

---

# Arithmétique et cryptologie

Karim Belabas

Karim.Belabas@math.u-psud.fr

<http://www.math.u-psud.fr/~belabas/>

Université Paris-Sud

France

Un grand nombre d'« informations » peuvent se traduire numériquement (parfois imparfaitement, mais avec des différences imperceptibles). Par exemple un programme informatique, un CD, une image, un texte.

Ce texte-ci par exemple :

Un mathématicien est une machine à  
transformer le café en théorèmes.

– Paul Erdős

On peut le coder en **ASCII** : chaque signe est représenté par deux symboles, choisis parmi les 16 suivants

$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f\}$ ,

c'est-à-dire un nombre à deux chiffres en base **16** :

'U'	→	55,	' '	→	20,
'n'	→	6e,	'm'	→	6d, ...

On peut interpréter cette suite de chiffres comme un grand nombre, écrit en base 16 :

U n m a t h é m a t i c i e n e s t u n e m a c h  
556e206d617468e96d6174696369656e2065737420756e65206d6163686  
96e6520e0207472616e73666f726d6572206c6520636166e920656e2074  
68e96f72e86d65732e202d2d205061756c20457264f673 (base 16)

$$= 3 + 7 \times 16^1 + 6 \times 16^2 + 15 \times 16^3 \dots =$$

99781154227264479227165858852054752813050341969418003789560  
01073332481166880538368439248938141894959742557027653964490  
42897857270188655105046183260538732733952271900145229312269  
36244913388202030707. (base 10 : 197 chiffres décimaux).

**Chiffrer** : modifier une information, en utilisant une procédure secrète ou **clé**.

**Déchiffrer** : le retrouver en utilisant la clé.

**Décrypter** : découvrir la clé.

Un chiffrage très simple :  $A \xrightarrow{+1} B, B \xrightarrow{+1} C, \text{ etc.}$

Bonjour  $\xrightarrow{+1}$  Cpokpvs  $\xrightarrow{-1}$  Bonjour

Plus compliqué : faire des groupes de lettres et les décaler en changeant le décalage au sein du groupe

Bonjour  $\xrightarrow{+1,3,2}$  Crpkrws  $\xrightarrow{-1,3,2}$  Bonjour

On dit que 1, 3, 2 (ou 132) est la **clé** utilisée pour chiffrer le message. Dans ce cas, plus la clé est longue, plus il est difficile de **décrypter**.

Problèmes :

- comment se mettre d'accord sur une clé sans risque d'interception ?
- chiffrer/déchiffrer sont des opérations très proches. Si le chiffeur se fait prendre, et avec lui la clé, l'ennemi peut déchiffrer tous les messages.

# Échange de clés (1/2)

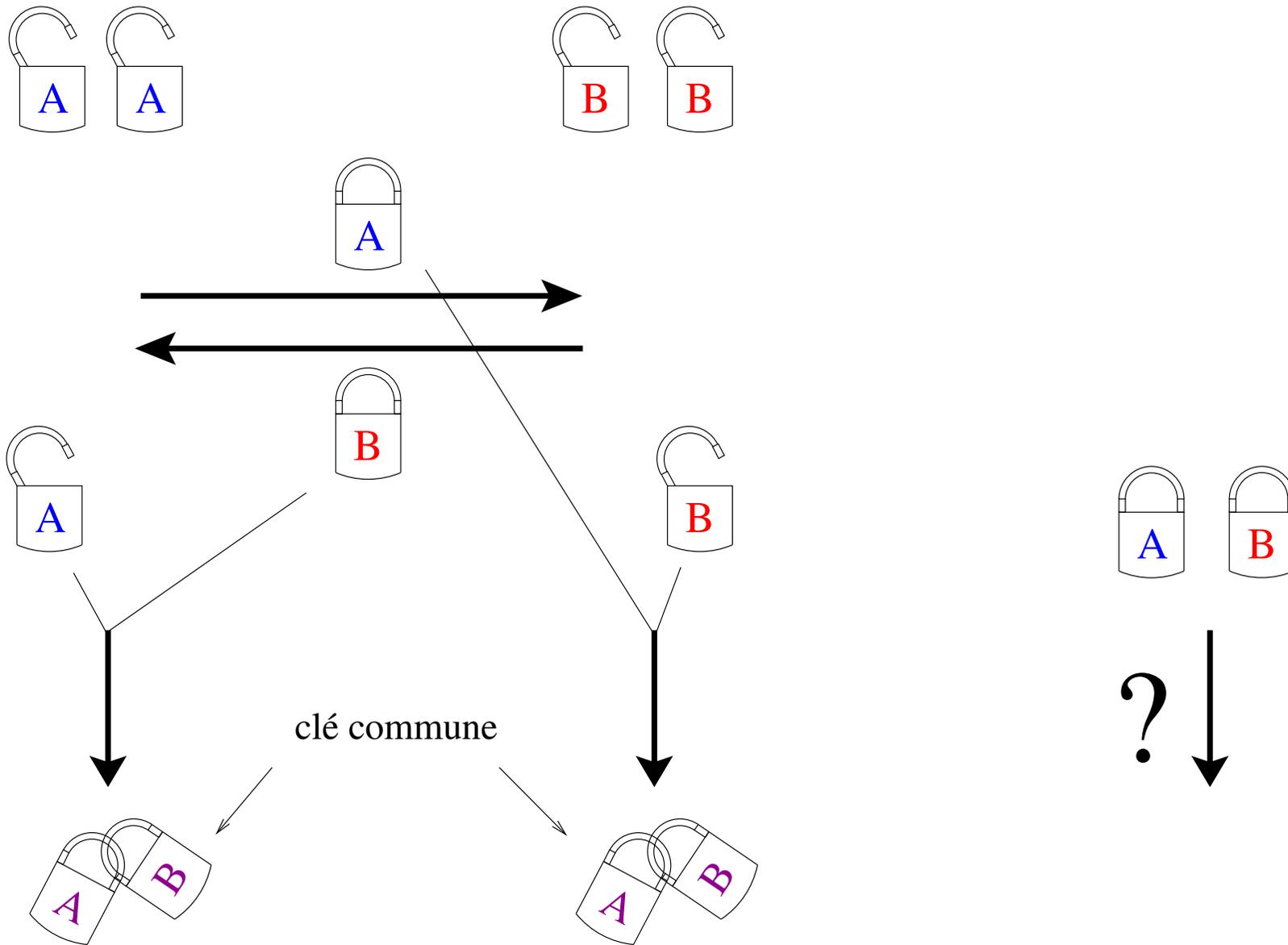
Anatole et Barnabé choisissent en secret, un entier chacun :  $a$  pour Anatole,  $b$  pour Barnabé. Ils se téléphonent, choisissent un ensemble  $G$  dont ils savent multiplier les éléments (par exemple, les entiers) et un objet  $g$  dans cet ensemble (par exemple le nombre 10).

Ils dévoilent chacun  $A = g^a$  et  $B = g^b$  ( $a$  et  $b$  restent secrets !). Tous deux peuvent alors calculer la clé secrète :

$$\text{clé} := A^b = B^a = g^{ab}$$

Un espion éventuel ne connaît que  $g$ ,  $A$ , et  $B$ . L'opération qui consiste à retrouver  $a$  à partir de  $A$  ou  $b$  à partir de  $B$  s'appelle **extraire un logarithme** (en base  $g$ ). Il faut que ce soit une opération difficile pour empêcher l'espion de déterminer la clé. Malheureusement, si  $G = \mathbb{N}$  c'est beaucoup trop simple. Par exemple, si  $g = 10$ , pour résoudre  $10^x = 1000000000$ , il suffit de compter les 0 ( $x = 9$ ).

# Échange de clés (2/2)



# Une étrange façon de compter (1/4)

---

On fixe un entier  $N$  et on regroupe tous les entiers dont la division par  $N$  donne le même reste. Par exemple si  $N = 2$ , on a deux groupes : les entiers pairs (reste 0) et les impairs (reste 1). On écrit

$$x \equiv y \pmod{N}$$

pour

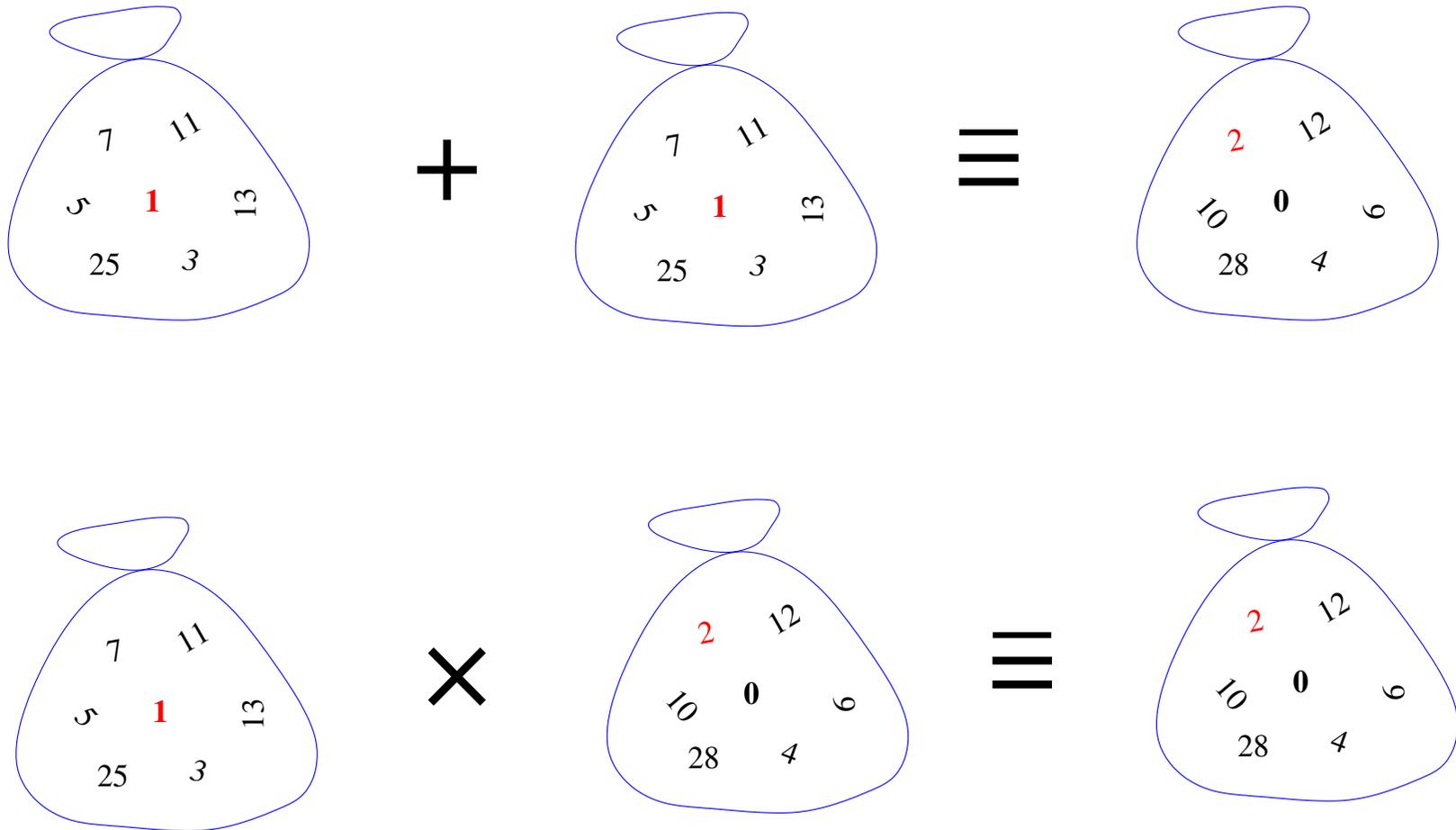
«  $x$  et  $y$  sont dans le même sac ».

Il y a exactement  $N$  sacs différents, et on appelle l'ensemble des sacs  $\mathbb{Z}/N$ .

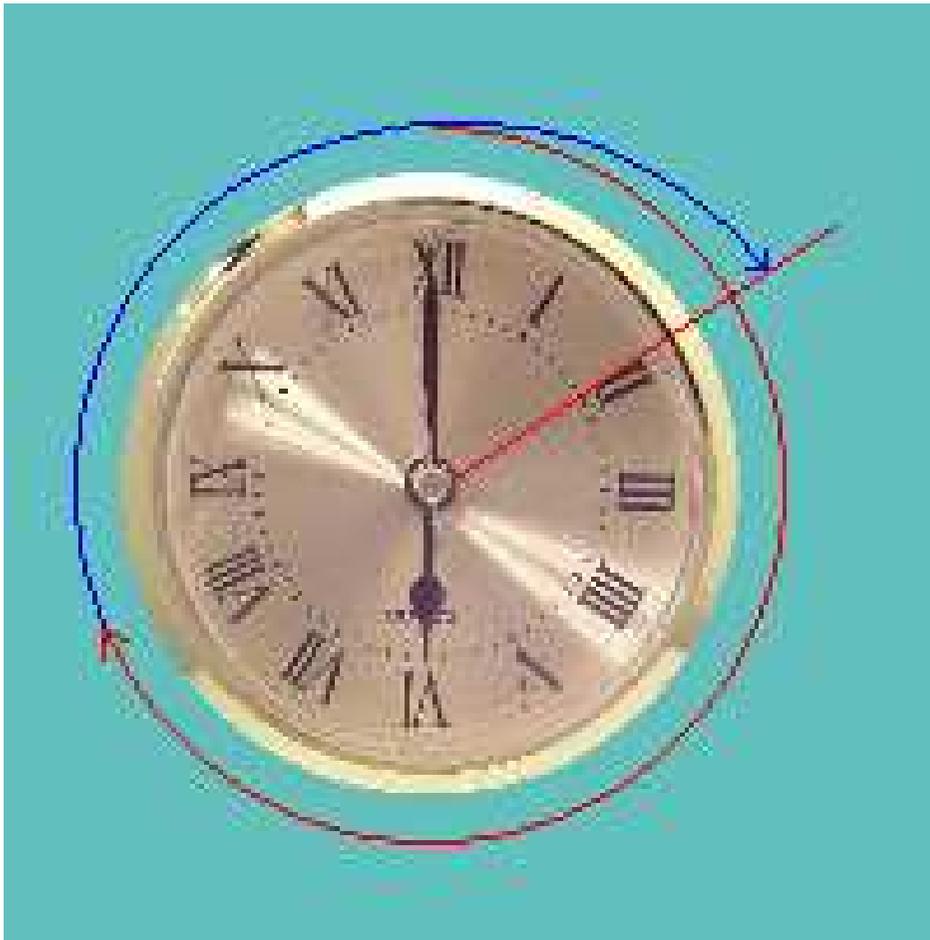
On additionne (ou multiplie) deux sacs, en effectuant l'opération sur un nombre au hasard de chaque sac, et en regardant dans quel sac se trouve le résultat.

# Une étrange façon de compter (2/4)

Addition et multiplication dans  $\mathbb{Z}/2$  :



# Une étrange façon de compter (3/4)



Une autre façon de voir : sur une horloge où les heures font  $N$  minutes, on oublie le nombre de tours (les heures) pour ne regarder que la grande aiguille.

$$40 + 30 \equiv 10 \pmod{60}$$

# Une étrange façon de compter (4/4)

---

Supposons maintenant qu'Anatole et Barnabé choisissent un grand  $N$  (200 chiffres), et font leurs calculs dans  $G = \mathbb{Z}/N$  :

$$g^a, \quad g^b, \quad A^b, \quad B^a$$

il n'y a que des multiplications ! On ne connaît pas de méthode raisonnable pour extraire de logarithmes.

Si on sait décomposer  $N$  en produit de nombres premiers et qu'on se donne un entier  $c$  (comme **chiffrer**), on sait calculer un entier  $d$  (comme **déchiffrer**) tel que

$$M^{cd} \equiv M \pmod{N}$$

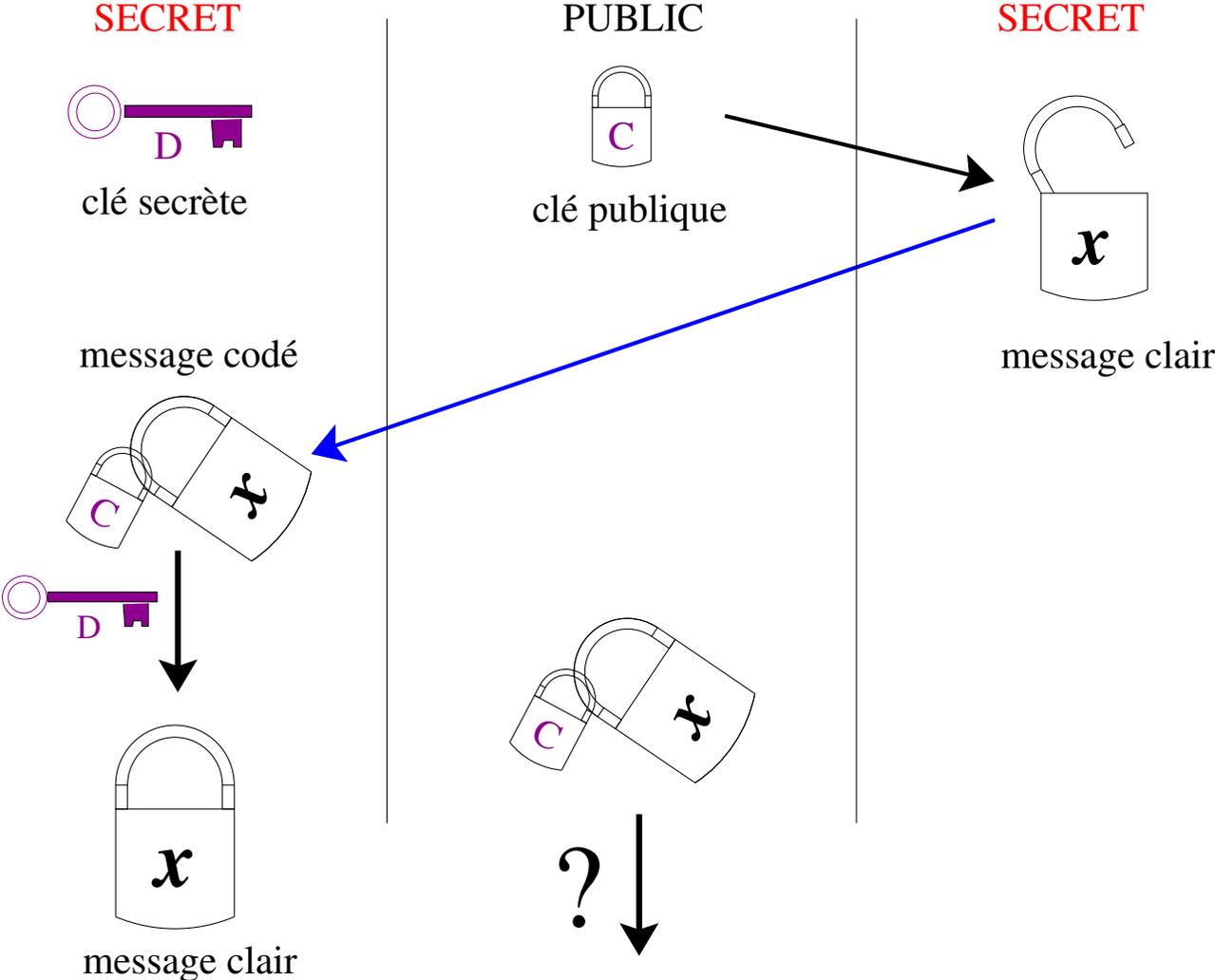
pour la plupart des sacs  $M$  (il faut supposer que  $\text{pgcd}(M, N) = 1$ ).

Actuellement, on ne sait pas calculer  $d$  à partir de  $(c, N)$  sans savoir factoriser le (grand) entier  $N$ .

Le chef du réseau Anatole, dévoile  $c$  et  $N$ , et garde  $d$  secret. Si  $M < N$  est un message à coder, n'importe qui peut écrire le message chiffré

$C \equiv M^c \pmod{N}$  puisque  $N$  et  $c$  sont publics. Pour le déchiffrer, Anatole calcule  $C^d \equiv M^{cd} \equiv M \pmod{N}$ . Mais comme on sait que  $0 \leq M < N$ , connaître le sac dans lequel tombe  $M$  suffit à le déterminer.

# Le système RSA (2/3)

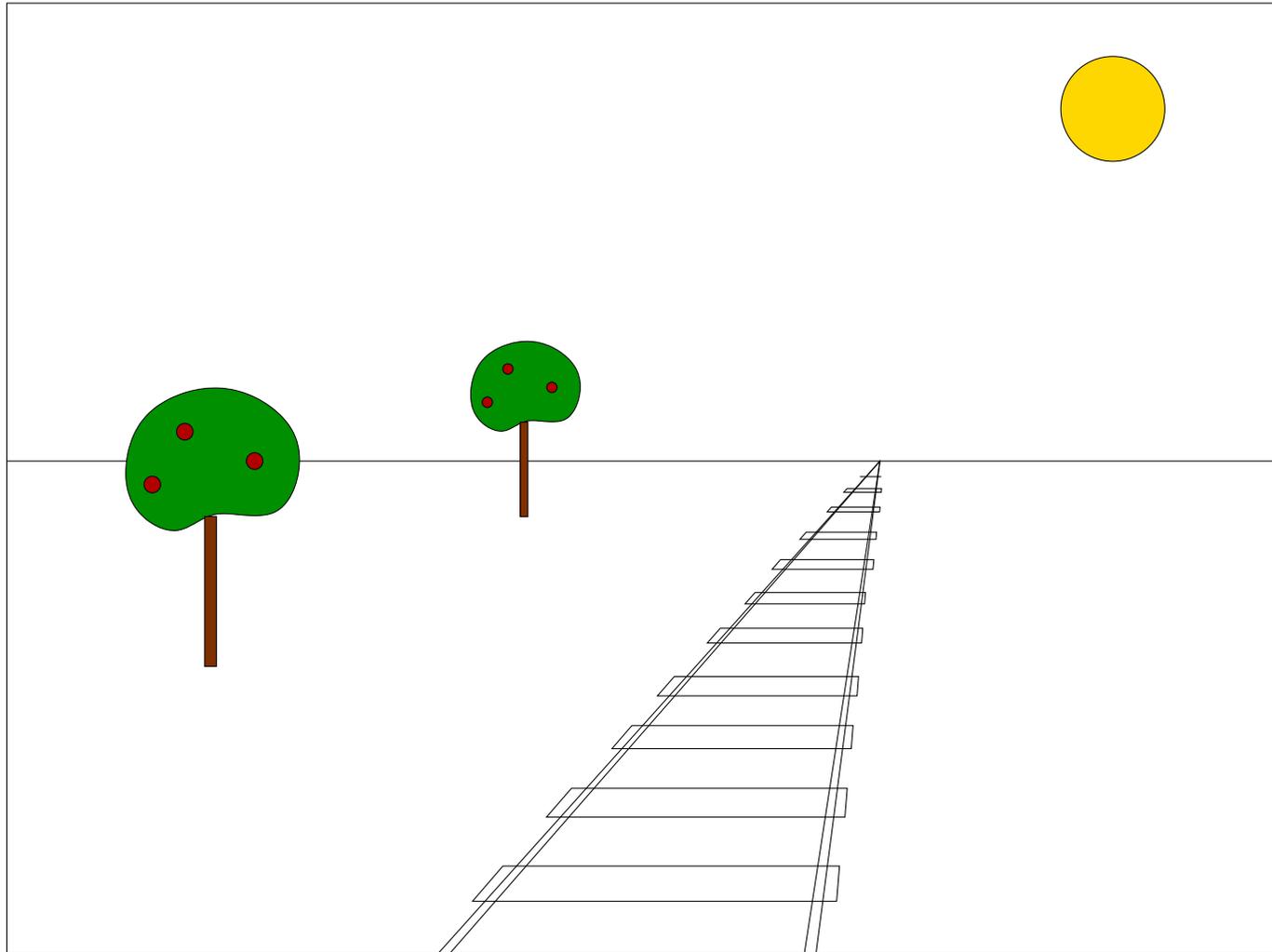


**Cryptographie clé publique : le système RSA (Rivest-Shamir-Adleman)**

Anatole peut aussi **signer** un message  $M$  sans le chiffrer, c'est-à-dire prouver qu'il connaît la clé secrète  $d$ ... sans la compromettre ! Il dévoile  $D \equiv M^d$  et n'importe qui peut calculer  $D^c \equiv M^{cd} \equiv M \pmod{N}$  à l'aide de la clé publique  $c$  et vérifier qu'il obtient bien un message intelligible.

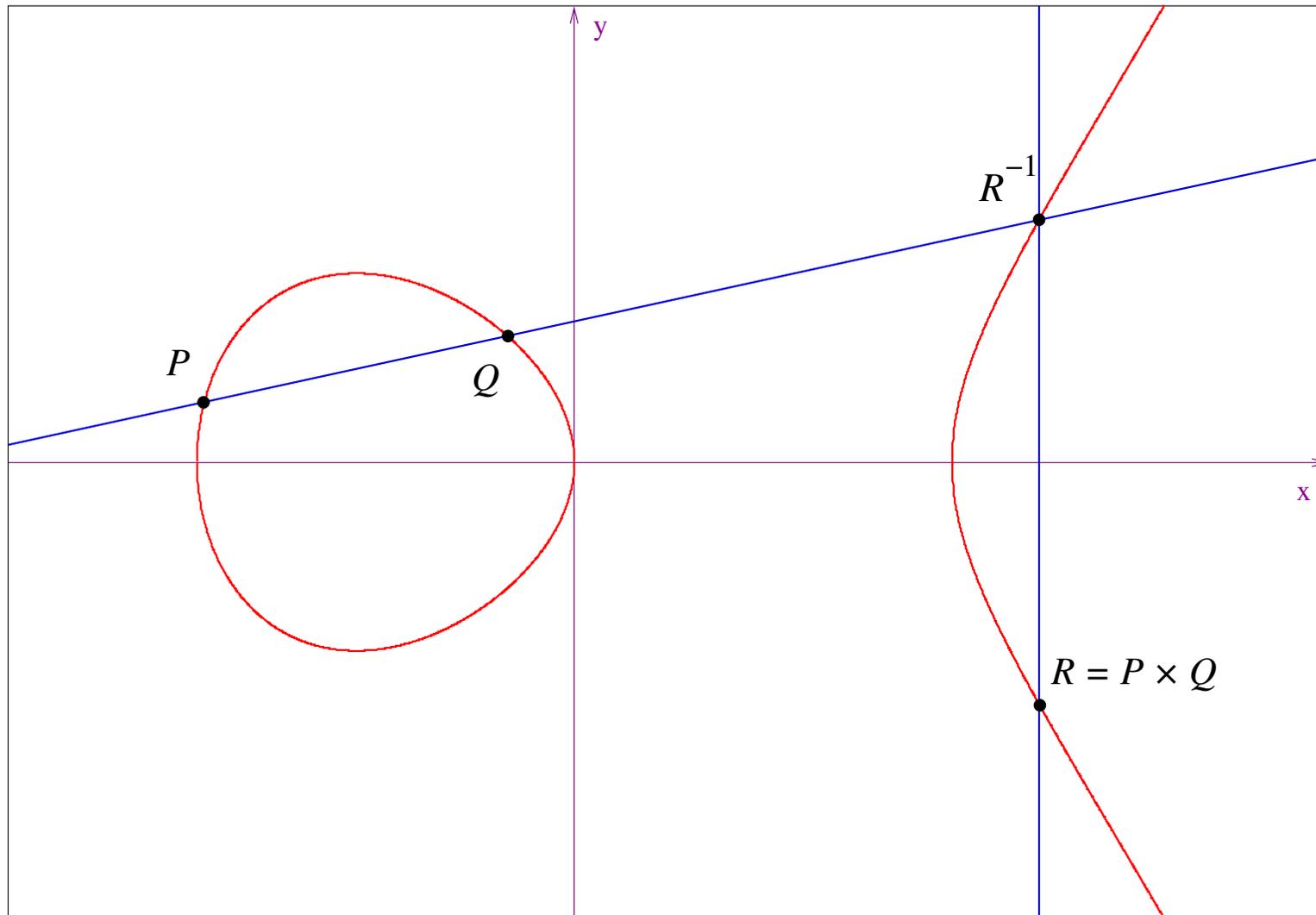
C'est exactement comme ça que le terminal du commerçant vérifie qu'une carte bleue est authentique : l'entier  $N$  (96 chiffres) est public, et la clé publique est  $c = 3$ . La carte contient un message de la forme  $D \equiv M^d$ , et le terminal de paiement vérifie que  $D^3$  est intelligible.

# Un autre groupe (1/3)



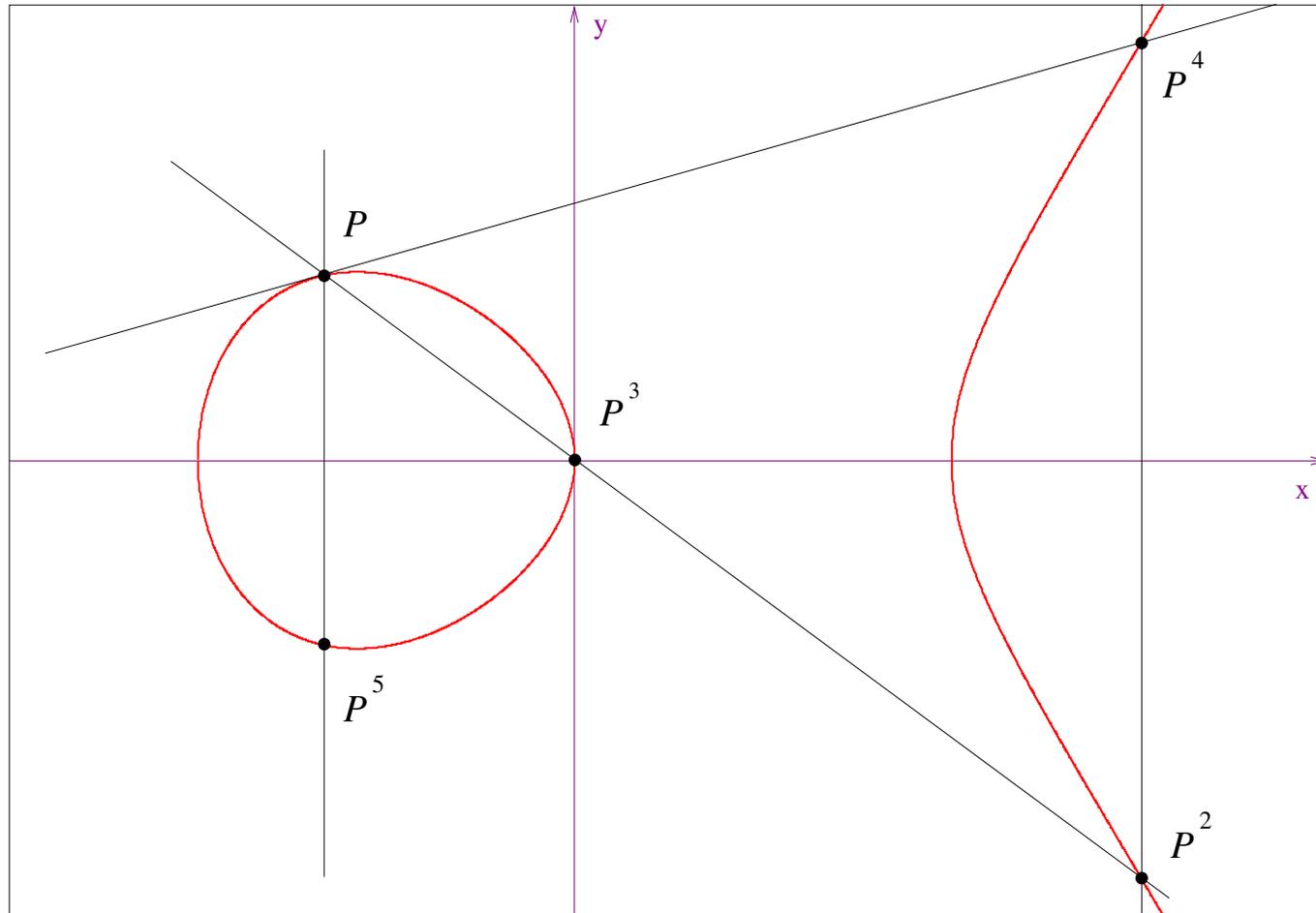
***Un point à l'infini (= une direction du plan)***

# Un autre groupe – multiplication (2/3)



**Multiplication sur la courbe elliptique**  $y^2 = x(x-1)(x+1)$

# Un autre groupe – puissances (3/3)



**Multiplication sur la courbe elliptique  $y^2 = x(x-1)(x+1)$**

On a  $P^6 = 1$ .