# Elliptic-Curve Diffie-Hellman

BEHAGUE Quentin, LECORNU Adrien
Sous la direction de CASTANHEIRA Stéphane

# Introduction

## Qu'est-ce que la cryptographie

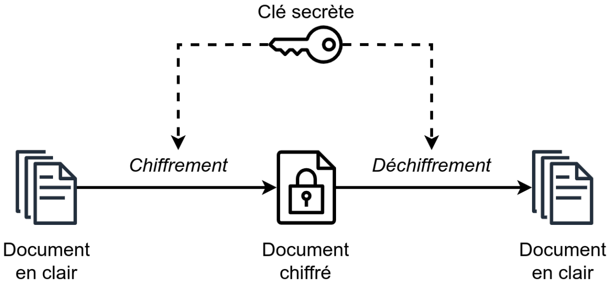



Figure – Chiffrement asymétrique

# Diffie-Hellman

## Principe du protocole

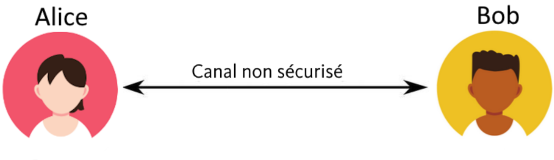



Figure – Protocole Diffie-Hellman ($\mathbb{Z}/p\mathbb{Z}$)

# Diffie-Hellman

## Principe du protocole

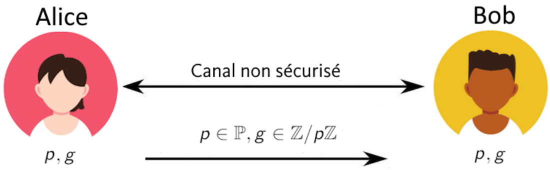



Figure – Protocole Diffie-Hellman ($\mathbb{Z}/p\mathbb{Z}$)

# Diffie-Hellman

## Principe du protocole

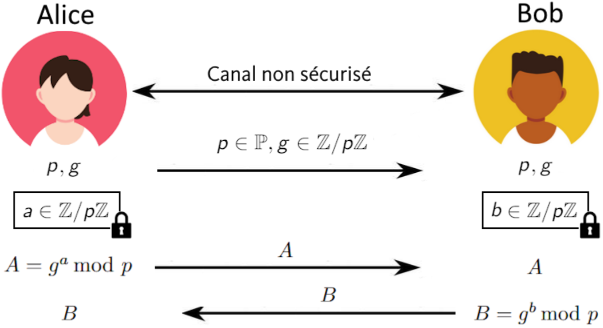



Figure – Protocole Diffie-Hellman ($\mathbb{Z}/p\mathbb{Z}$)

# Diffie-Hellman

## Principe du protocole

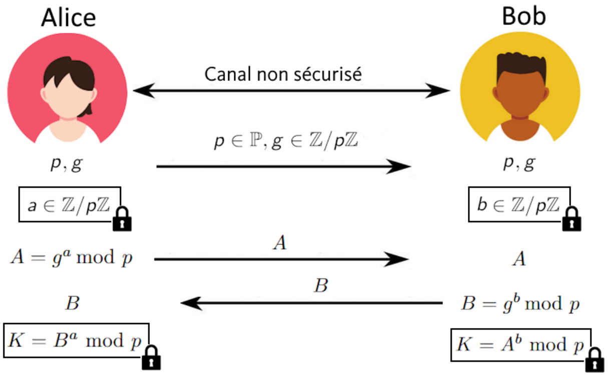



Figure – Protocole Diffie-Hellman ($\mathbb{Z}/p\mathbb{Z}$)

# Diffie-Hellman

## Problème Diffie-Hellman et logarithme discret

Données échangées

$$\boxed{\begin{array}{c} g \in (\mathbb{Z}/p\mathbb{Z}, \cdot) \\ \\ A \ (= g^a \mod p) \\ \\ B \ (= g^b \mod p) \end{array}} \xrightarrow{\quad ? \quad} K = g^{ab} \mod p$$

Figure – Problème Diffie-Hellman

# Diffie-Hellman

## Attaque brute force

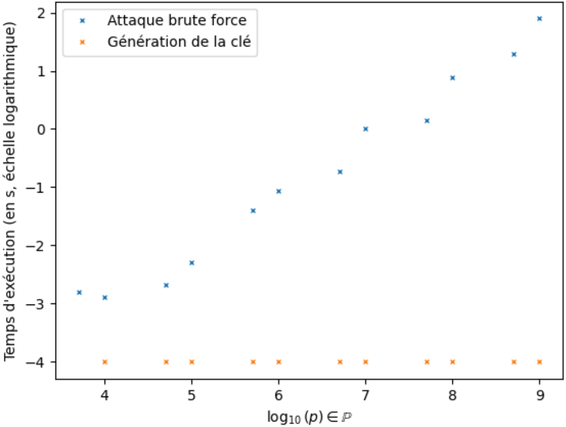



Figure – Temps d'exécution moyen de l'algorithme 4 (sur 1000 échantillons $(a, b, g)$ aléatoires)

**Définition :** (Courbe plane affine)

Soit $P \in K[X_1, \cdots, X_n]$, on appelle courbe plane affine sur $K$ associée à $P$ et on note $C_P$ l'ensemble :

$$C_P := \{(x_1, \cdots, x_n) \in K^n \mid P(x_1, \cdots, x_n) = 0\} = P^{-1}(\{0\})$$

**Définition :** (Point singulier)

$P \in K[X_1, \cdots, X_n]$, on dit que $(x_1, \cdots, x_n) \in K^n$ est singulier si :

$$\frac{\partial P}{\partial X_1}(x_1, \cdots, x_n) = \cdots = \frac{\partial P}{\partial X_n}(x_1, \cdots, x_n) = 0$$

Si un point est non singulier, il est lisse.

**Définition :** (Espace projectif)

On note $\mathbb{P}^n$ l'ensemble :

$$\mathbb{P}^n = \left(K^{n+1}\right)^* / \sim .$$

Où $\sim$ est définie par :

$$(x_0, \cdots, x_n) \sim (y_0, \cdots, y_n) \iff \exists\, \lambda \in K^*, \forall\, i \in [\![0, n]\!], x_i = \lambda y_i .$$

**Définition :** (Droite projective dans $\mathbb{P}^2$)

Une droite de $\mathbb{P}^2$ d'équation $ux + vy + wz = 0$ avec $u, v, w \in K$ non tous nuls est l'ensemble :

$$\left\{[x : y : z] \in \mathbb{P}^2 \;\middle|\; ux + vy + wz = 0\right\}.$$

Il existe une unique droite projective passant par 2 points distincts.

**Définition :** (Tangente à un point lisse d'une courbe dans $\mathbb{P}^2$)

Soit E une courbe plane affine de polynôme $F \in K[X, Y, Z]$ et $P$ un point lisse de la courbe, la tangente à E en $P \in E$ est la droite d'équation :

$$\frac{\partial F}{\partial X}(P)x + \frac{\partial F}{\partial Y}(P)y + \frac{\partial F}{\partial Z}(P)z = 0.$$

**Définition :** (Equation de Weierstrass)

On appelle équation de Weierstrass une équation de la forme :

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \quad (1)$$

On note

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3)$$

le polynôme associé.

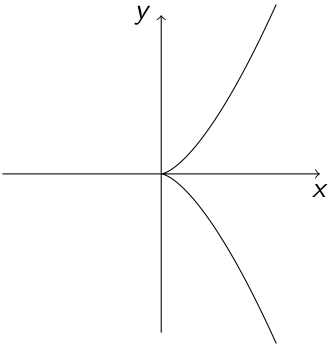
Une courbe de Weierstrass a un seul point à l'infini. C'est le point $[0:1:0]$. Il est lisse (non singulier) et la tangente à la courbe en ce point a pour équation $z = 0$.

Pour un corps $K$ de caractéristique différente de 2 ou 3, on peut se ramener à une équation de la forme :

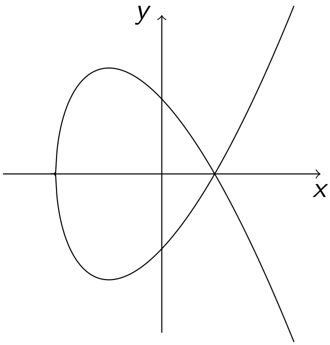
$$y^2 = x^3 + ax + b \tag{2}$$

pour les points finis de $\mathbb{P}^2$ : (les $[x, y, 1] \in \mathbb{P}^2$)

$$\mathcal{C}_F \text{ est lisse } \iff \Delta \neq 0$$




Point de rebroussement
$(y^2 = x^3)$




Noeud
$(y^2 = x^3 - 3x + 2)$

Figure – Courbes possédant des points singuliers

**Définition :** (Courbes Elliptiques)

Une courbe elliptique sur $K$ est un couple $(E, \mathcal{O})$ où :

- $E$ est une courbe plane affine lisse associée à un polynôme de $K[X, Y, Z]$.
- $\mathcal{O}$ désigne l'origine.

**Théorème :**
Une droite coupe une courbe elliptique en au plus 3 points.

# Courbes Elliptiques

## Loi de groupe : représentation géométrique

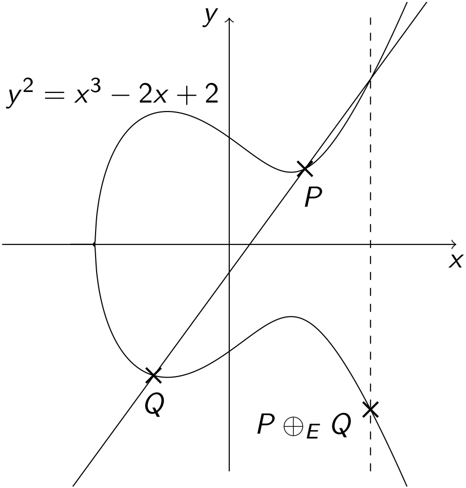



Figure – Représentation géométrique de la somme de $P = (1, 1)$ et $Q = (-1, -1.732) \in E$

Soit $P = (x_P, y_P), Q = (x_Q, y_Q) \in (E, \mathcal{O})$, en notant :

$$\begin{cases} s = \frac{y_P - y_Q}{x_P - x_Q} & \text{si } x_P \neq x_Q \text{ et } y_P \neq y_Q \\ s = \frac{3x_P^2 + a}{2y_P} & \text{si } x_P = x_Q \neq 0 \text{ et } y_P = y_Q \end{cases}$$

Les coordonnées de $R = P \oplus Q$ sont données par :

$$\begin{cases} x_R = s^2 - (x_P + x_Q) \\ y_R = s(x_P - x_R) - y_P \end{cases}$$

Enfin, si $y_P \neq y_Q$ et $x_P \neq x_Q$, on a $R = \mathcal{O}$

**Définition :** ($E(\mathbb{Z}/p\mathbb{Z})$)

Soit $(E, \mathcal{O})$ une courbe elliptique d'équation $y^2 = x^3 + ax + b$.
On définit l'ensemble $E(\mathbb{Z}/p\mathbb{Z})$ par :

$$E(\mathbb{Z}/p\mathbb{Z}) := \left\{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \;\middle|\; y^2 \equiv x^3 + ax + b \mod p\right\} \cup \{\mathcal{O}\}$$

# Courbes Elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

## Ensemble $E(\mathbb{Z}/p\mathbb{Z})$

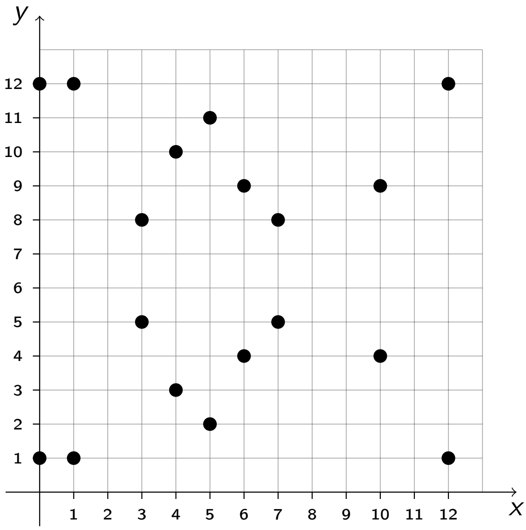



Figure – Courbe elliptique $y^2 = x^3 - x + 1$ dans $\mathbb{Z}/13\mathbb{Z}$

# Courbes Elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

## Loi de groupe : Représentation géométrique

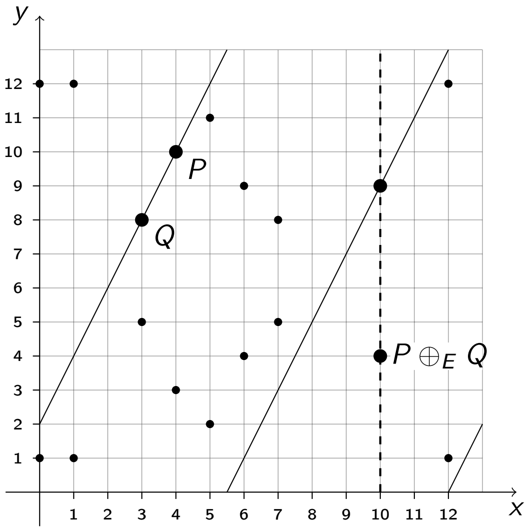



Figure – Représentation géométrique de la somme $(4, 10) \oplus_E (3, 8)$

**Définition :** (Inverse modulaire) Soit $p, q, n \in \mathbb{Z}^2 \times \mathbb{N}^*$. On dit que $q$ est l'inverse modulaire de $p$ modulo $n$, noté $p^{-1}$ si :

$$pq \equiv 1 \mod n$$

**Remarque :** On l'obtient à l'aide de l'algorithme d'Euclide étendu (Annexe 1) pour les entrées $a = p$ et $b = n$.

Soit $P = (x_P, y_P), Q = (x_Q, y_Q) \in E(\mathbb{Z}/p\mathbb{Z})$, en notant :

$$\begin{cases} s = (y_P - y_Q) \times (x_P - x_Q)^{-1} & \text{si } x_P \neq x_Q \text{ et } y_P \neq y_Q \\ s = (3x_P^2 + a) \times (2y_P)^{-1} & \text{si } x_P = x_Q \neq 0 \text{ et } y_P = y_Q \end{cases}$$

Où $^{-1}$ désigne l'inverse modulaire.

Les coordonnées de $R = P \oplus_E Q$ sont données par :

$$\begin{cases} x_R = s^2 - (x_P + x_Q) \\ y_R = s(x_P - x_R) - y_P \end{cases}$$

Enfin, si $y_P \neq y_Q$ et $x_P \neq x_Q$, on a $R = \mathcal{O}$

# Elliptic-Curve-Diffie-Hellman

## Principe du protocole

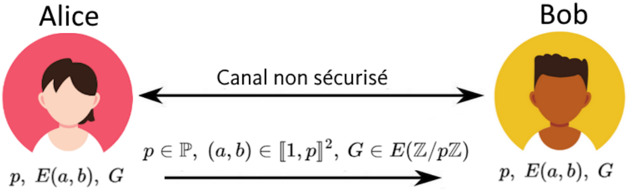



Figure – Protocole ECDH ($E(\mathbb{Z}/p\mathbb{Z})$)

# Elliptic-Curve-Diffie-Hellman

## Principe du protocole

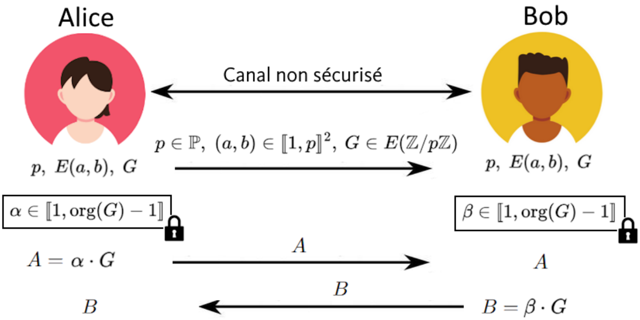



Figure – Protocole ECDH ($E(\mathbb{Z}/p\mathbb{Z})$)

# Elliptic-Curve-Diffie-Hellman

## Principe du protocole

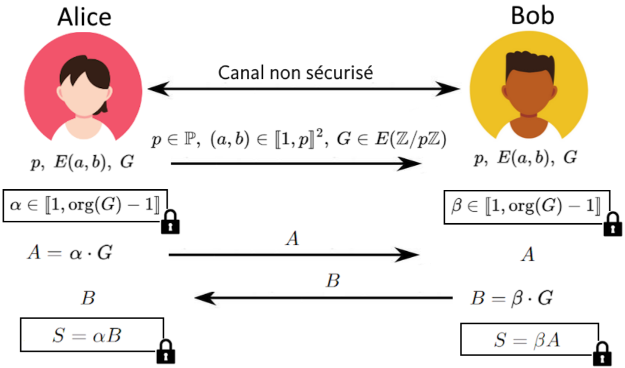



Figure – Protocole ECDH ($E(\mathbb{Z}/p\mathbb{Z})$)

L'algorithme double-and-add (Annexe n°2) utilise la relation suivante :

$$n \cdot P = \begin{cases} \frac{n}{2} \cdot (2 \cdot P) & \text{si } n \mod 2 = 0 \\ \frac{n-1}{2} \cdot (2 \cdot P) \oplus_E P & \text{sinon.} \end{cases}$$

Double-and-add effecute $O(\log_2(n))$ opérations de somme au lieu de $n$.

> **Définition :** (Isogénie) Soient $(E_1, \mathcal{O}_1), (E_2, \mathcal{O}_2)$ deux courbes elliptiques.
> On appelle isogénie un morphisme $\varphi : E_1 \longrightarrow E_2$ vérifiant :
> $$\varphi(\mathcal{O}_1) = \mathcal{O}_2.$$

**Exemple :** morphisme de Frobenius :

$$\pi_p : \begin{array}{ccc} E & \longrightarrow & E^{(r)} \\ (x, y) & \longmapsto & (x^p, y^p) \end{array}$$

où $E^{(r)}$ désigne la courbe elliptique d'équation $x^3 = a^r x^2 + b^r$.

**Théorème :** (Hasse)
Soit $p \in \mathbb{P}$, on a :

$$|\mathrm{Card}(E(\mathbb{Z}/p\mathbb{Z})) - (p+1)| \leq 2\sqrt{p}.$$

**Remarque :** De manière équivalente, on a l'encadrement :

$$(\sqrt{p}-1)^2 \leq \mathrm{Card}(E(\mathbb{Z}/p\mathbb{Z})) \leq (\sqrt{p}+1)^2.$$

# Choix du générateur

## Théorème de Hasse

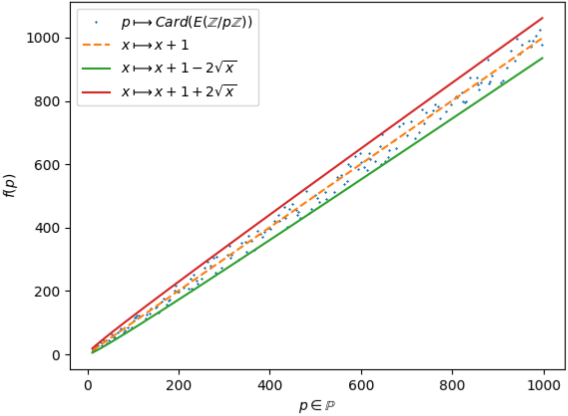



Figure – $\mathrm{Card}(E(\mathbb{Z}/p\mathbb{Z}))$ pour $p \in \mathbb{P} \cap [\![10, 1000]\!]$ et pour $E$ d'équation $y^2 = x^3 - 2x + 3$.

**Théorème :** (Admis)
Si $\varphi : E_1 \longrightarrow E_2$ est une isogénie séparable. Alors :

$$\mathrm{Card}(\ker(\varphi)) = \deg(\varphi).$$

**Lemme :** (Inégalité de Cauchy-Schwartz)
Soit $d : G \longrightarrow \mathbb{Z}$ une forme quadratique définie positive :

$$\forall g, h \in G, |d(g+h) - d(g) - d(h)| \leq \sqrt{2d(h)d(g)}.$$

# Choix du générateur

## Cofacteur

> **Definition :** (Cofacteur) On appelle cofacteur, et on note $h$ la quantité :
> $$h(G) = \frac{\mathrm{Card}(E(\mathbb{Z}/p\mathbb{Z}))}{\mathrm{ord}(G)}.$$

# Choix du générateur

## Cofacteur

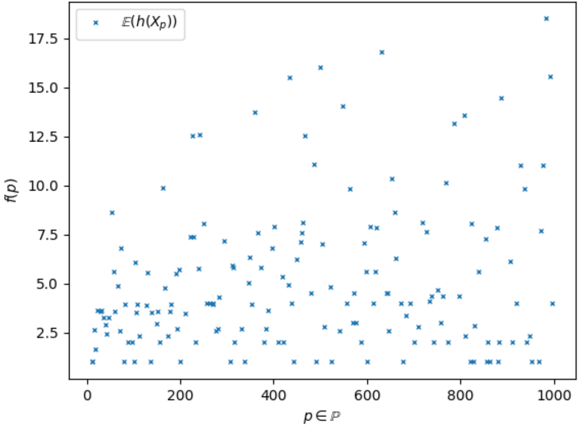



Figure – $\mathbb{E}(h(X_p))$ pour $X_p$ suivant une loi uniforme sur $E(\mathbb{Z}/p\mathbb{Z})$ avec $p \in \mathbb{P} \cap [\![10, 1000]\!]$ et pour $E$ d'équation $y^2 = x^3 - 2x + 3$.

# Choix du générateur

## Cofacteur

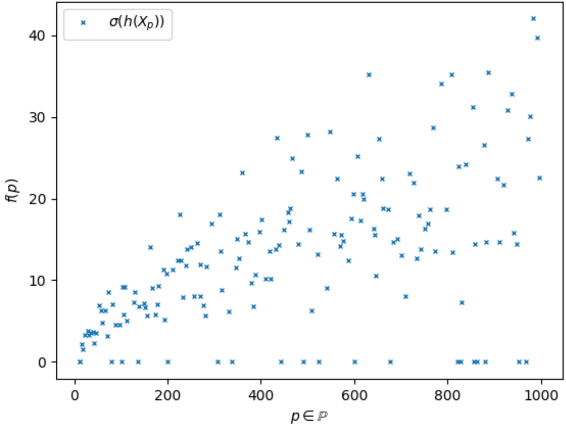



Figure – $\sigma(h(X_p))$ pour $X_p$ suivant une loi uniforme sur $E(\mathbb{Z}/p\mathbb{Z})$ avec $p \in \mathbb{P} \cap [\![10, 1000]\!]$ et pour $E$ d'équation $y^2 = x^3 - 2x + 3$.

Dans la suite, on adopte les notations suivantes :

- Un point quelconque $G \in E(\mathbb{Z}/p\mathbb{Z})$
- Le cardinal de la courbe $N := \mathrm{Card}(E(\mathbb{Z}/p\mathbb{Z})) = \prod_{k=1}^{n} p_k^{a_k}$
- Pour tout $k \in [\![1, n]\!]$, $G_k := \dfrac{N}{p_k^{a_k}} \cdot G$

**Propriété :** Pour tout $k \in [\![1, n]\!]$ :

$$\mathrm{ord}(G_k) = \min\left\{p_k^i \;\middle|\; i \in [\![1, a_k]\!],\ p_k^i \cdot G_k = \mathcal{O}\right\}.$$

**Remarque :** Se calcule en $O(a_k \log_2(p_k))$ additions (Algo. [3])

**Propriété :**

$$\mathrm{ord}(G) = \prod_{k=1}^{n} \mathrm{ord}(G_k)$$

# Bibliographie


- Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Second edition, Springer, 2009, ISBN 978-0-387-09493-9.
- Johannes A. Buchmann, *Introduction to cryptography*, Springer, 2001, ISBN 978-0-387-95034-1.
- A van Tuyl, *The field of N-torsion points of an elliptic curve over a finite field*, PhD thesis, M. Sc. Thesis, McMaster University, 1997.
- Rene Schoof, *Elliptic Curves over Finite Fields and the Computation of Square Roots mod p*, Mathematics of Computation, Vol. 44, No. 170, 1985.

## Annexe n°1 : Algorithme d'Euclide étendu pour le calcul de l'inverse modulaire

**Input :** $k \in \mathbb{Z}, p \in \mathbb{N}$ avec $p > 0$
**Output :** L'inverse modulaire $k^{-1} \mod p$ si celui-ci existe,
sinon lève une erreur
$a \leftarrow k,\ b \leftarrow p$
$x_0 \leftarrow 1,\ x_1 \leftarrow 0$
**tant que** $b \neq 0$ **faire**
  $q \leftarrow \lfloor a/b \rfloor$
  $(a, b) \leftarrow (b, a \mod b)$
  $(x_0, x_1) \leftarrow (x_1, x_0 - q \times x_1)$
**fin**
**si** $a \neq 1$ **alors**
  **lever** erreur
**fin**
**retourner** $x_0 \mod p$

**Input :** $k \in \mathbb{N}, P \in E(\mathbb{Z}/p\mathbb{Z})$
**Output :** $kP$
**si** $k = 0$ **alors**
  **retourner** $\mathcal{O}$
**fin**
$R \leftarrow \mathcal{O}$
$P_0 = P$ **tant que** $k > 0$ **faire**
  **si** $k \mod 2 = 1$ **alors**
    $R \leftarrow R \oplus_E P_0$
  **fin**
  $P_0 \leftarrow P_0 \oplus_E P_0$
  $k \leftarrow \lfloor k/2 \rfloor$
**fin**
**retourner** $R$

**Input :** $G_k \in E(\mathbb{Z}/p\mathbb{Z}), p_k \in \mathbb{P}$

**Output :** $\mathrm{ord}(G_k) = \min\left\{p_k^i \;\middle|\; i \in [\![1, a_k]\!],\ p_k^i \cdot G_k = \mathcal{O}\right\}$

$P \leftarrow G_k$

$i \leftarrow 0$

**tant que** $P \neq \mathcal{O}$ **faire**

  $i \leftarrow i + 1$

  $P \leftarrow p_k \cdot P$ (Algorithme 2)

**fin**

**retourner** $p^i$

**Input :** $p \in \mathbb{P}$, $A, B \in [\![1, p-1]\!]$, $g \in p$
**Output :** La clé secrète $A^b$ ou $B^a$
$r \leftarrow g$;
**pour** $k \in [\![1, p-1]\!]$ **faire**
  **si** $r = A$ **alors**
    **retourner** $B^k \mod p$
  **fin**
  **si** $r = B$ **alors**
    **retourner** $A^k \mod p$
  **fin**
  $r \leftarrow (r \times g) \bmod p$;
**fin**