Advanced Cryptology Final exam - (3 h)

Documents allowed. No computer.

Exercise 1. Consider the elliptic curve $E : y^2 = x^3 + x$ over $\mathbb{F}_p$, where p is the prime

$$p = 3^{101} + 15880.$$

Let ζ be a primitive 4-th root of unity in $\overline{\mathbb{F}}_p$ and ψ be the automorphism of E defined by

$$\psi : (x, y) \mapsto (-x, \zeta y).$$

1. Write down a point of order 2 in $E(\mathbb{F}_p)$.
2. Check that ψ is indeed an automorphism of E. What is its characteristic polynomial?
3. Let $\Phi_p : (x, y) \mapsto (x^p, y^p)$ be the Frobenius endomorphism of E. Show that $\Phi_p \circ \psi \neq \psi \circ \Phi_p$, and hence show that $\#E(\mathbb{F}_p) = p + 1$.
4. Knowing that the prime factorization of this cardinality is $\#E(\mathbb{F}_p) = 4 \cdot 11 \cdot r$ where

   $$r = 35139376413546227116122349756746904956961876861,$$

   compute the embedding degree k with respect to r and p.
5. Is the elliptic curve E pairing-friendly?

Exercise 2. Let E be the elliptic curve defined over $\mathbb{F}_2$ of equation $y^2 + xy = x^3 + x^2 + 1$. We denote by $\Phi_2 : E(\overline{\mathbb{F}}_2) \to E(\overline{\mathbb{F}}_2)$, $(x, y) \mapsto (x^2, y^2)$ its Frobenius endomorphism.

1. Show that the characteristic polynomial of Φ_2 is $X^2 - X + 2$.
2. Compute the cardinality of $E(\mathbb{F}_4)$, $E(\mathbb{F}_8)$, $E(\mathbb{F}_{16})$ and $E(\mathbb{F}_{32})$.
3. Use Hasse's bound to prove that $\#E(\mathbb{F}_{2^m}) < \#E(\mathbb{F}_{2^{m+1}})$ for any $m \geqslant 5$. Combine with the result of the previous question to show that this inequality is true for any $m \geqslant 1$.
4. Explain why $\#E(\mathbb{F}_{2^m})$ cannot be prime for any $m \geqslant 2$. Show that if $\#E(\mathbb{F}_{2^m})$ is twice a prime integer then m is a prime.
5. Let τ be a complex root of $X^2 - X + 2$. Give the fundamental discriminant of the imaginary quadratic field $K = \mathbb{Q}(\tau)$ and its ring of integers $\mathcal{O}_K$.
6. Show that the endomorphism ring of E is isomorphic to the ring $\mathbb{Z}[\tau] = \{a + b\tau : a, b \in \mathbb{Z}\}$.

We will admit that any integer $n \in \mathbb{Z}$ has a τ-adic expansion of the form $n = \sum_{i=0}^{d} c_i \tau^i$, with $c_i \in \{0, 1\}$ and d approximately equal to $\log_2(n)$.

4. Use this result to show that the multiplication by n map can be computed as

$$[n]P = \sum_{i\,:\,c_i=1} (\Phi_2)^i(P) \quad \forall P \in E.$$

Explain why this is faster than the standard double-and-add algorithm.

Exercise 3. In order to speed up point multiplication, it is convenient to work with elliptic curves having an easily computable endomorphism (other than a multiplication by m map), as in the previous exercises. This exercise investigates a construction of Galbraith, Lin and Scott.
Let $E' : y^2 = x^3 + ax + b$ be an elliptic curve defined over a prime field $\mathbb{F}_p$ ($p \geqslant 5$) with j-invariant different from 0 and 1728.

1. Let m be a positive integer and u a non-square in $\mathbb{F}_{p^m}$. Show that the elliptic curve defined over $\mathbb{F}_{p^m}$ of equation $y^2 = x^3 + au^2x + bu^3$ (the *quadratic twist* of E' over $\mathbb{F}_{p^m}$) is isomorphic to E' over $\mathbb{F}_{p^{2m}}$ but not over $\mathbb{F}_{p^m}$. Show that any curve defined over $\mathbb{F}_{p^m}$ whose j-invariant equals $j(E')$ is isomorphic over $\mathbb{F}_{p^m}$ to either E' or its twist.

Let E be the quadratic twist of E' over $\mathbb{F}_{p^2}$. We suppose that there exists a (large) prime integer r such that r divides $\#E(\mathbb{F}_{p^2})$ but r^2 does not divide $\#E(\mathbb{F}_{p^4})$. Let ψ be the $\mathbb{F}_{p^4}$-isomorphism from E to E' and $\Phi_p : (x, y) \mapsto (x^p, y^p)$ the Frobenius endomorphism of E'. Finally, let $\varphi = \psi^{-1} \circ \Phi_p \circ \psi$.

2. Show that φ belongs to $End_{\mathbb{F}_{p^4}}(E)$.

3. Show that $\varphi^4(P) = P$ for any $P \in E(\mathbb{F}_{p^4})$, and that $\varphi^2 - t'\varphi + p = 0$ where t' is equal to $p + 1 - \#E'(\mathbb{F}_p)$.

4. Show that $\varphi^2(P) = -P$ for any $P \in E(\mathbb{F}_{p^2})$ (hint: write down equations for ψ and φ).

5. Show that there exists an integer λ such that $\varphi(P) = [\lambda]P$ for all $P \in E(\mathbb{F}_{p^2})[r]$, and that $\lambda^2 = -1 \bmod r$.

Let n be an integer in $[1, r-1]$. We will admit that there exist two (easily computable) integers a and b of size approximately half the size of r such that $n = a + b\lambda \bmod r$.

6. Explain heuristically why this assumption is reasonable.

7. If P is in $E(\mathbb{F}_{p^2})[r]$, show that $[n]P = [a]P + [b]\varphi(P)$. Compare the computation of $[n]P$ using this formula with two double-and-add algorithms and using the standard method (with only one double-and-add algorithm).

To speed up the computation of $[a]P + [b]\varphi(P)$, we can use the following Shamir's trick:

```
Input  : P, φ(P), a, b
Express the binary representations (a_{ℓ-1} ... a_0) of a and (b_{ℓ-1} ... b_0) of b, padding the shorter
one with 0 on the left if need be
R ← P + φ(P)
T ← O
for i = ℓ - 1 down to 0 do
    T ← [2]T
    if a_i = 1 and b_i = 0 then
        T ← T + P
    if a_i = 0 and b_i = 1 then
        T ← T + φ(P)
    if a_i = 1 and b_i = 1 then
        T ← T + R
return T
```

8. Apply this algorithm step by step for $a = 13$ and $b = 23$.
9. What is the number of additions and/or doublings in this direct computation of $[n]P = [a]P + [b]\varphi(P)$? What is the speed-up as compared to the above methods?
10. Is it possible to modify Shamir's trick into a right-to-left algorithm?

Exercise 4.

A Gröbner basis with respect to a monomial order is usually not a Gröbner basis for another monomial order. The goal of this exercise is to show that for a given ideal I of $k[X_1, \ldots, X_n]$, there are in fact only finitely many possible reduced Gröbner bases.

1. Let $\prec_1$ and $\prec_2$ be two monomial orders. Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis for I with respect to $\prec_1$, and assume that $\mathrm{LM}_{\prec_1}(g_i) = \mathrm{LM}_{\prec_2}(g_i)$ for $i = 1, \ldots, t$. Prove that G is then also a Gröbner basis for I with respect to $\prec_2$ (hint: show that $\overline{f}^{G,\prec_2} = 0$ for any $f \in I$).
2. Let $\prec_1$ and $\prec_2$ be two monomial orders such that $\mathrm{LM}_{\prec_1}(I) = \mathrm{LM}_{\prec_2}(I)$. Show that the reduced Gröbner bases of I with respect to $\prec_1$ and $\prec_2$ are equal.

Let $\mathcal{T}$ be the (infinite) set of all possible monomial orders on $k[X_1, \ldots, X_n]$ and let $\mathcal{L}$ be the set of the initial ideals of I with respect to the orders in $\mathcal{T}$. The goal of the next questions is to show by contradiction that $\mathcal{L}$ (and hence the set of possible reduced Gröbner bases) is finite.

3. For each initial ideal in $\mathcal{L}$, we choose one monomial order $\prec$ in $\mathcal{T}$ which gives this initial ideal. Let $\mathcal{T}' \subset \mathcal{T}$ be the set of these chosen monomial orders. By contradiction, we suppose that this set $\mathcal{T}'$ is infinite.
   (a) Let $\{f_1, \ldots, f_r\}$ be a generating set of I. Prove that there exist only finitely many possibilities for the set $\{\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_r)\}$. Use the pigeonhole principle to show that there

exists monomials $m_1, \dots, m_r$ and an infinite set $\mathcal{T}_0 \subset \mathcal{T}'$ such that $\{\mathrm{LM}(f_1), \dots, \mathrm{LM}(f_r)\} = \{m_1, \dots, m_r\}$ for all monomial orders in $\mathcal{T}_0$.

(b) Assume that $\{f_1, \dots, f_r\}$ is not a Gröbner basis for any order in $\mathcal{T}_0$. Prove that there exists $f_{r+1} \in I$ such that $m_i \nmid \mathrm{LM}_{\prec}(f_{r+1})$ for $i = 1, \dots, r$ and for any monomial order $\prec$ in $\mathcal{T}_0$. Show that there exists a monomial m_{r+1} and an infinite set $\mathcal{T}_1 \subset \mathcal{T}_0$ such that $\{\mathrm{LM}(f_1), \dots, \mathrm{LM}(f_{r+1})\} = \{m_1, \dots, m_{r+1}\}$ for all orders in $\mathcal{T}_1$.

(c) We can repeat this process, adding new polynomials $f_{r+1}, \dots, f_{r+k}$ and monomials $m_{r+1}, \dots, m_{r+k}$ and constructing a decreasing sequence of infinite sets $\mathcal{T}_k \subset \cdots \subset \mathcal{T}_0$ such that $\{\mathrm{LM}(f_1), \dots, \mathrm{LM}(f_{r+k})\} = \{m_1, \dots, m_{r+k}\}$ for all orders in $\mathcal{T}_k$, as long as $\{f_1, \dots, f_{r+k}\}$ is not a Gröbner basis for any order in $\mathcal{T}_k$. Show that this process stops at some point.

(d) The previous question shows that there exists an integer k_0 and an order $\prec$ in $\mathcal{T}_{k_0}$ for which $\{f_1, \dots, f_{r+k_0}\}$ is a Gröbner basis of I. Use question 1 to prove that $\{f_1, \dots, f_{r+k_0}\}$ is then a Gröbner basis for any order in $\mathcal{T}_{k_0}$. Show that this implies that $\mathrm{LM}_{\prec_1}(I) = \mathrm{LM}_{\prec_2}(I)$ for any orders $\prec_1$ and $\prec_2$ in $\mathcal{T}_{k_0}$ and deduce a contradiction with the construction of $\mathcal{T}'$. Conclude.

4. Show that the union of all the possible reduced Gröbner bases of I is a *universal Gröbner basis*, i.e. a (non-minimal) Gröbner basis of I for any monomial order.

5. Find a universal Gröbner basis for the ideal of $\mathbb{Q}[x, y]$ generated by $x - y^2$ and $xy - x$ (hint: consider all possible leading terms at each stage of Buchberger's algorithm).