Master CSI, AGTN/ALGANT 2018-2019

Courbes elliptiques — 4TMA902U

Responsables : G. Castagnos, D. Robert

Terminal Exam — December 14, 2018

3h

Documents are not allowed

Answer the two parts on separate sheets

G. Castagnos' Part

I Let q be a large prime number and let $(G, \times)$ be a cyclic group of order q. We denote by g a generator of G. We define a variant of the Elgamal encryption scheme. The secret key is a random integer x with $1 < x < q$. The public key is $h = g^x$. To encrypt $m \in G$ with the public key h, one takes a random integer r with $1 < r < q$. The ciphertext for m is $c := (c_1, c_2) := (mg^r, h^r) \in G \times G$.

(a) What role does encryption play in data security? What problem an opponent must resolve in order to compute the private key from the public key in this variant of the Elgamal scheme? Give a decryption algorithm for this variant of the Elgamal scheme.

Alice and Bob both use this encryption scheme. We denote h_A (resp. h_B) Alice's public key (resp. Bob's public key) and x_A her private key (resp. x_B his private key). We suppose that Carl knows the number $x_B x_A^{-1} \mod q$.

(b) Let c_A a ciphertext of m using Alice's public key. Show that Carl can transform c_A in a ciphertext c_B which Bob can decrypt in order to recover m. Show that Carl can also transform a ciphertext c'_B of m' using Bob's public key in a ciphertext c'_A of m' that Alice can decrypt.

(c) What can Carl and Alice do if they share their knowledge?

In the remainder of the exercise we consider ℓ a large prime number and $(G, +)$ and $(G_t, \times)$ two cyclic groups of order ℓ. We denote P a generator of G. Let $e : G \times G \to G_t$ a cryptographic pairing of type I, *i.e*, a non degenerate efficiently computable bilinear map.

(d) Recall what is a non degenerate bilinear map. Why e is said to be of type I? Is there other types of pairing? Which one is the most suitable for cryptographic applications? Why?

Until the end of the exercise, we consider the following encryption scheme. The private key is a random integer $1 < x < \ell$. The public key is the point $Q = xP$. To encrypt $m \in G_t$ with the public key Q, we take at random an integer r with $1 < r < \ell$. The ciphertext for m is $c := (c_1, c_2) := (m \times e(P, P)^r, rQ) \in G_t \times G$.

(e) Give the description of a decryption algorithm.

Alice and Bob both use this encryption scheme. We denote Q_A (resp. Q_B) Alice's public key (resp. Bob's public key) and x_A her private key (resp. x_B his private key). We suppose now that Carl knows the point $(x_B x_A^{-1} \ mod\ \ell)P$.

(f) Let c_A a ciphertext of m using Alice's public key. Show that Carl can transform c_A in a c_B from which Bob can recover m with his private key (precise how).

(g) Can Carl now transform ciphertexts c'_B of m' using Bob's public key in a c'_A from which Alice can recover m' with her private key? Moreover is it possible for Carl by sharing his knowledge with Alice to deduce information on the secret key of Bob?

2 Let p be a prime number with $p > 3$ and $p \equiv 3 \ (mod\ 4)$. We denote by E the elliptic curve of equation $y^2 = x^3 + x$ over $\mathbf{F}_p$.

(a) Let $x \in \mathbf{F}_p$ and denote $f(x) = x^3 + x$. Show that $f(x)$ is a square if and only if $f(-x)$ is not a square.

(b) Show that $E(\mathbf{F}_p)$ has $p + 1$ points (Hint: one can use the fact that $\mathbf{F}_p$ can be written as $\mathbf{F}_p = \{0, \pm 1, \pm 2, \ldots, \pm(p-1)/2\}$).

(c) Show that there exists $i \in \mathbf{F}_{p^2}$ such that $i^2 = -1$.

In the following, we denote by ϕ the map that sends a point $Q = (x, y)$ of $E(\mathbf{F}_p)$ to $\phi(Q) = (-x, iy)$ and that sends O_E to itself.

(d) Prove that $\phi(Q) \in E(\mathbf{F}_{p^2})$ for all $Q \in E(\mathbf{F}_p)$.

We assume in the following that ϕ is a morphism for the group law of the points of the curve. Moreover, we will assume that there exists a prime factor ℓ of $p+1$ with $\ell > 2$. We will denote $G = \langle P \rangle$ where P is a point of $E(\mathbf{F}_p)$ of order ℓ.

(e) Give an algorithm (in pseudo code or Sage) that takes an integer λ as input, and that outputs (with the previous notations) ℓ of λ bits, the prime p, and the point P.

(f) What is the embedding degree of ℓ in $\mathbf{F}_p$?

(g) Let us denote $P = (x_P, y_P)$ the affine coordinates of P. Show that $y_P \neq 0$. Deduce that P and $\phi(P)$ generate the ℓ–torsion of the curve E.

(h) Show how to define a cryptographic pairing of type I with this curve.

(i) Show how to use this pairing to do a tripartite key exchange in one round between Alice, Bob and Carl.

(j) Suppose that Alice and Bob do a Diffie-Hellman key exchange in the group $G = \langle P \rangle$. Suppose we know the values X and Y exchanged by Alice and Bob. Given and element $Z \in G$ show how to efficiently tell if Z is the secret common quantity established by Alice and Bob.

D. Robert's Part

3 Let E be an elliptic curve over $\mathbf{F}_q$ and $P_0 = (x_0, y_0) \in E(\mathbf{F}_q)$. Let $\oplus$ be the composition of $+$ (the standard group law on E) with the translation by $-P_0$: $P \oplus Q = P + Q - P_0$.

(a) Show that $\oplus$ define an abelian group law on E. What is its neutral point?

(b) Let $\phi_{P_0} : P \mapsto P - P_0$. Show that ϕ_{P_0} is an isomorphism between $(E(\overline{\mathbf{F}}_q), +)$ and $(E(\overline{\mathbf{F}}_q), \oplus)$ (ie $\phi_{P_0}(P + Q) = \phi_{P_0}(P) \oplus \phi_{P_0}(Q)$) if and only if P_0 is a Weierstrass point.

(c) Show the following interpretation in terms of divisors: let $\psi_{P_0} : P \mapsto (P) - (P_0)$ which maps a point on E to a degree 0 divisor. Then $\psi_{P_0}(P) + \psi_{P_0}(Q)$ is linearly equivalent to $\psi_{P_0}(P \oplus Q)$.

(d) Give a geometric interpretation of $\oplus$, where $P \oplus Q$ is computed using only two lines (Hint: either use the geometric interpretation of $P + Q$ or use the preceding question).

(e) Give an algorithm to compute $\oplus$ from the coordinates of P and Q.

4 Let $E/\mathbf{F}_q$ be an elliptic curve defined over $\mathbf{F}_q$, with $q = p^a$.

(a) Recall the definition of the Weil pairing $e_{W,\ell}$ on the ℓ-torsion of E for $\ell \neq p$ prime.

(b) We admit that the same definition works for n non prime (but prime to p) to give a bilinear application $e_{W,n} : E[n](\overline{\mathbf{F}}_q) \times E[n](\overline{\mathbf{F}}_q) \to \mu_n \subset \overline{\mathbf{F}}_q^*$.
What is the smallest extension of $\mathbf{F}_q$ that contains μ_n?

(c) Prove that if $m \mid n$ and $P, Q \in E[m](\overline{\mathbf{F}}_q)$, $e_{W,m}(P, Q) = e_{W,n}(P, Q)^{n/m}$.

(d) More generally, we admit that if $Q \in E[m](\overline{\mathbf{F}}_q)$, then for every $P \in E[n](\overline{\mathbf{F}}_q)$, $e_{W,n}(P, Q) = e_{W,m}(\frac{n}{m}P, Q)$. Deduce that $e_{W,n}$ is non degenerate, that is $e_{W,n}$ is a pairing.

(e) Show that if $P, Q \in E[n](\overline{\mathbf{F}}_q)$, they generate a basis of the n-torsion if and only if $e_{W,n}(P, Q)$ is a primitive n-root of unity.

(f) Assuming that we know the factorisation of n, deduce an algorithm to check if $P, Q \in E[n]$ generate the n-torsion in time $O(\log n^2)$ operations in the field where P and Q are defined.

(g) Recall that as an abelian group, $E(\mathbf{F}_q) \simeq \mathbf{Z}/a\mathbf{Z} \oplus \mathbf{Z}/b\mathbf{Z}$ where $a \mid b$. Show that $a \mid q - 1$.

5 Let $E/\mathbf{F}_q$ be an elliptic curve defined over $\mathbf{F}_q$, with $q = p^a$, and $\pi_q : E \to E, (x, y) \mapsto (x^q, y^q)$ be the Frobenius endomorphism. We recall that the characteristic polynomial of the Frobenius is of the form $\chi_\pi(X) = X^2 - tX + q$. This exercice is split into two independent parts.

Part 1:

(a) Recall how to compute $\#E(\mathbf{F}_q)$ in terms of χ_π.

(b) Explain how to use the resultant to get χ_{π^n} from χ_π.

(c) Let $X^n \equiv a_n X + b_n \mod \chi_\pi(X)$. Show that $\#E(\mathbf{F}_{q^n}) = q^n + 1 - (a_n t + 2b_n)$.

(d) Show that $\#E(\mathbf{F}_{q^2}) = q^2 + 1 - (t^2 - 2q)$ and $\#E(\mathbf{F}_{q^3}) = q^3 + 1 - (t^3 - 3qt)$.

(e) Deduce that from $\#E(\mathbf{F}_q)$, one can recover $\#E(\mathbf{F}_{q^n})$ in time $O(\log n \log q^n)$.

Part 2:

(a) Let $\ell \neq p$ be a prime number. Then $E[\ell](\overline{\mathbf{F}}_q)$ is a $\mathbf{Z}/\ell\mathbf{Z}$-vector space of dimension 2. Show that the Frobenius π acts on $E[\ell](\overline{\mathbf{F}}_q)$, and the smallest extension $\mathbf{F}_{q^n}$ of $\mathbf{F}_q$ such that all points of ℓ-torsion are defined in $\mathbf{F}_{q^n}$ is also the order of π as an endomorphism of $E[\ell](\overline{\mathbf{F}}_q)$.

(b) We admit that the characteristic polynomial of the Frobenius endomorphism acting on $E[\ell](\overline{\mathbf{F}}_q)$ is $\chi_\pi \mod \ell$. Show that there exists a basis of $E[\ell](\overline{\mathbf{F}}_q)$ such that the matrix of the Frobenius on this basis is either of the form $\begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}$ with λ, μ in $\mathbf{F}_\ell$ or $\mathbf{F}_{\ell^2}$, or of the form $\begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$ with $\lambda \in \mathbf{F}_\ell$.

(c) Let n be as above the degree over $\mathbf{F}_q$ of the smallest extension which contains all points of n-torsion. Let d be the embedding degree (relative to ℓ), and k be the order of λ. Show that in the first case, $n = d \vee k$ (the ppcm of d and k), and that in particular, $n \mid \ell - 1$ or $n \mid \ell^2 - 1$ according to whether $\lambda \in \mathbf{F}_\ell$ or $\lambda \in \mathbf{F}_{\ell^2}$. Show that in the second case, $n = \ell k$, so that $n \mid \ell(\ell - 1)$.

(d) Assume that $E(\mathbf{F}_q)$ already contains a point of ℓ-torsion. Show that if the embedding degree d is strictly greater than 1 ($d > 1$), then $n = d$, while if d equals to 1 ($d = 1$), then either $n = 1$ or $n = \ell$.

(e) Assume that $E(\mathbf{F}_q)$ already contains all the points of ℓ-torsion, but not all the points of ℓ^2-torsion. Then show that $E(\mathbf{F}_{q^\ell})$ is the smallest extension which contains all the points of ℓ^2-torsion.

(f) Show that if $\ell \mid q - 1$ but $\ell^2 \nmid q - 1$, then the smallest n such that $\ell^2 \mid q^n - 1$ is $n = \ell$. What is the link with the preceding question?