DEFINITION DES COURBES ELLIPTIQUES

On appelle **courbe elliptique** une courbe dans le plan définie par l'équation de la forme :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

qui n'est pas singulière, c'est-à-dire que la courbe n'a aucune intersection avec elle-même. Les coefficients a_1, a_2, a_3, a_4, a_6 sont des éléments d'un corps K donné.

En cryptographie, on s'intéresse plus particulièrement aux courbes qui ont une équation de la forme

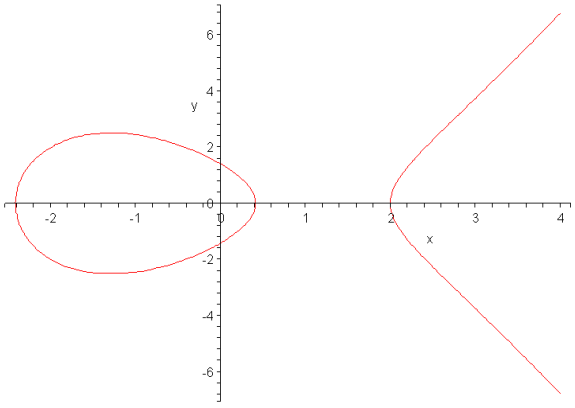
$$\boxed{y^2 = x^3 + ax + b}$$

Pour qu'une courbe de ce type ne soit pas singulière, le discriminant $\Delta = -16(4a^3 + 27b^2)$ doit être non nul.

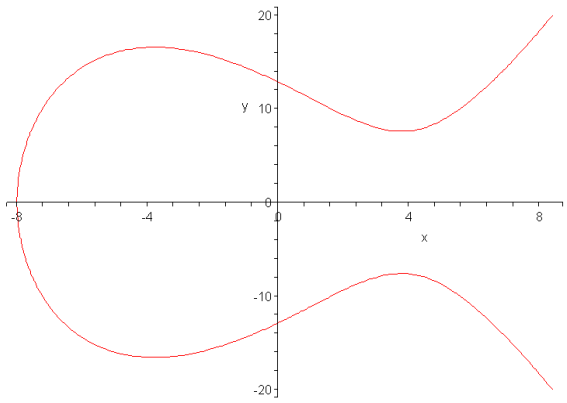
On note $E(K) = \left\{(x, y) \in K^2 \;\middle|\; y^2 = x^3 + ax + b\right\}$ l'ensemble des points de la courbe elliptique.

COURBES ELLIPTIQUES SUR LE CORPS DES REELS $\mathbb{R}$

Courbes elliptiques non singulières

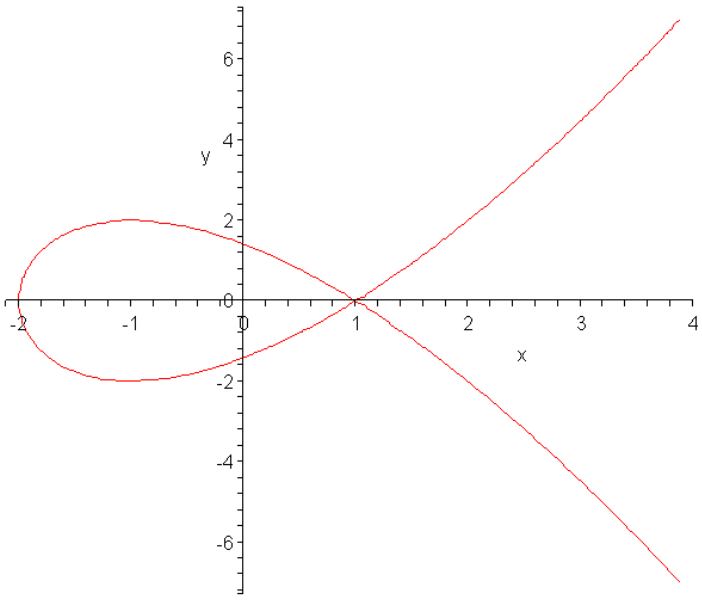


$y^2 = x^3 - 5x + 2$



$y^2 = x^3 - 43x + 166$

Courbe elliptique singulière



$y^2 = x^3 - 3x + 2$

COURBES ELLIPTIQUES SUR LE CORPS ($\mathbb{Z}_{/p\mathbb{Z}}$)

Soit *p* un nombre premier

On pose $\mathbb{Z}_{/p\mathbb{Z}} = \left\{\bar{0},\bar{1},...,\overline{p-1}\right\}$ défini tel que $\forall a \in \mathbb{Z},\ a = \bar{x}$, où *x* est le reste dans la division euclidienne de *a* par *p*.

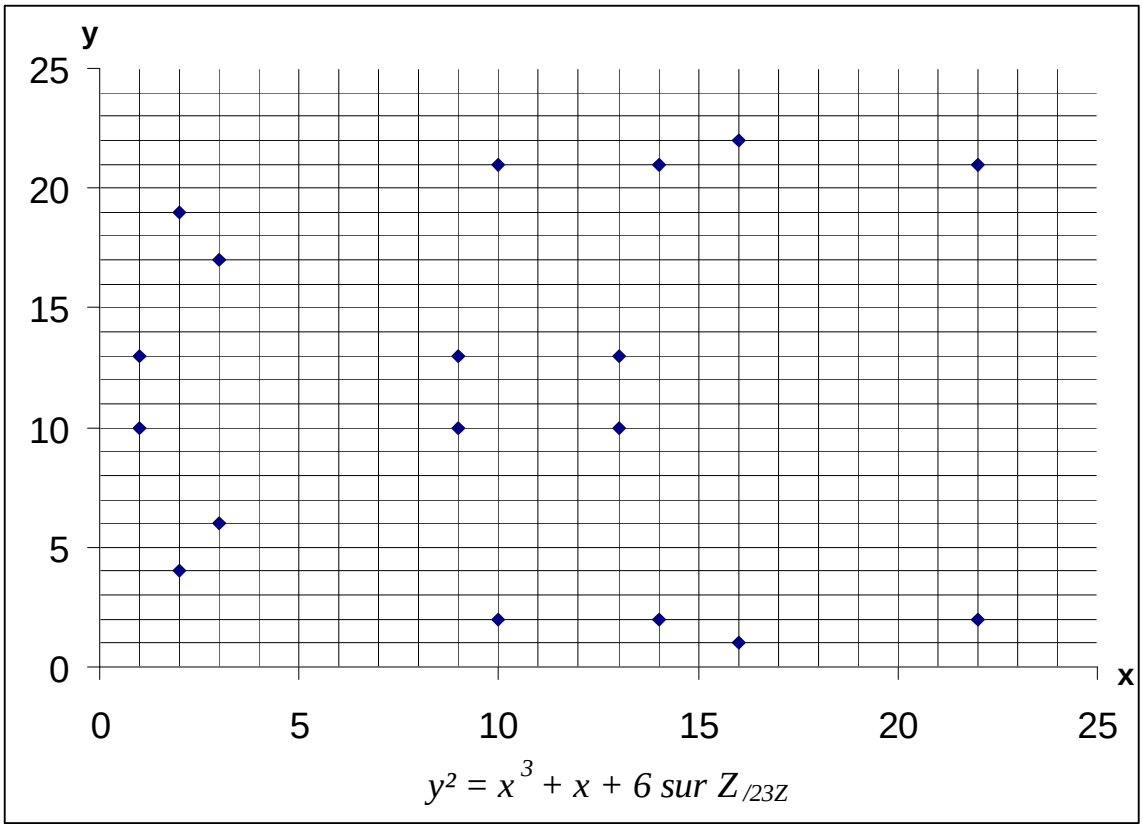
($\mathbb{Z}_{/p\mathbb{Z}}$, +) est un groupe commutatif :

- $\forall(\bar{x},\bar{y}) \in (\mathbb{Z}_{/p\mathbb{Z}})^2,\ \bar{x}+\bar{y} = \bar{y}+\bar{x}$
- $\forall(\bar{x},\bar{y},\bar{z}) \in (\mathbb{Z}_{/p\mathbb{Z}})^3,\ (\bar{x}+\bar{y})+\bar{z} = \bar{x}+(\bar{y}+\bar{z})$
- $\forall \bar{x} \in \mathbb{Z}_{/p\mathbb{Z}},\ \bar{x}+\bar{0} = \bar{x}$
- $\forall \bar{x} \in \mathbb{Z}_{/p\mathbb{Z}},\ \bar{x}+\overline{(-x)} = \bar{0}$

($\mathbb{Z}_{/p\mathbb{Z}}^{*}$, ×) est un groupe commutatif :

- $\forall(\bar{x},\bar{y}) \in (\mathbb{Z}_{/p\mathbb{Z}}^{*})^2,\ \bar{x}\times\bar{y} = \bar{y}\times\bar{x}$
- $\forall(\bar{x},\bar{y},\bar{z}) \in (\mathbb{Z}_{/p\mathbb{Z}}^{*})^3,\ (\bar{x}\times\bar{y})\times\bar{z} = \bar{x}\times(\bar{y}\times\bar{z})$
- $\forall \bar{x} \in \mathbb{Z}_{/p\mathbb{Z}}^{*},\ \bar{x}\times\bar{1} = \bar{x}$
- $\forall \bar{x} \in \mathbb{Z}_{/p\mathbb{Z}}^{*},\ \exists!\,\overline{x'} \in \mathbb{Z}_{/p\mathbb{Z}}^{*} \mid \bar{x}\times\overline{x'} = \bar{1}$

Pour résumer tout cela, on dit que ($\mathbb{Z}_{/p\mathbb{Z}}$, + , ×) est un corps commutatif. On peut donc définir des courbes elliptiques sur ce corps.



ADDITION DES POINTS SUR UNE COURBE ELLIPTIQUE

On définit une loi additive sur E(K) où l'on a rajouté également un point noté $\mathcal{O}$ appelé point à l'infini et qui vérifie : P + $\mathcal{O}$ = P

Soient P(x_1,y_1) et Q(x_2,y_2) deux points de E($\mathbb{R}$).
On définit les coordonnées (x_3,y_3) du point P+Q ainsi :

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = -\lambda(x_3 - x_1) - y_1 \end{cases} \quad \text{où} \quad \lambda = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & si\ x_1 \neq x_2 \\ \dfrac{3x_1^2 + a}{2y_1} & si\ x_1 = x_2 \end{cases}$$

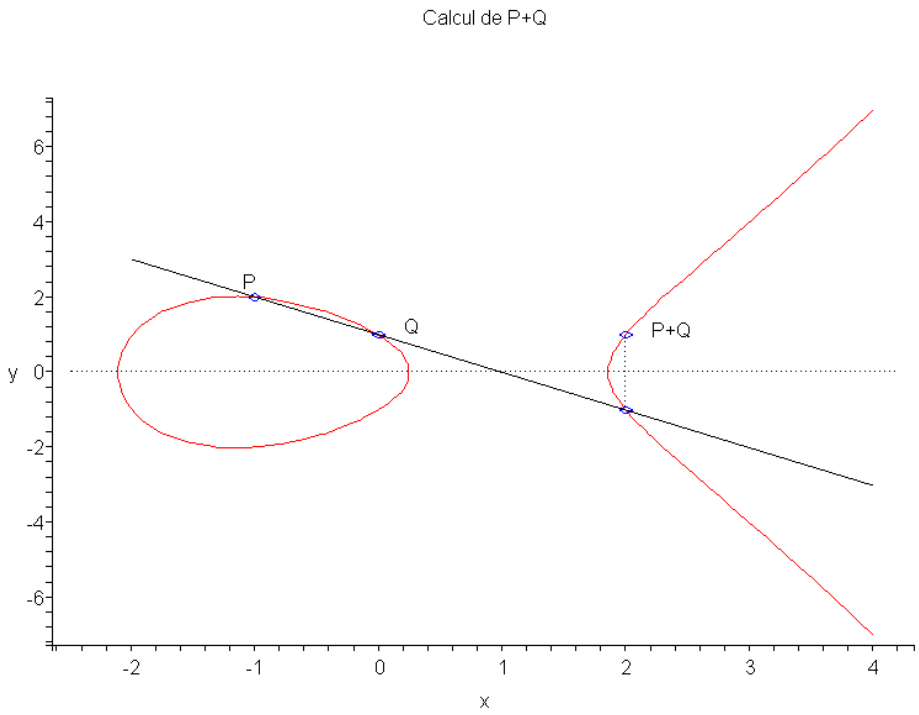
Dans $\mathbb{Z}_{/p\mathbb{Z}}$, ces égalités deviennent des congruences, c'est à dire :

$$\begin{cases} x_3 \equiv \lambda^2 - x_1 - x_2\ [p] \\ y_3 \equiv -\lambda(x_3 - x_1) - y_1\ [p] \end{cases} \quad \text{où} \quad \lambda \equiv \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2}\ [p]\ si\ x_1 \neq x_2 \\ \dfrac{3x_1^2 + a}{2y_1}\ [p]\ si\ x_1 = x_2 \end{cases}$$

(E(K) , +) est un groupe! C'est la base de la cryptographie.

Remarque : - P(x,y) = P(x,-y)

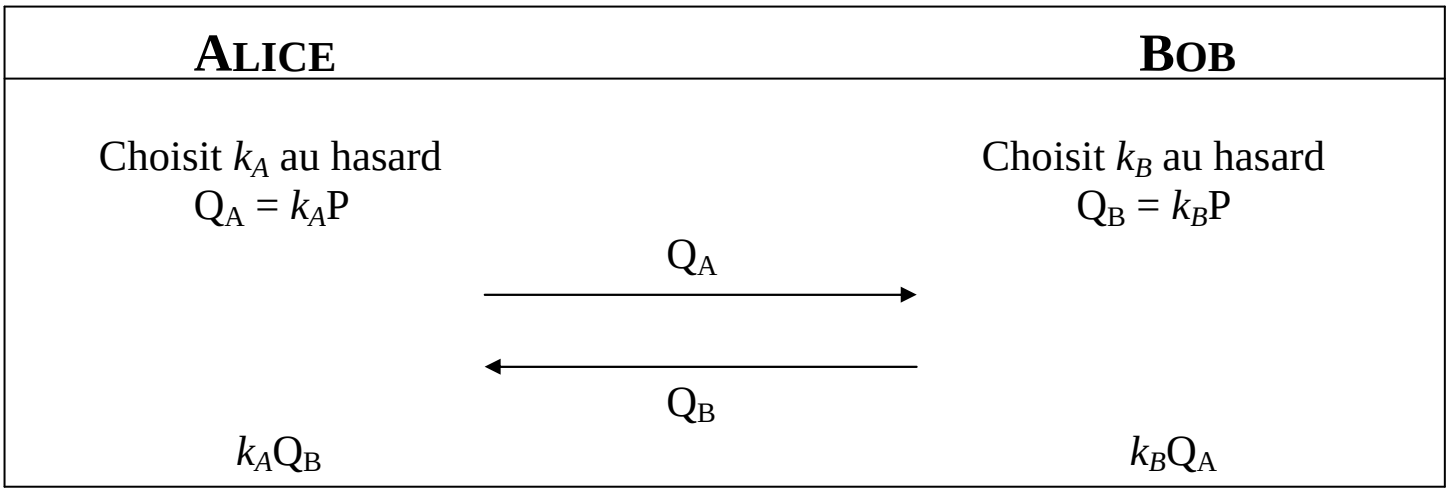
Propriété géométrique de l'addition de deux points sur une courbe elliptique définie sur $\mathbb{R}$:



FABRICATION DE LA CLE SECRETE

Alice et Bob se mettent d'accord sur une courbe elliptique E(a,b,K), c'est-à-dire qu'ils choisissent un corps fini K (ex : $\mathbb{Z}_{/p\mathbb{Z}}$), et une courbe elliptique $y^2 = x^3 + ax + b$. Ils se mettent aussi d'accord sur un point P situé sur la courbe.

La donnée de (a,b,K,P) constitue la **clé publique**.



Après l'échange, Alice posséde $k_A Q_B = k_A k_B P$ et Bob possède $k_B Q_A = k_B k_A P$.

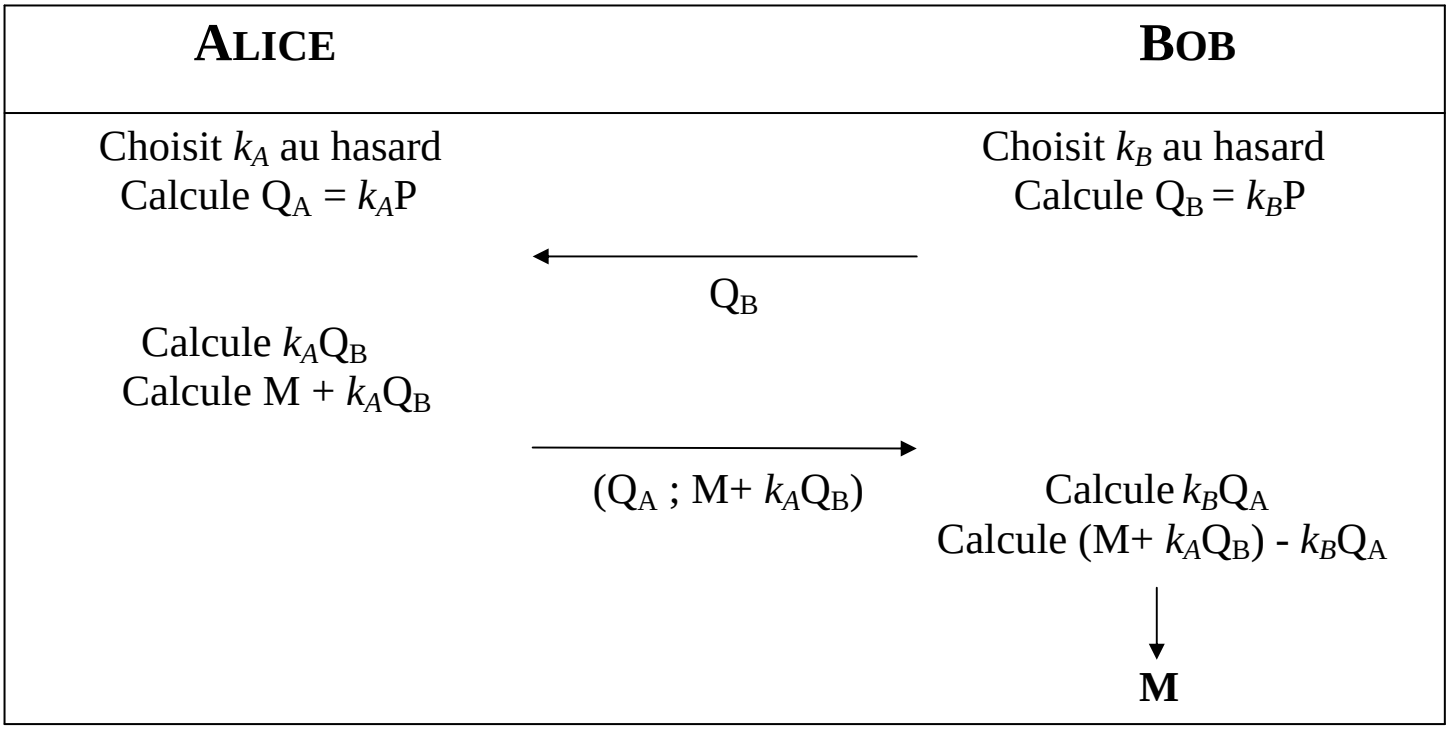
$$k_A k_B P = k_B k_A P$$

Alice et Bob sont chacun en possession de $k_A k_B P$, qui constitue leur **clé secrète.**

PROTOCOLE DE LA TRANSMISSION D'UN MESSAGE

Dans la réalité, l'échange n'a pas lieu comme décrit ci-dessus.
Supposons que Alice souhaite envoyer un message à Bob.
On suppose qu'auparavant Alice et Bob se sont mis d'accord sur une façon d'associer les caractères alphanumériques à des points de la courbe.

Alice choisit un point M de la courbe correspondant au caractère qu'elle souhaite envoyer à Bob.



Bob a donc récupéré le point M et est capable de le faire correspondre à une lettre.
Pour envoyer un texte, Alice envoie donc une liste de couples de points et son $Q_A = k_A P$ à Bob, qu'il parvient à décrypter en calculant $k_B Q_A$ et en retranchant ce point a chacun des points de la liste

SURETE DU CRYPTAGE

La sécurité de ce protocole est basée sur le fait que si un individu extérieur intercepte Q_A et Q_B, il lui est quasiment impossible de retrouver k_A ou k_B, donnée indispensable pour pouvoir calculer $k_A k_B P$ et donc décrypter le message. C'est ce qu'on appelle le problème du logarithme discret.

Par exemple, dans le groupe $(\mathbb{Z}_{/97\mathbb{Z}}^{*}, \times)$ (97 est un nombre premier) :
Pour trouver la $k^{ième}$ puissance de l'un des nombres de ce groupe (exponentiation discrète), il faut élever ce nombre à la puissance k et calculer le reste de la division par p.

Ex : $50^{12} = 244140625000000000000$ et le reste de la division entière de 50^{12} par 97 est 96.

Le logarithme discret est le problème inverse : étant donné $50^k \equiv 96 \pmod{97}$, quel est le plus petit k pour lequel cette proposition est vrai ?

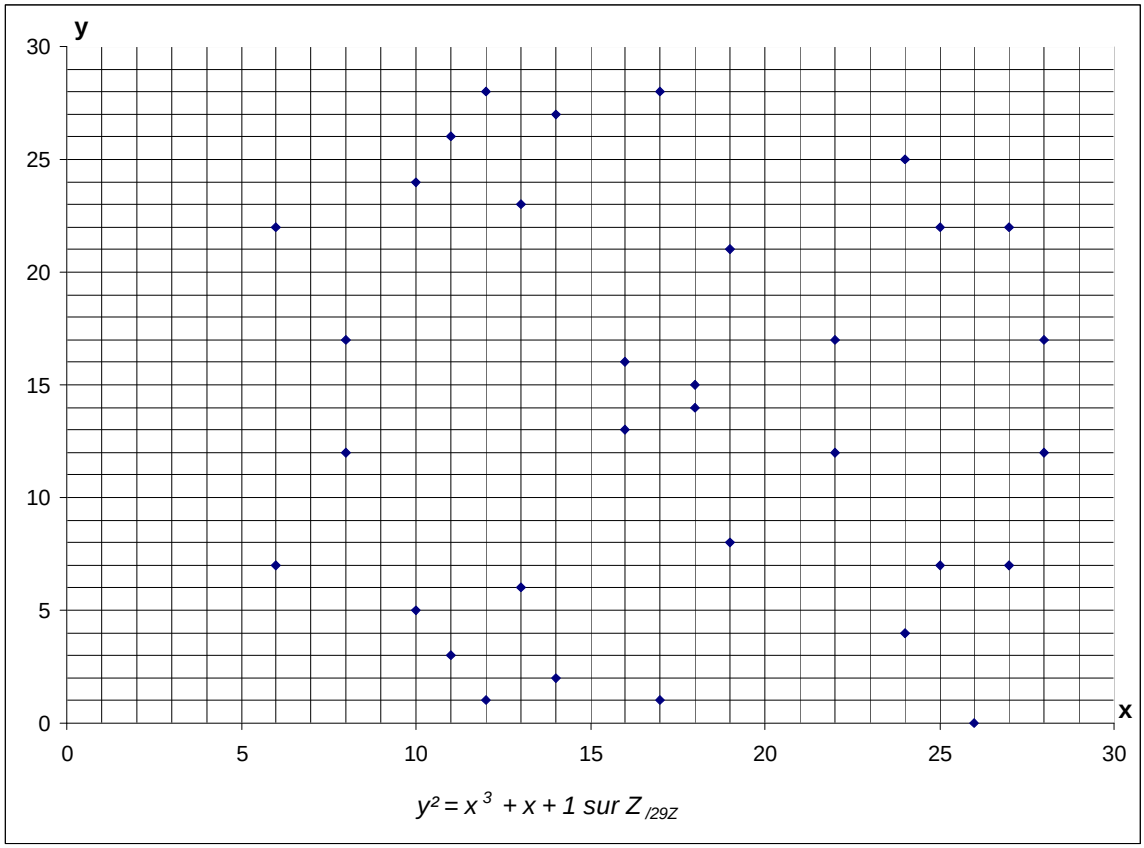
On comprend que pour des nombres premiers relativement grands, le problème du logarithme discret devient insoluble en un temps raisonnable avec les algorithmes existant actuellement.

Retour sur le cas des courbes elliptiques :

Etant donné kP, le problème est de retrouver k connaissant P.

Un algorithme naïf calculant successivement 2P, 3P, … jusqu'à trouver k est envisageable lorsque k est suffisamment petit. L'inconvénient est que, dans la pratique, il est possible de choisir k suffisamment grand pour rendre cet algorithme inefficace.
Il existe d'autres algorithmes plus poussés, mais qui peuvent être rendus inefficaces également par quelques précautions lors du choix du corps K et de k.

Aujourd'hui, on ne dispose donc pas d'algorithme efficace pour résoudre le problème du logarithme discret sur le groupe des courbes elliptiques.



A=(6,7)	F=(10,24)	K=(13,6)	P=(16,13)	U=(19,8)
B=(6,22)	G=(11,3)	L=(13,23)	Q=(17,1)	V=(19,21)
C=(8,12)	H=(11,26)	M=(14,2)	R=(17,28)	W=(22,12)
D=(8,17)	I=(12,1)	N=(14,27)	S=(18,14)	X=(22,17)
E=(10,5)	J=(12,28)	O=(16,16)	T=(18,15)	Y=(24,4)
				Z=(24,25)

On choisit Ω=(28,12)

Benoît prend k_B=4 et calcule k_B Ω =(13,23), puis l'envoie à Alexandre
Alexandre prend k_A=8 et calcule k_A Ω = (10,24) et $k_A(k_B$ Ω)= (13,6)

Alexandre veut envoyer à Benoît le texte suivant : « BONJOUR ».
Il calcule donc B + (13,6) , O + (13,6) , N + (13,6) , J + (13,6) , U + (13,6), R + (13,6)
Il obtient alors la liste Δ={(17,28) ; (24,25) ; (8,12) ; (24,4) ; (24,25) ; (10,24) ; (22,17)}
Il envoie à Benoît la liste :

{**(10,24)** ; **(17,28)** ; **(24,25)** ; **(8,12)** ; **(24,4)** ; **(24,25)** ; **(10,24)** ; **(22,17)**}

k_A Ω — Δ

Lorsque Benoît reçoit cette liste, il calcule $k_B(k_A$ Ω)=(13,6), puis retranche ce point a chaque point de la liste Δ pour retrouver le texte en clair.
Par exemple, (17,28) - (13,6) = (17,28) + (13,-6) = (6,22) = B
Il retrouve donc bien la première lettre du message.
En itérant le processus, Benoît découvre le message « BONJOUR ».