equiv e_q \pmod{q-1}$. So, $x^e \equiv x^{e_q} \pmod q$.

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?

Computing $x^{e_1} \bmod n_1$ is done using $(\log_2 n_1)^2 \log_2 e_1$ steps. Computing $x^{e_2} \bmod n_2$ is done using $(\log_2 n_2)^2 \log_2 e_2$ steps. Computing $x^e \bmod (n_1 n_1)$ is done using $(\log_2(n_1 n_2))^2 \log_2 e$ steps. Since e is likely to be of same size as $n_1 n_2$, this requires $(\log_2(n_1 n_2))^3$ steps.
If $n_1 \approx n_2 \approx 2^\ell$ and $e_1 \approx e_2 \approx 2^\varepsilon$, the two RSA operations roughly take $2\ell^2\varepsilon$ steps. The combined computation takes $8\ell^3$ steps. So, this is not interesting.
In the case that $e_1 = e_2$, the same computation gives $4\ell^2\varepsilon$. So, this is not interesting either.
Actually, the CRT acceleration consists of doing in in the other way: instead of computing one exponentiation modulo a large modulus, it is more interesting to compute several modulo pieces of the modulus.

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.

> *If* $p \bmod 3 = 2$*, then* 3 *is coprime with* $p-1$*. So,* $y \equiv x^3 \pmod p$ *is equivalent to* $y^e \equiv x \pmod p$*, where* $e = 3^{-1} \bmod (p-1)$*. So,* y *has a unique cubic root which is* $y^e \bmod p$*.*

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.

> -1 *is a quadratic residue if and only if* $(-1/p) = +1$*. We have* $(-1/p) = (-1)^{\frac{p-1}{2}}$ *by definition. So,* $(-1/p) = +1$ *if and only if* $\frac{p-1}{2}$ *is even, which is equivalent to* $p \bmod 4 = 1$*.*

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.

> *Using the quadratic reciprocity leads to distinguishing whether* $p \bmod 4 = 3$ *or not, since* $3 \bmod 4 = 3$*. If* $p \bmod 4 = 3$*, we have* $(3/p) = -(p/3) = -(1/3) = -1$*. If* $p \bmod 4 = 1$*, we have* $(3/p) = (p/3) = (1/3) = 1$*.*

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

> *Based on the previous questions, we can see that* $(-3/p) = (-1/p).(3/p) = 1$ *in any case. So,* -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?

> *Let* $\theta = \frac{-1+j}{2}$*.*
> *We have* $\theta^2 = \frac{1-2j+j^2}{4} = \frac{-1-j}{2}$*. Then,* $\theta^3 = \theta^2\theta = \frac{1-j^2}{4} = 1$*.*
> *The two others are* 1 *and* $\theta^2 = \frac{-1-j}{2}$*.*

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.

If x has a cubic root y, then $y\theta$ and $y\theta^2$ are two other cubic roots. We cannot have more than 3 cubic roots in a field. So, either we have none, or we have exactly 3.

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.

As in Q.5, we let j denote a square root of -3 and $\theta = \frac{-1+j}{2}$. Let $y = x^{\frac{p+2}{9}} \bmod p$. If $x = z^3 \bmod p$, then

$$y^3 \equiv z^{p+2} \equiv z^3 \equiv x \pmod p$$

So, y is a cubic root of x. The two others are θy and $\theta^2 y$.

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

We select two prime numbers p and q such that $p \bmod 9 = 7$ and $q \bmod 3 = 2$, then form $n = pq$. We take $e = 3$, then $d_p = \frac{p+2}{9}$ and $d_q = 3^{-1} \bmod (q-1)$. To encrypt, we compute $y = x^3 \bmod n$. To decrypt, we compute $x_p = y^{d_p} \bmod p$, $x_q = y^{d_q} \bmod q$, and $x = \mathsf{CRT}_{p,q}(x_p, x_q)$.
If $\mathsf{gcd}(\frac{p-1}{2}, \frac{q-1}{2}) = 1$, since $d_p \bmod 2 = d_q \bmod 2$, we can find d such that $d \equiv d_p \bmod (p-1)$ and $d \equiv d_q \bmod (q-1)$. So, we could decrypt directly by $x = y^d \bmod n$.
In the above proposal, p and q play two different roles. Another option would be more symmetric, with $p \bmod 9 = q \bmod 9 = 7$ and $d_q = \frac{q+2}{9}$.
The proposed cryptosystem has similar properties as the Rabin cryptosystem. (This cryptosystem will be covered in a future lecture.)

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?

One a/b computation costs $T_{\mathsf{mul}} + T_{\mathsf{inv}}$.
For $P \neq Q$, computing λ costs $T_{\mathsf{mul}} + T_{\mathsf{inv}}$. Overall, it costs $3T_{\mathsf{mul}} + T_{\mathsf{inv}}$.
For $P = Q$, computing λ costs $2T_{\mathsf{mul}} + T_{\mathsf{inv}}$. Overall, it costs $4T_{\mathsf{mul}} + T_{\mathsf{inv}}$.

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 $E_{a,b}$?

Let (x,y,z) and (x',y',z') be elements of $E'_{a,b}$. If $z = 0$ and $z' = 0$, they both represent $\mathcal{O}$. If $z \neq 0$, $z' \neq 0$, $\frac{x}{z} = \frac{x'}{z'}$, and $\frac{y}{z} = \frac{y'}{z'}$, they represent the same point as well. In other cases, they don't.
An all-in-one condition could be that $xz' = x'z$ and $yz' = y'z$.

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

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

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 $\frac{y_R}{z_R}$.

We can see that $\lambda = \frac{u}{v}$ *from the definition. We compute*

$$\frac{x_R}{z_R} = \lambda^2 - 2\frac{x_P}{z_P} - \frac{v}{z_P z_Q}$$

and by substituting v *we obtain the expression of the first coordinate of* $f(P)+f(Q)$. *Next,*

$$\frac{y_R}{z_R} = 3\lambda\frac{x_P}{z_P} - \frac{y_P}{z_P} - \lambda^3 + \frac{u}{z_P z_Q}$$

and by substituting u *and one expression for* λ, *we obtain the expression of the second coordinate of* $f(P) + f(Q)$.

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.

We first compute u *and* v *in a straightforward way using* $4T_{\mathsf{mul}}$ *time. Then, we compute* u^2 *and* v^2, *then* uv^2, v^3, *and* uv^3. *So far, it takes* $9T_{\mathsf{mul}}$ *time. We can then compute* $z_P u^2$, $x_P v^2$, *then* $z_Q(z_P u^2 - 2x_P v^2)$, *and finally* x_R. *So far, this takes* $13T_{\mathsf{mul}}$ *time. We reuse* $x_P v^2$ *to compute* $x_P uv^2$, *then* $y_P v^3$ *and* $z_P u^3$, *and finally* y_R. *So far, this takes* $17T_{\mathsf{mul}}$ *time. We need two more multiplications for* z_R *and reach* $19T_{\mathsf{mul}}$ *time.*
There may exist some better strategy to compute $P + Q$.
Compared to $3T_{\mathsf{mul}} + T_{\mathsf{inv}}$, *this is competitive for* $T_{\mathsf{inv}}/T_{\mathsf{mul}} \geq 16$.

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.

Once we obtain a result P, *we can just multiply all coordinates by some random* $r \in \mathbf{Z}_p^*$. *We obtain a random element of* $E'_{a,b}$ *representing the same point. So, at an extra cost of* $3T_{\mathsf{mul}}$, *we can hide a possible leak.*