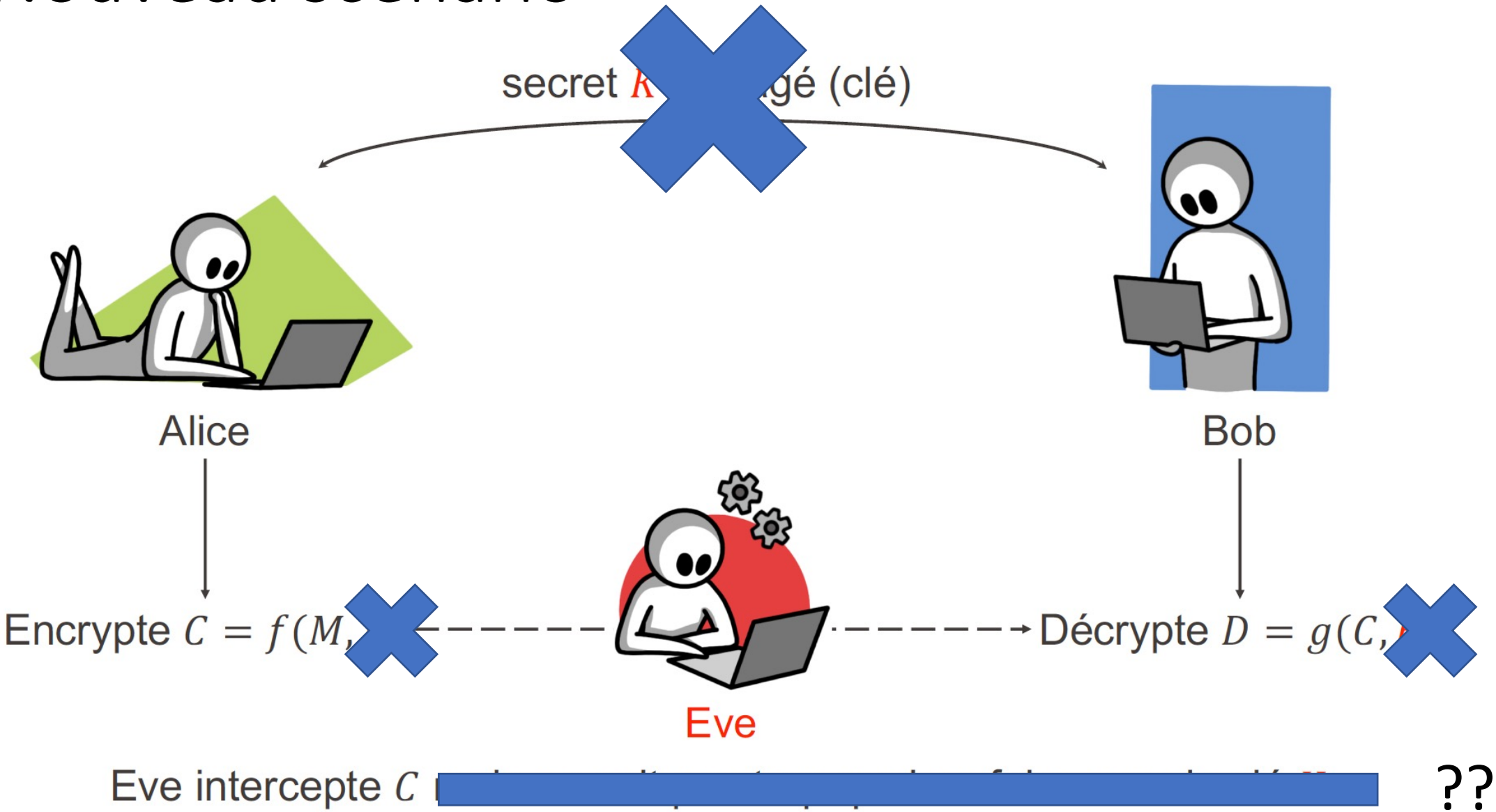
Cryptographie à clé publique

Cours Turing – Semaine 11

Nouveau scénario



???

Protocole d'échange de clé de Diffie-Hellman-Merkle: principe

Tout le monde sait multiplier
Mais personne ne sait diviser

Kevin (N_1) , Tressy (N_2) , autre nombre M

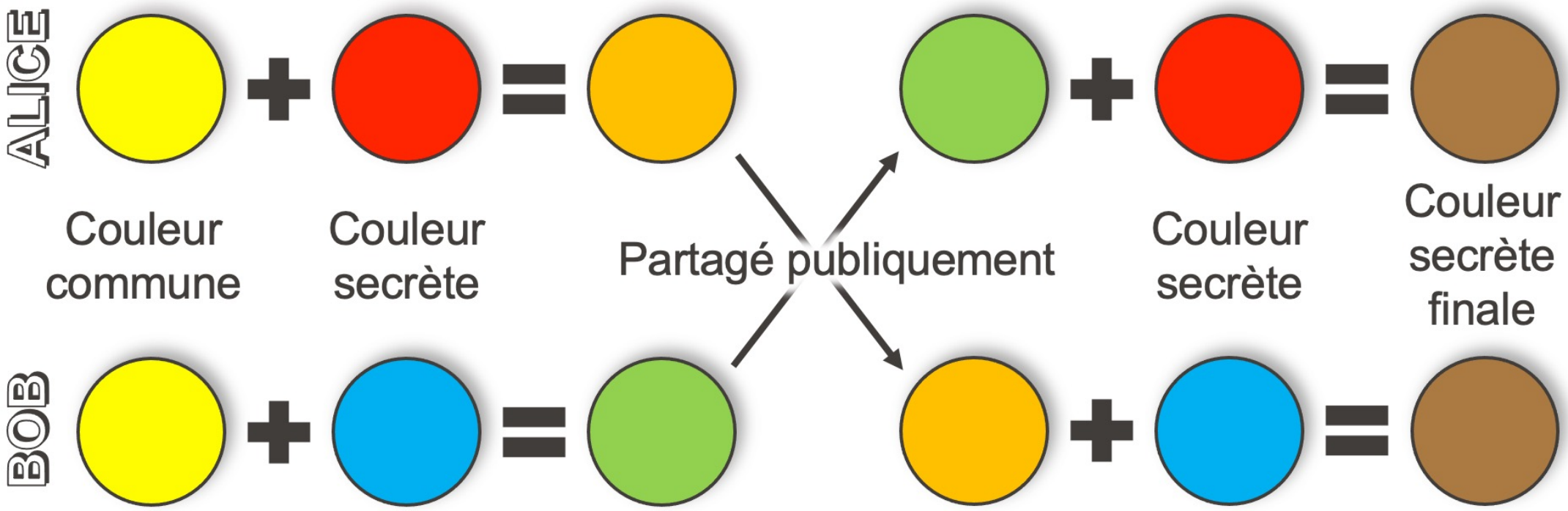
M = 147

$N_3 = 135'681$

$N_4 = 115'101$

$(K) = \boxed{106'238'223}$

Avec des pots de peinture



Fonctions à sens unique

Définition

F est une fonction à sens unique si

1. Pour toute valeur de A, $F(A)$ est facile à calculer.

2. Pour toute valeur de B dans l'image de F, il est très difficile de retrouver une valeur de A telle que $F(A) = B$.

Contre-exemples

- $F(A) = 0$ pour toute valeur de A

B = 0 => n'importe quel A convient !

- $F(A) = A\ (mod\ N)$

B => choisir A = B !

Exemples

- $F(A) = A^2 (mod\ N)$ où $N = P \cdot Q$ avec P et Q premiers

→ exercices

- $F(B) = A^B (mod\ N)$ où N est premier et $2 \leq A \leq N - 1$

Si on donne $C = A^B \pmod N$, et A et N,

il est très difficile de retrouver B [Si N est un grand nombre premier !]

= problème du logarithme discret !

En arithmétique classique :

Si $A^B = C$ et on nous donne A et C

$\Longrightarrow$ $B = \log_A(C)$

⚠ utiliser pow(A, B, N)

Le vrai protocole de Diffie-Hellman-Merkle

- Alice choisit A_1 (secret)
  Bob choisit B_1 (secret)
  } choisissent ensemble N (grand nb premier) et $2 \leq M \leq N-1$ publics

- Alice calcule $A_2 = M^{A_1} \pmod N$ et publie A_2
  Bob calcule $B_2 = M^{B_1} \pmod N$ et publie B_2

- Alice calcule $B_2^{A_1} \pmod N = K$
  Bob calcule $A_2^{B_1} \pmod N = K$

- $B_2^{A_1} \pmod N = \left(M^{B_1} \pmod N\right)^{A_1} \pmod N$

$= \left(M^{B_1}\right)^{A_1} \pmod N = \underbrace{M^{B_1 \cdot A_1} \pmod N}_{= K}$

- $A_2^{B_1} \pmod N = \left(M^{A_1} \pmod N\right)^{B_1} \pmod N$

$= \left(M^{A_1}\right)^{B_1} \pmod N = \underbrace{M^{A_1 \cdot B_1} \pmod N}_{= K}$

$=$

Le vrai protocole de Diffie-Hellman-Merkle

Que peut faire Eve ?

Elle connaît M, N, $A_2 = M^{A_1} \pmod N$

et $B_2 = M^{B_1} \pmod N$

Remarque : Alice n'est pas capable de retrouver B_1

Bob " " A_1

Eve : $C_1 \oplus C_2 \oplus C_3 = K$

Intermède: un autre protocole d'échange de clé ??

- Pour transmettre une clé K à Bob, Alice protège celle-ci avec une clé K_1 et envoie $C_1 = K \oplus K_1$ à Bob.

- Puis Bob protège C_1 avec une clé K_2 et renvoie ainsi à Alice:

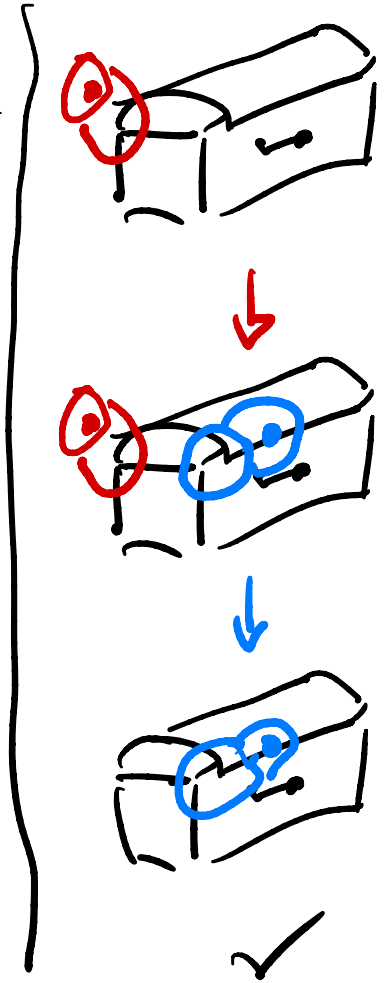
$$C_2 = C_1 \oplus K_2 = K \oplus K_1 \oplus K_2$$

- Alice effectue le XOR de C_2 avec sa clé K_1 et renvoie à Bob:

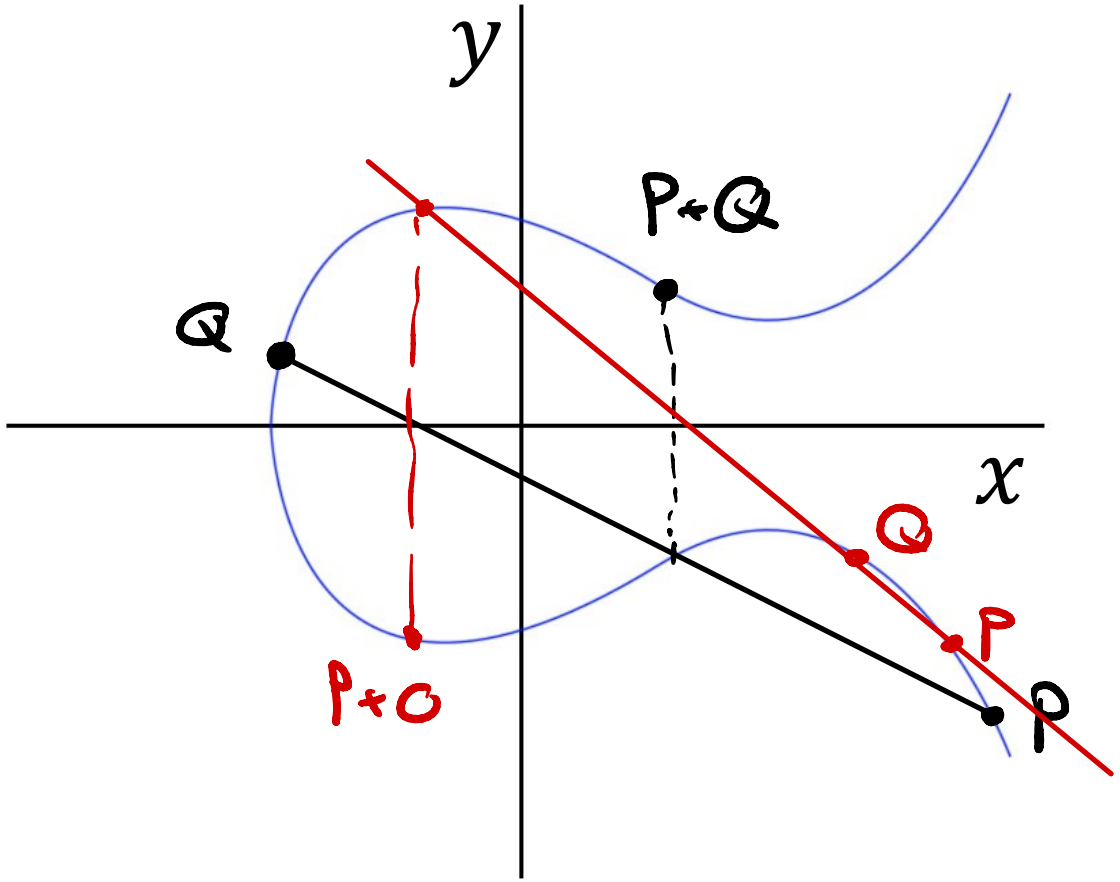
$$C_3 = C_2 \oplus K_1 = K \oplus K_1 \oplus K_2 \oplus K_1 = K \oplus K_2$$

- Bob effectue à son tour le XOR de C_3 avec sa clé K_2 et obtient ainsi:

$$C_3 \oplus K_2 = K \oplus K_2 \oplus K_2 = K$$



Et maintenant avec des courbes elliptiques!

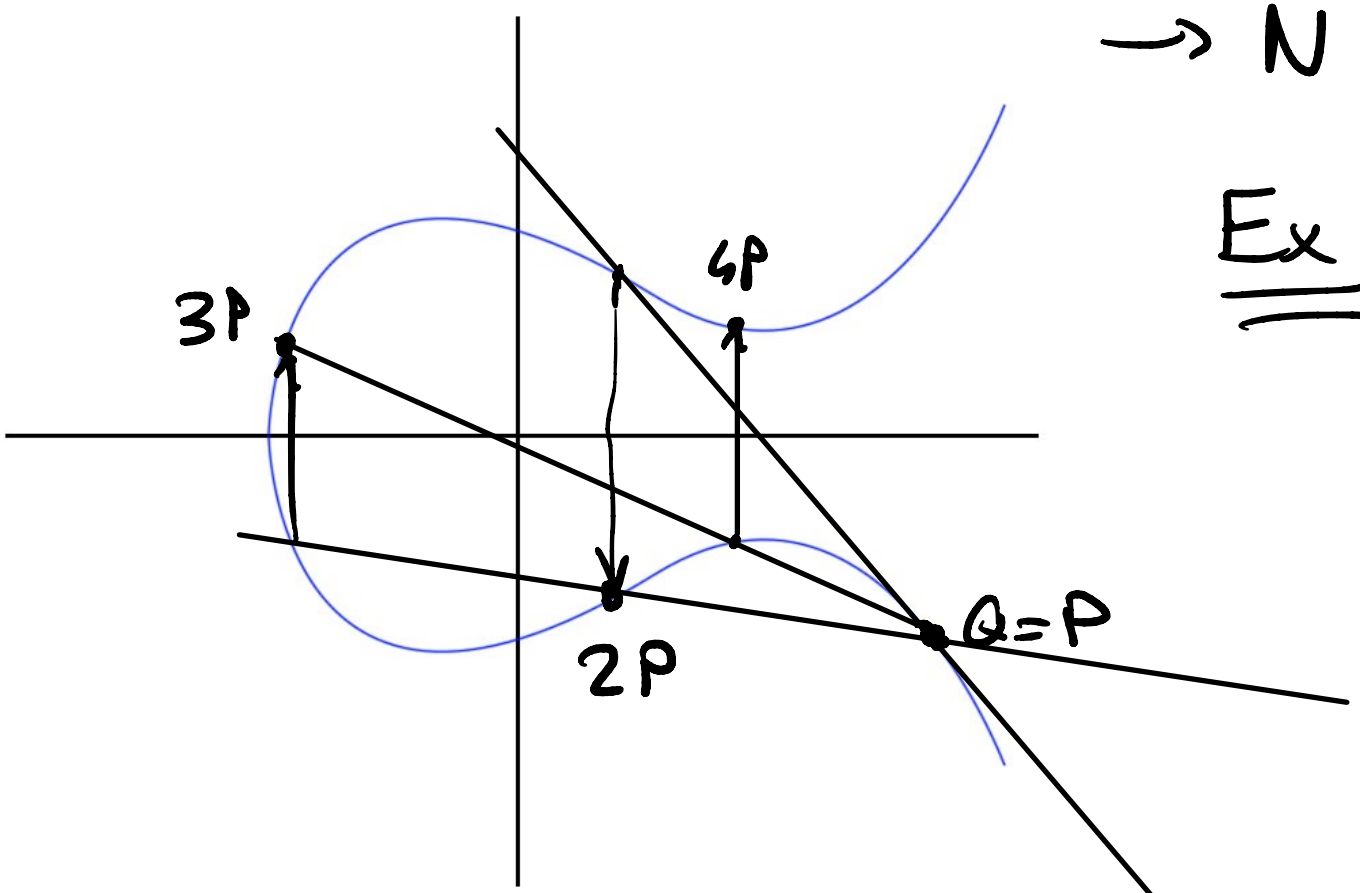


$$y^2 = x^3 + ax + b \quad (a = -3,\ b = +5)$$

Courbes elliptiques (suite)

$P \to 2P \to 3P \to 4P$

$\to NP$



Ex : $N = 43$

$= 32 + 8 + 2 + 1$

$43P = 32P + 8P + 2P + P = 2(2(2(2(2P)))) + 2(2(2P)) + 2P + P$

Courbes elliptiques (suite)

Alice et Bob choisissent P

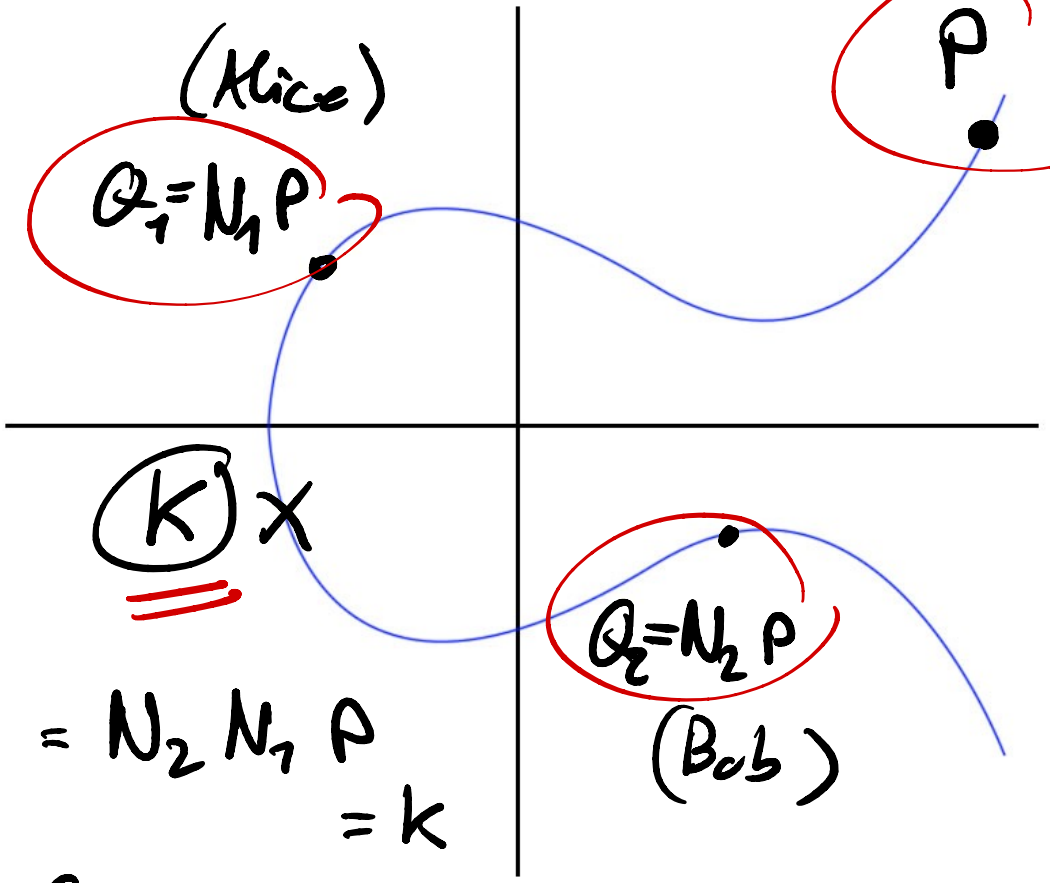
Alice choisit N_1

Bob choisit N_2

Alice calcule $N_1 P$

Bob calcul $N_2 P$

publiés



Bob calcule $N_2 Q_1 = N_2 N_1 P = k$

Alice calcule $N_1 Q_2 = N_1 N_2 P$

Ex. 2 & 3 calcul de la racine modulo N

ie. pour un nombre C donné

trouver le nombre M tel que $M^2 \pmod N = C$

Ex 2 : $N = P$ premier $\Rightarrow$ facile de calculer M

Ex 3 : $N = P \cdot Q$, avec P et Q premiers

on cherche M tq $M^2 \pmod N = C$