Cryptographic Trends

Exercise 1 - Elliptic Curves

An elliptic curve E defined on a field $\mathbb{K}$ is a curve given by the following equation, named *Weierstrass equation*:

$$y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$$

In most of the case, this equation can be rewritten:

$$y^2 = x^3 + ax + b$$

With an additional point at infinity $\mathcal{O}$, $(E, +)$ defines a group structure, with $\mathcal{O}$ as neutral element.

We consider the elliptic curve E with equation $y^2 = x^3 + 3x + 1$ on $\mathbb{F}_7$.

1) Complete the following table and list all points of E.

	0	1	2	3	4	5	6
$x^3 + 3x + 1 \mod 7$							
$y^2 \mod 7$							

2) Compute the affine equation of the line passing through the points $A = (0, 1)$ and $B = (3, 4)$.

3) Find the third point (α, β) of E which is on this line. The value of $(0, 1) + (3, 4)$ is defined as $(\alpha, -\beta)$

The global formula to compute the sum $R = (x_R, y_R)$ of two points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ is given below:

$$\begin{cases} x_R = m^2 - x_P - x_Q \\ y_R = m(x_P - x_R) - y_P \end{cases} \quad \text{where } m = \begin{cases} \dfrac{y_P - y_Q}{x_P - x_Q} & \text{if } x_P \neq x_Q \text{ (case 1)} \\ \dfrac{3x_P^2 + a}{2y_P} & \text{if } P = Q \text{ (case 2)} \end{cases}$$

If $P = -Q$ ($x_P = x_Q$ and $y_P = -y_Q$), $P + Q = \mathcal{O}$ (case 3 et 4)

4) Compute $x^{-1} \mod 7$ for $x \in \{1, 2, 3, 4, 5, 6\}$.

5) Computation of $2(0, 1) = (0, 1) + (0, 1)$:

- $P = Q$ so we are in case 2:

$$m = (3x_p^2 + 3)/(2y_p) = 3/2 = 3 \times 2^{-1} = 3 \times 4 = 12 \equiv 5 \mod 7$$

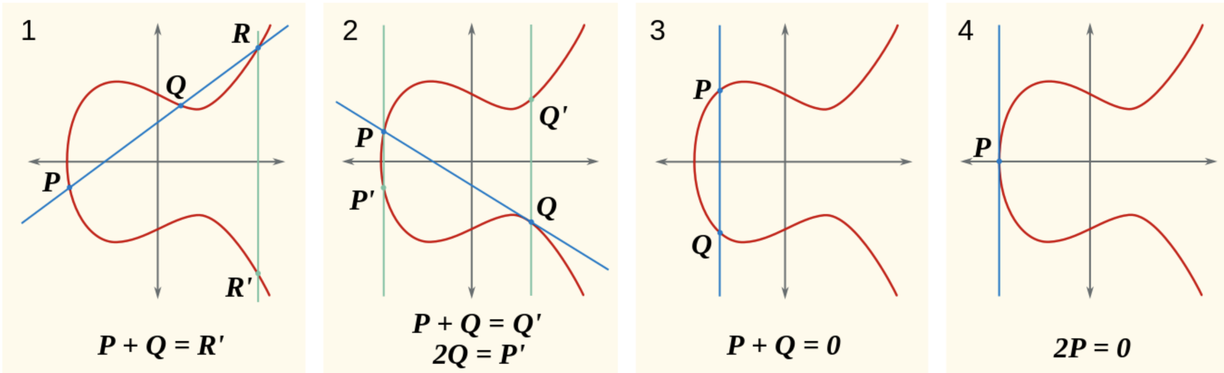

Figure 1: Visual representation of addition on elliptic curves

- $x_R = m^2 - x_P - x_Q = 5^2 - 0 - 0 = 25 \equiv 4 \mod 7$
- $y_R = m(x_P - x_R) - y_P = 5(0-4) - 1 = -21 \equiv 0 \mod 7$
- $2(0,1) = (4,0)$

a. Compute $3(0,1) = 2(0,1) + (0,1)$ and $4(0,1) = 3(0,1) + (0,1)$

b. What is the order of the point $(0,1)$?

5) Same questions with the point (6,2)

5) What is the order of E ?

Exercise 2 - Shamir Secret Sharing

Generate a secret nuclear code: 2253. Then, suppose that three people are needed to launch the nuclear bomb. Next, we generate two (3-1) random numbers : 245 and 985. By consequent, the polynomial generating the secret sharing keys is: $P(x) = 2253 + 245x + 985x^2$.

1) Compute the points $(i, f(i))$ for $i \in \{1, \dots, 6\}$. Each couple is a secret key

2) Randomly choose 3 keys $D_j = (x_j, f(x_j))$, and compute for each of them:

$$\ell_j(x) = \prod_{\substack{k=1 \\ k \neq j}}^{3} \frac{x - x_k}{x_j - x_k}$$

3) Check that $\sum_{j=1}^{3} f(x_j) \cdot l_j(0) = 2253$

Exercise 3 - Homomorphic Encryption

Consider Paillier encryption scheme, who is defined as follows:

- **Key Generation** : Choose two larges prime numbers p and q of equal length. Set $N = pq$ as the public key and $\varphi(N)$ as the secret key.
- **Encryption** To encrypt a message m, generate a random value $0 < r < N$ and compute $\mathsf{enc}(\mathsf{pk}, m) = c = (1+N)^m \cdot r^N \mod N^2$ as the ciphertext
- **Decryption** To decrypt a ciphertext c, retrieve r by computing $r = c^{N^{-1} \bmod \varphi(N)} \mod N$. Then, compute

$$\mathsf{dec}(\mathsf{sk}, c) = m = \frac{(c \cdot r^{-N} \mod N^2) - 1}{N}$$

1) Let m_1, m_2 be two messages in $\mathbb{Z}_p$. Compute $\mathsf{enc}(\mathsf{pk}, m_1) \times \mathsf{enc}(\mathsf{pk}, m_2)$

2) Write a relation between $\mathsf{enc}(\mathsf{pk}, m_1)$, $\mathsf{enc}(\mathsf{pk}, m_2)$ and $\mathsf{enc}(\mathsf{pk}, m_1 + m_2)$

3) Write $\mathsf{enc}(\mathsf{pk}, m_1 \cdot m_2)$ depending on $\mathsf{enc}(\mathsf{pk}, m_1)$

4) Is Paillier multiplicatively homomorphic ? Why ?

Exercise 4 - Pairings

Let G_1, G_2 and G_T three cyclic additive groups with order q. A *pairing* e is a function mapping a couple in $G_1 \times G_2$ to an element of G_T with the following properties:
- bilinearity : $\forall a, b \in \mathbb{F}_q^*,\ \forall P \in G_1, Q \in G_2 :\ e(aP, bQ) = e(P, Q)^{ab}$
- Non-degenerency : $\forall (P, G) \neq (1, 1), e(P, G) \neq 1$

2) Write $e(aP, bP)^c$ in fucntion of $e(P, P)$

3) Deduce a tripartite key exchange protocol relying on pairings.