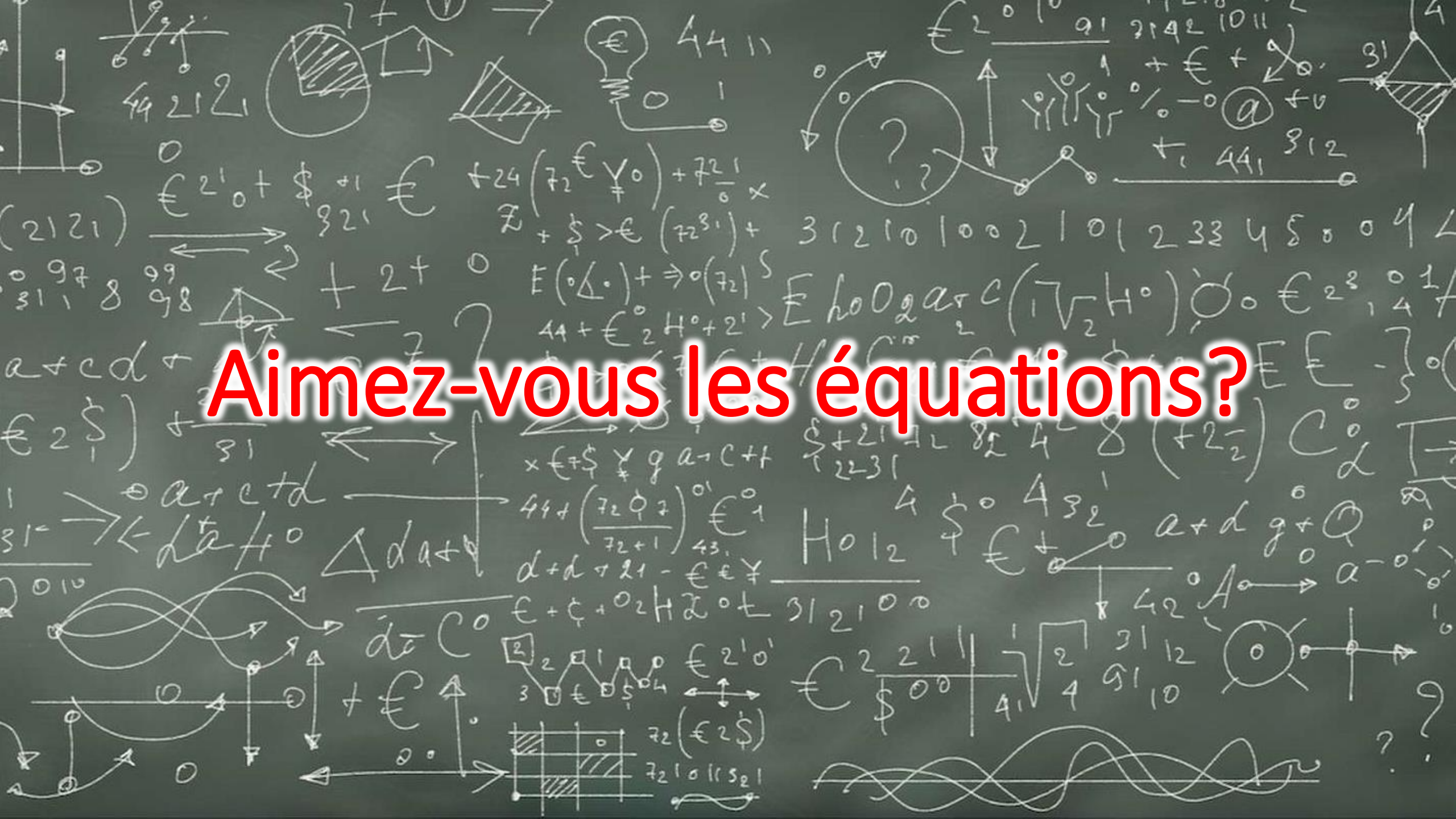
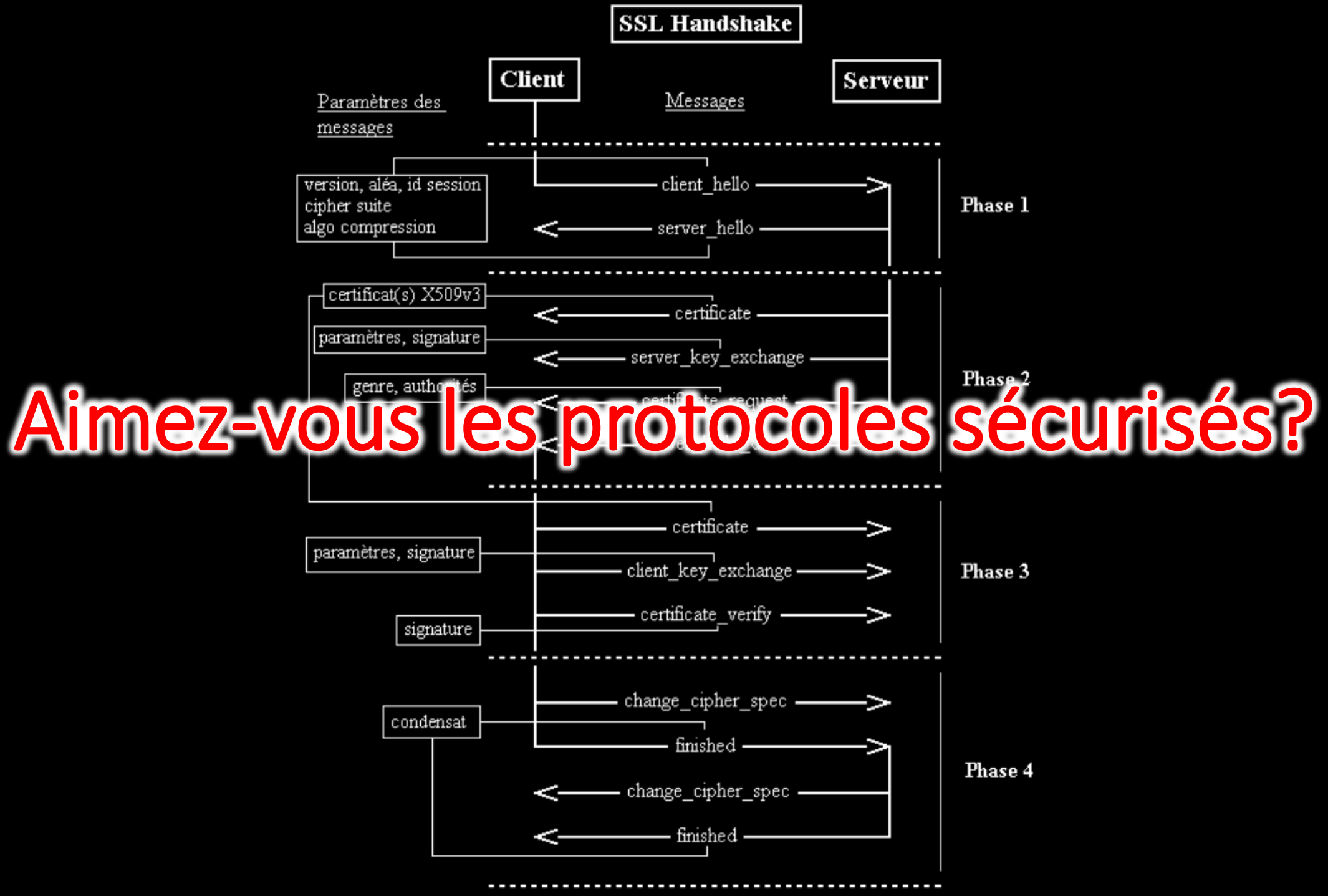
Cryptographie Asymétrique

Paul Dubois

pour

info@lèze


Aimez-vous les équations?

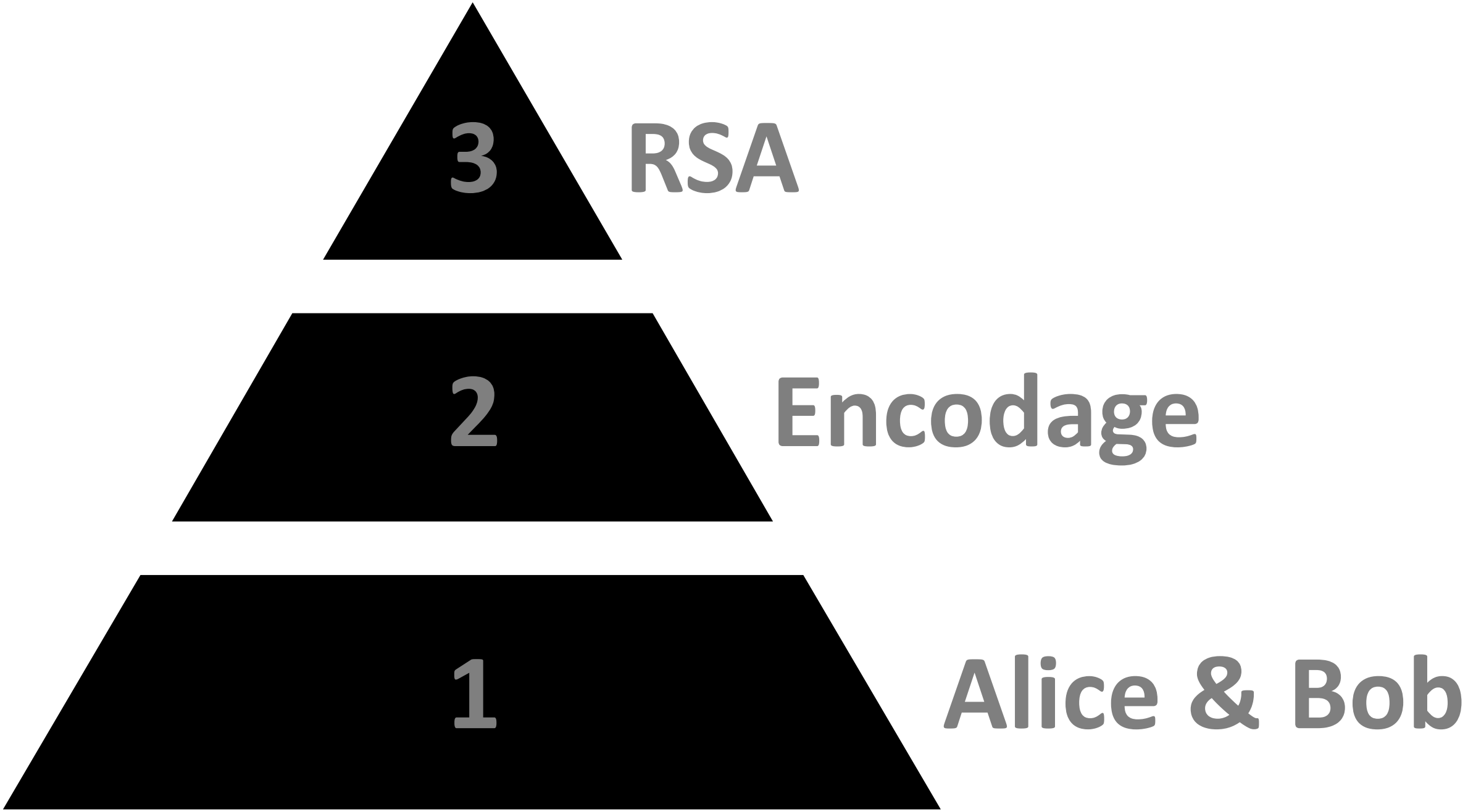


Aimez-vous les protocoles sécurisés?


Aimez-vous l’argent?


Aimez-vous Toulouse?

Comment faire passer un message secret…
… avec un haut-parleur?


3
RSA
2
Encodage
1
Alice & Bob

5 Courbes Elliptiques

4 ElGamal

3 RSA

2 Encodage

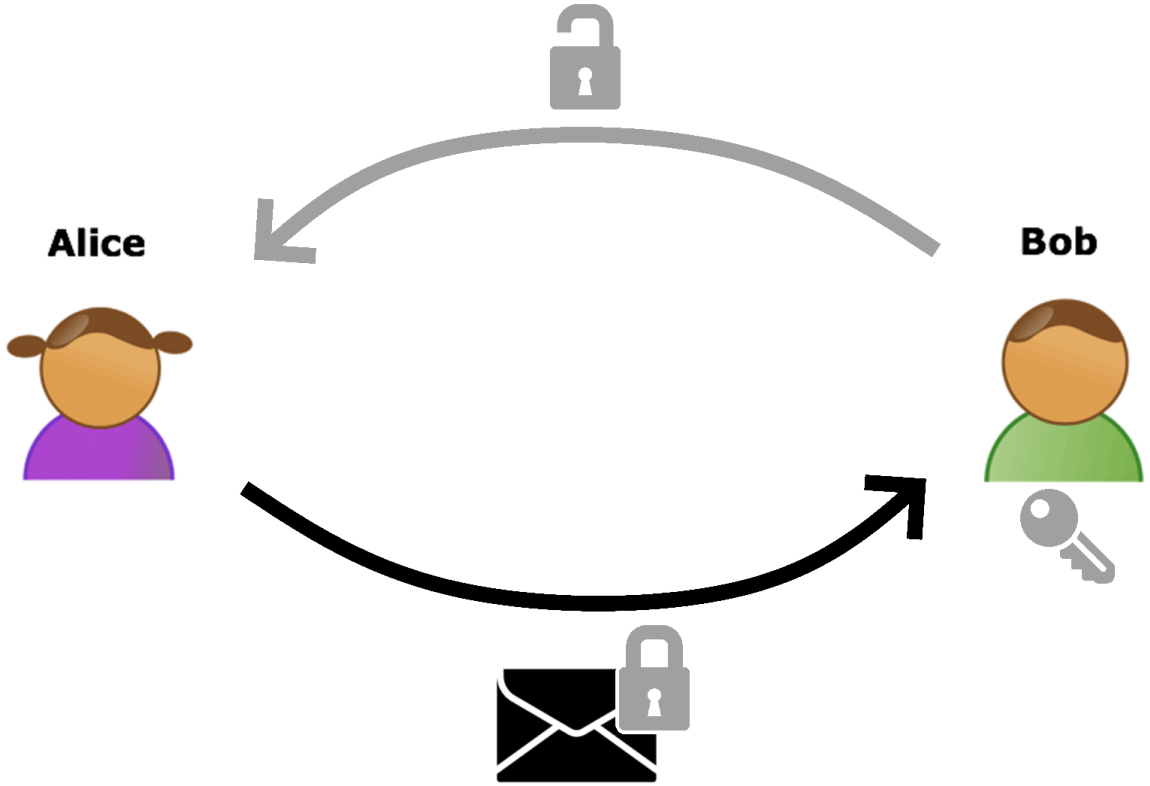
1 Alice & Bob

2ème Partie

1ère Partie

Niveau 1

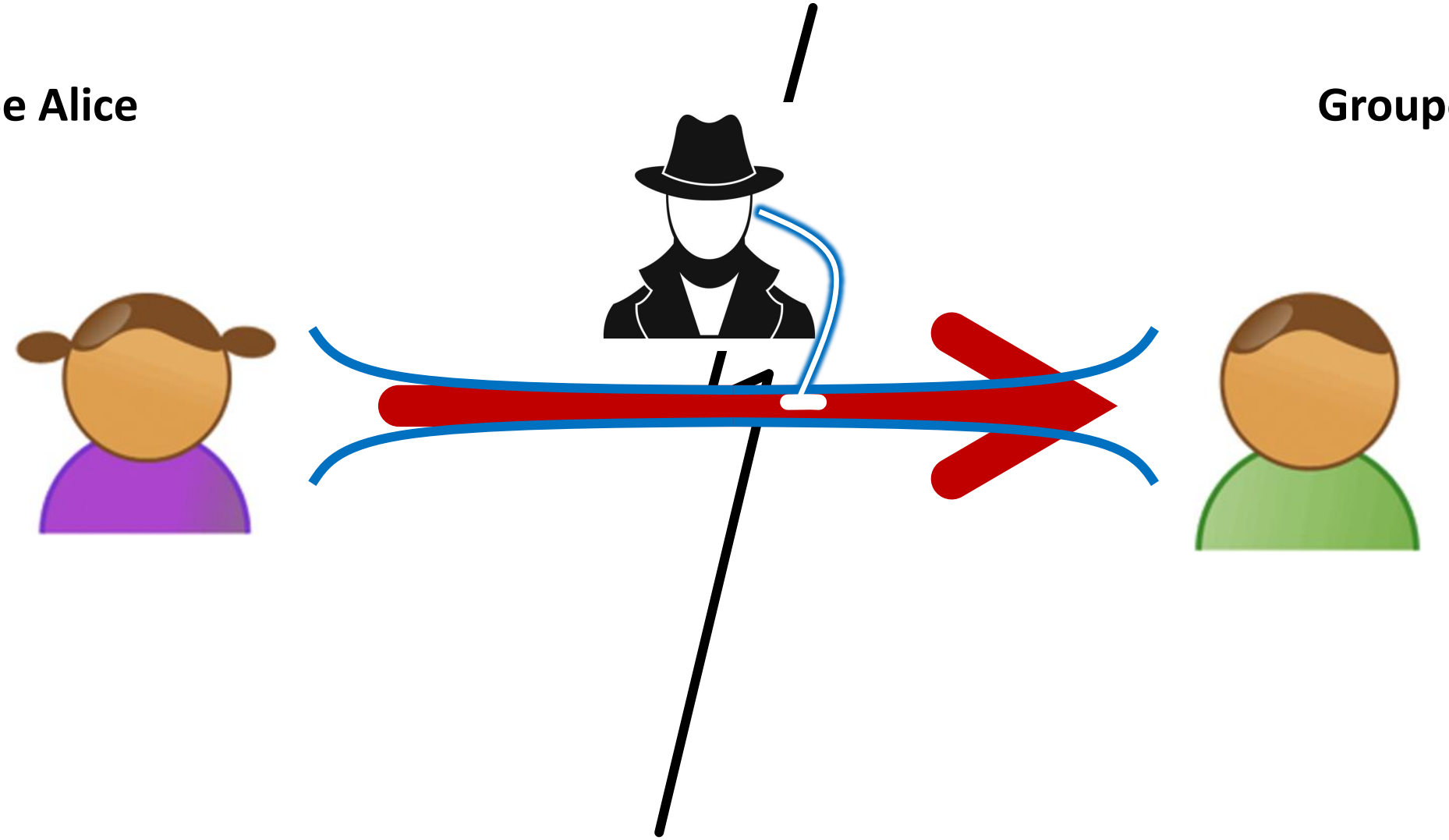
Analogie du cadenas



Envoyer un message sans connexion sécurisée

Groupe Alice

Groupe Bob

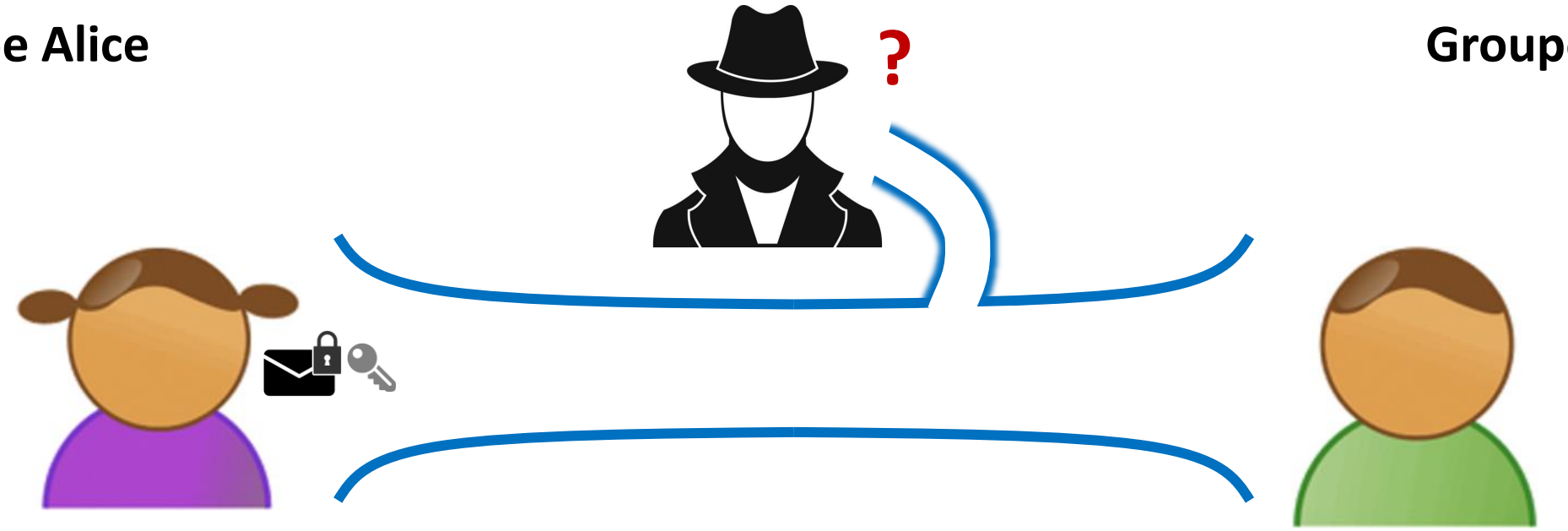


Do it yourself

Envoyer un message sans connexion sécurisée:

Intuition

Groupe Alice



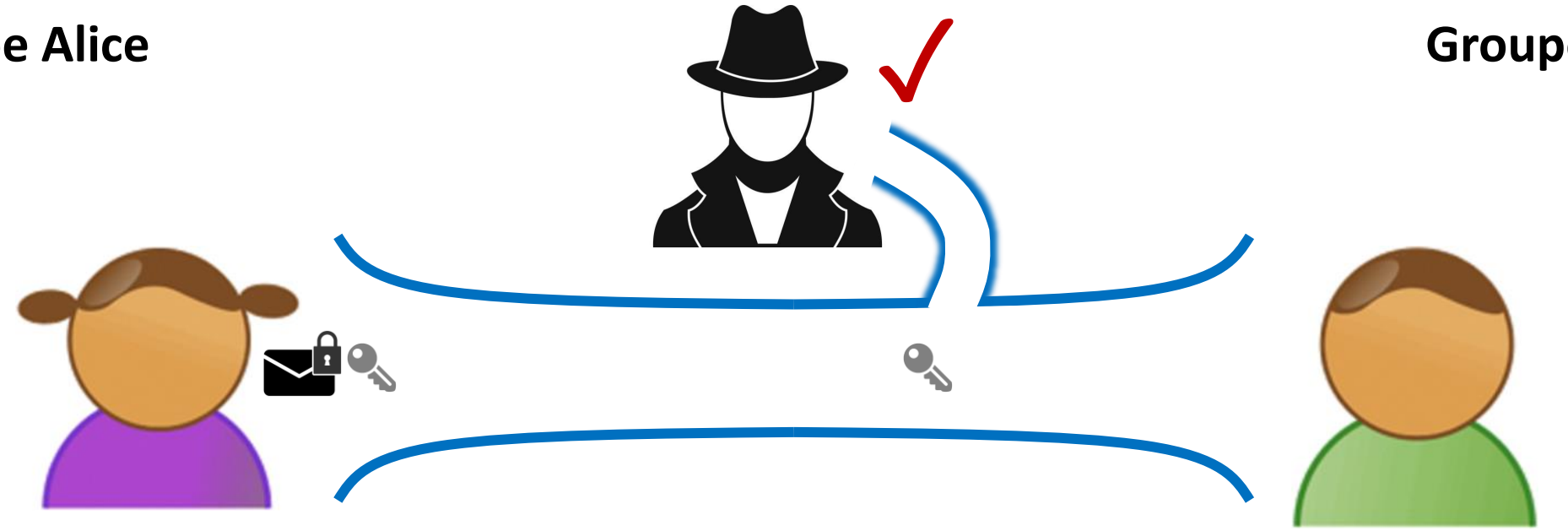
Groupe Bob

Envoyer un message sans connexion sécurisée:

Réalité

Groupe Alice

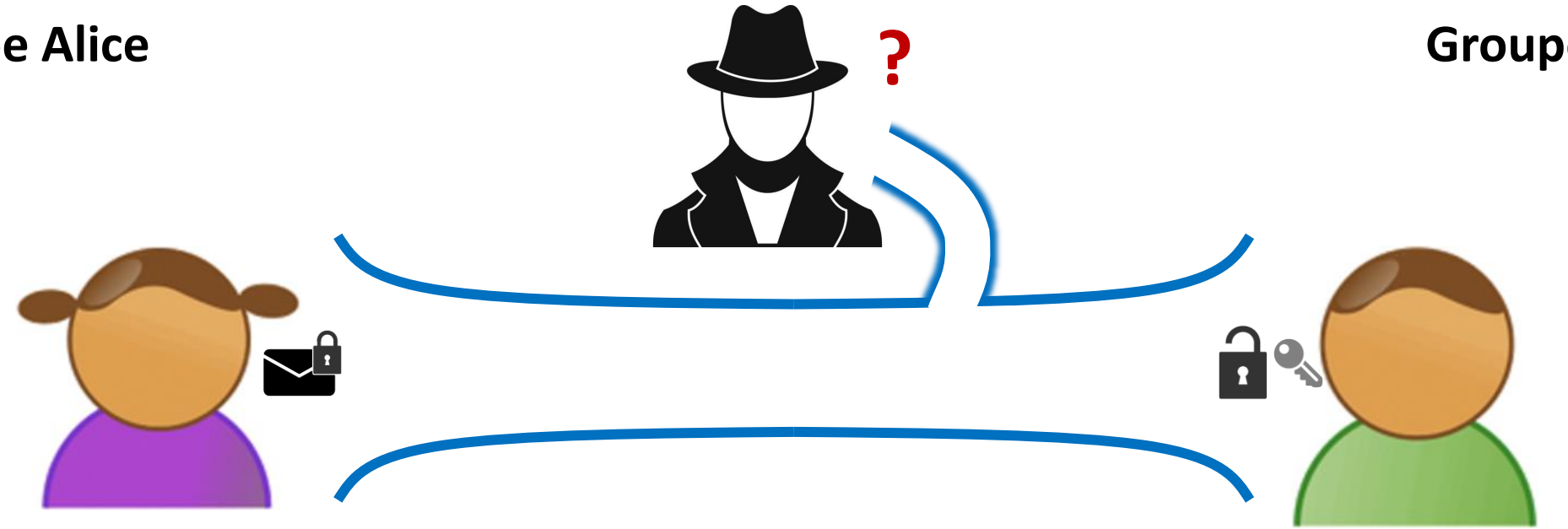
Groupe Bob



Envoyer un message sans connexion sécurisée:

Solution

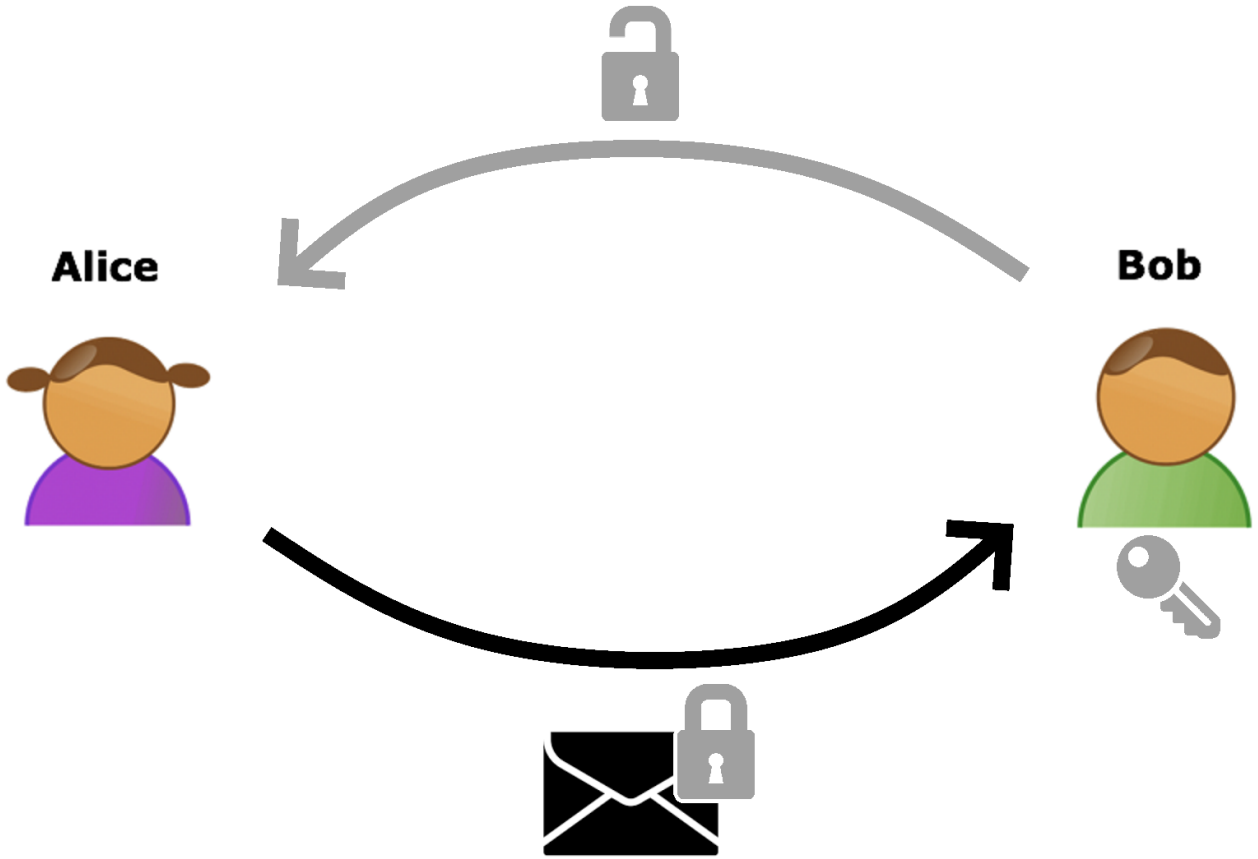
Groupe Alice



Groupe Bob

Envoyer un message sans connexion sécurisée:

Synthèse



Niveau 2

Encodage d’un message en numérique

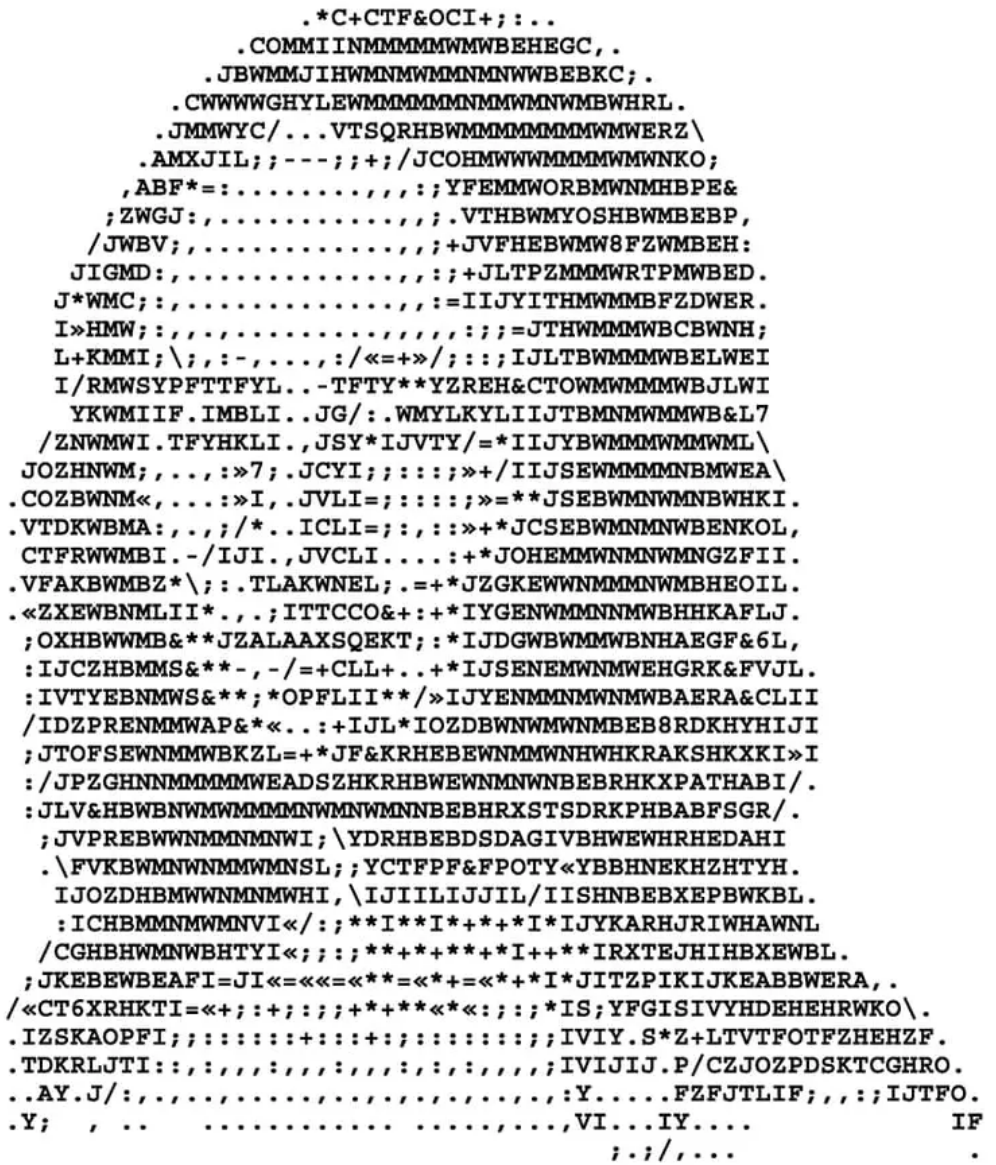


Photo non-contractuelle

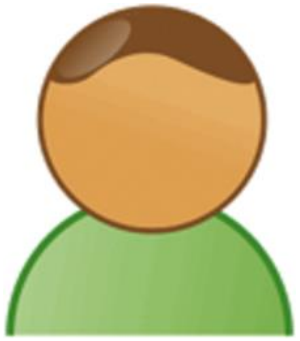
Coder un message

Groupe Alice

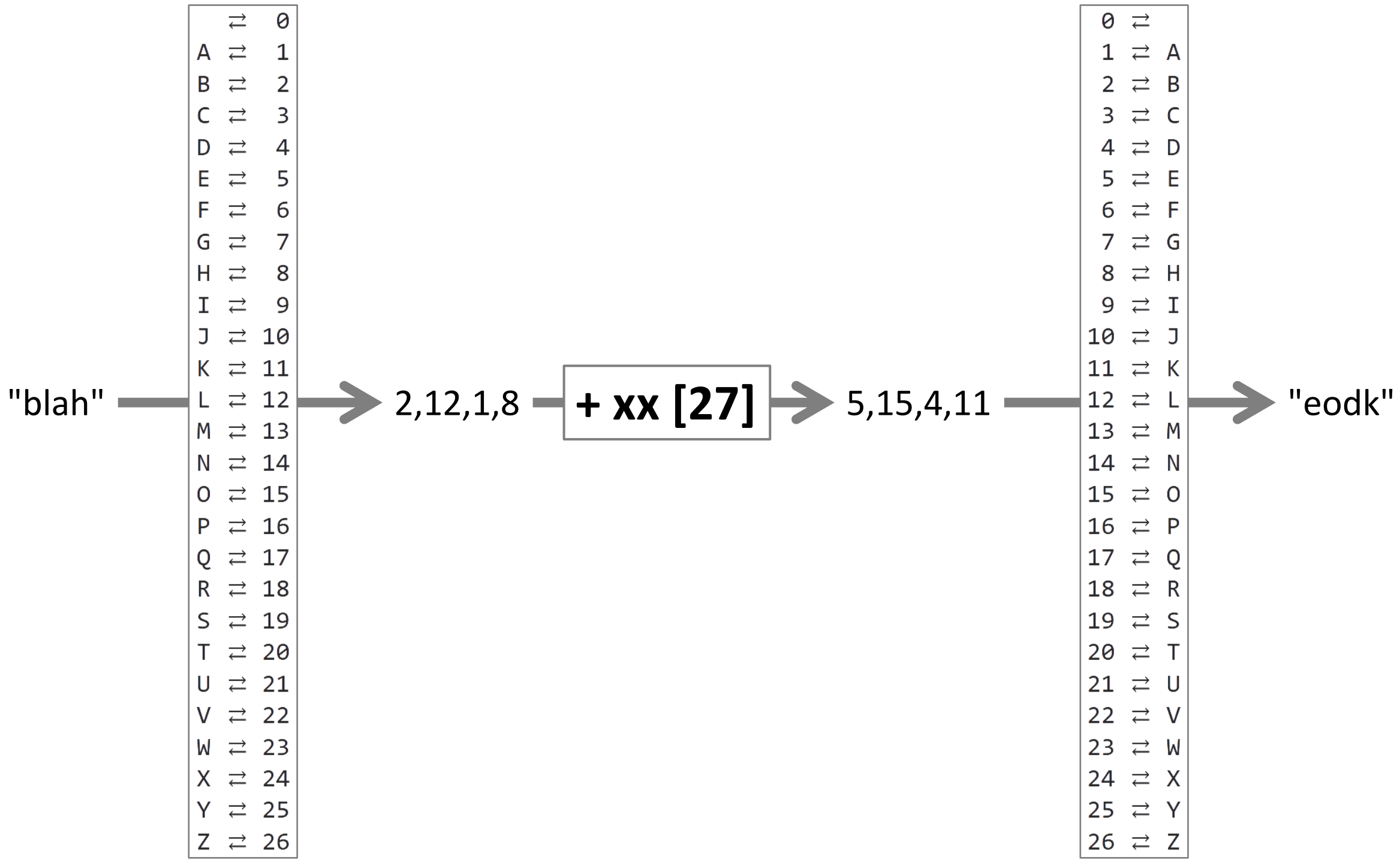
Groupe Bob

Code: ???

Code: xxx



Code: xxx

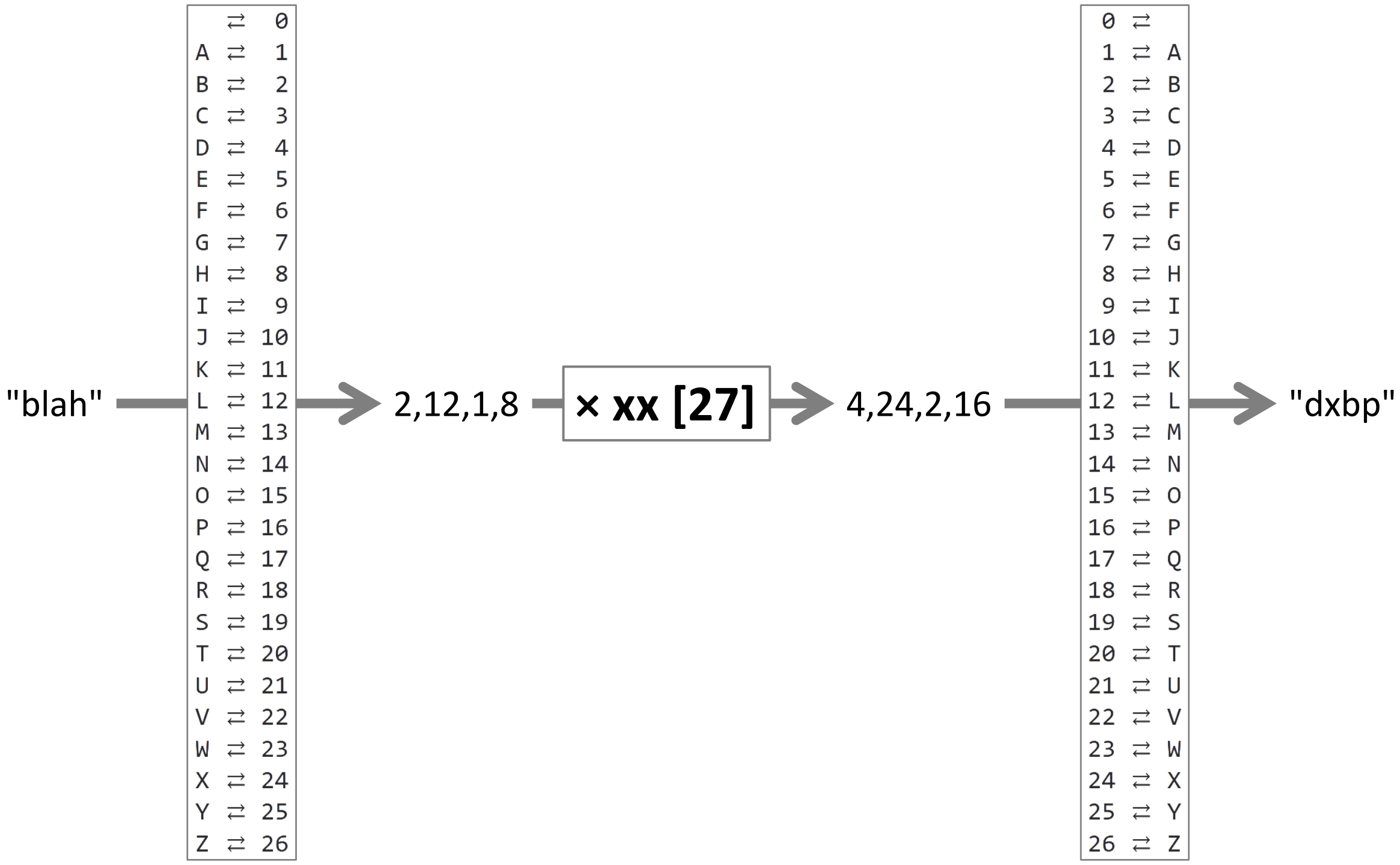

"blah"
2,12,1,8
+ xx [27]
5,15,4,11
"eodk"
A ⇄ 1
B ⇄ 2
C ⇄ 3
D ⇄ 4
E ⇄ 5
F ⇄ 6
G ⇄ 7
H ⇄ 8
I ⇄ 9
J ⇄ 10
K ⇄ 11
L ⇄ 12
M ⇄ 13
N ⇄ 14
O ⇄ 15
P ⇄ 16
Q ⇄ 17
R ⇄ 18
S ⇄ 19
T ⇄ 20
U ⇄ 21
V ⇄ 22
W ⇄ 23
X ⇄ 24
Y ⇄ 25
Z ⇄ 26
1 ⇄ A
2 ⇄ B
3 ⇄ C
4 ⇄ D
5 ⇄ E
6 ⇄ F
7 ⇄ G
8 ⇄ H
9 ⇄ I
10 ⇄ J
11 ⇄ K
12 ⇄ L
13 ⇄ M
14 ⇄ N
15 ⇄ O
16 ⇄ P
17 ⇄ Q
18 ⇄ R
19 ⇄ S
20 ⇄ T
21 ⇄ U
22 ⇄ V
23 ⇄ W
24 ⇄ X
25 ⇄ Y
26 ⇄ Z

Représentation de l’encodage

(addition)

https://pauldubois98.github.io/AsymmetricCryptographyTalk/tools/code_add.html

Do it yourself


"blah"
2,12,1,8
× xx [27]
4,24,2,16
"dxbp"
⇄ 0
A ⇄ 1
B ⇄ 2
C ⇄ 3
D ⇄ 4
E ⇄ 5
F ⇄ 6
G ⇄ 7
H ⇄ 8
I ⇄ 9
J ⇄ 10
K ⇄ 11
L ⇄ 12
M ⇄ 13
N ⇄ 14
O ⇄ 15
P ⇄ 16
Q ⇄ 17
R ⇄ 18
S ⇄ 19
T ⇄ 20
U ⇄ 21
V ⇄ 22
W ⇄ 23
X ⇄ 24
Y ⇄ 25
Z ⇄ 26
0 ⇄
1 ⇄ A
2 ⇄ B
3 ⇄ C
4 ⇄ D
5 ⇄ E
6 ⇄ F
7 ⇄ G
8 ⇄ H
9 ⇄ I
10 ⇄ J
11 ⇄ K
12 ⇄ L
13 ⇄ M
14 ⇄ N
15 ⇄ O
16 ⇄ P
17 ⇄ Q
18 ⇄ R
19 ⇄ S
20 ⇄ T
21 ⇄ U
22 ⇄ V
23 ⇄ W
24 ⇄ X
25 ⇄ Y
26 ⇄ Z

Représentation de l’encodage

(multiplication)

https://pauldubois98.github.io/AsymmetricCryptographyTalk/tools/code_mult.html

Principales conclusions

- **Représentation** de l'alphabet par des **nombre**
- **Modulo** pour que la plage de nombre utilisé reste petite
- Code par **multiplication** plus complexe que par addition
- Chiffrement **symétrique**

« + » :

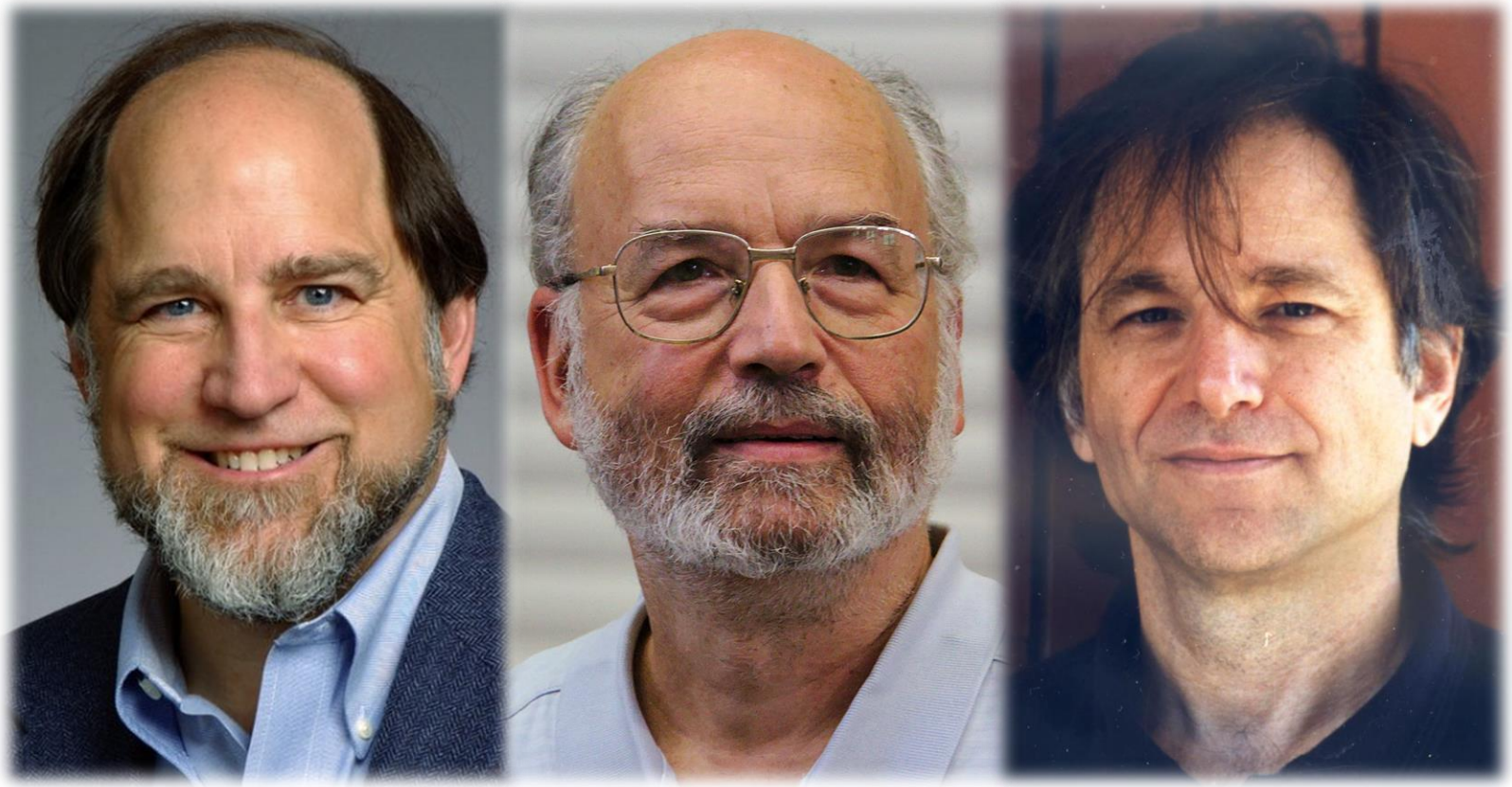
- **Peu couteux** en terme de calculs

« - » :

- Besoin d'une clef de **code inconnue par l'espion**

Niveau 3

Chiffrement RSA



*Ronald **R**ivest* *Adi **S**hamir* *Leonard **A**dleman*

Un nombre premier, késaco?

« un nombre qu'on ne peut pas factoriser »

$6 = 2 * 3$ ✗

$7 = 1 * 7$ ✓ Trivial !

11 ✓ 12 ✗ 35 ✗

Communiquer par l’intermédiaire d’un espion

(sans clef privée)

m, le message

$c = m^e [n]$

(n, e)

c

p,q premiers

$n = pq$

$\varphi(n) = (p - 1)(q - 1)$

e tel que:

- $e < \varphi(n)$
- $pgcd(e, \varphi(n)) = 1$

$d = e^{-1}[\varphi(n)]$

$m = c^d\ [n]$

« petit théorème de Fermat »

RSA Helper

https://pauldubois98.github.io/AsymmetricCryptographyTalk/tools/rsa_helper.html

Do it yourself

m, le message

$c = m^e[n]$

(n, e)

c

p,q premiers

$n = pq$

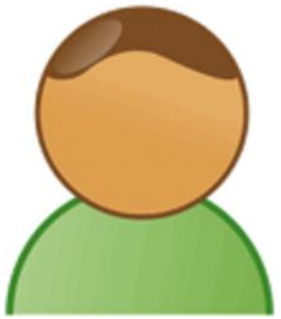
$\varphi(n) = (p - 1)(q - 1)$

e tel que:

- $e < \varphi(n)$
- $pgcd(e, \varphi(n)) = 1$

$d = e^{-1}[\varphi(n)]$

$m = c^d\ [n]$



Principales conclusions

- L'espion est **bloqué** par la **factorisation** de n en p et q
- Alors que la **multiplication** $p * q = n$ est **rapide**
- Besoin de **générer des nombres premier** (p et q) **très grand**
- Chiffrement **asymétrique**

« + »:

- **Pas** besoin d'une clef de **code inconnue par l'espion**

« - »:

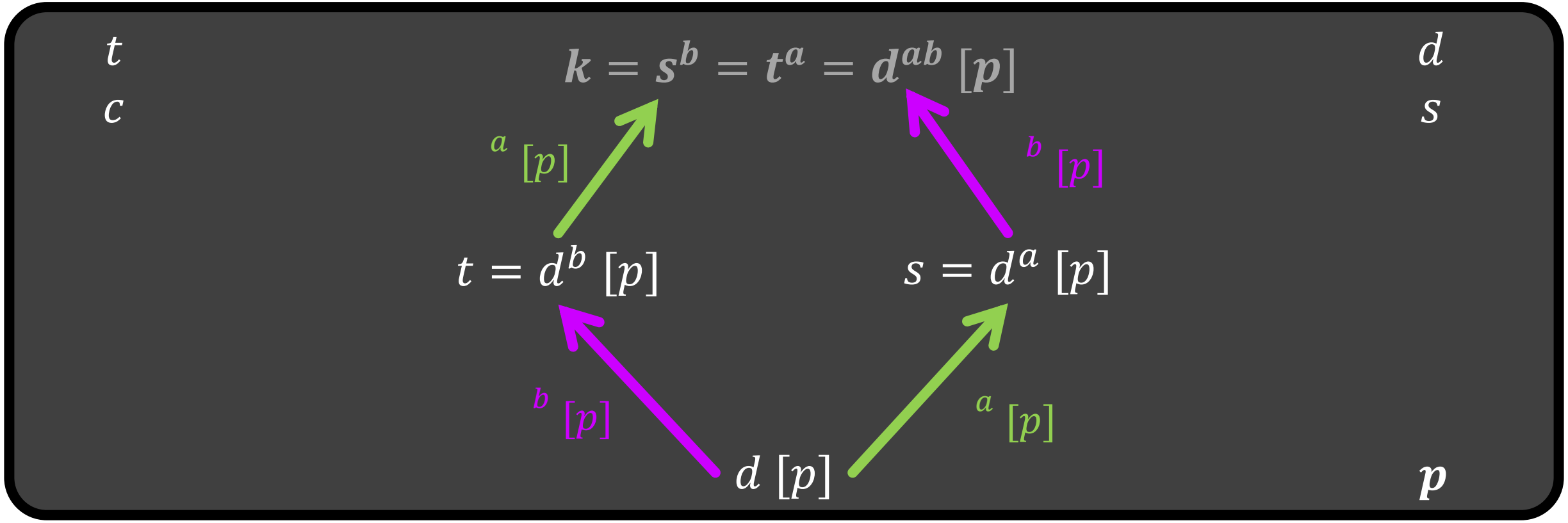
- **Assez couteux** en terme de calculs
- Sujet aux **attaques par ordinateurs quantiques**

$\Rightarrow$ Echange de clef de chiffrement symétrique

Niveau 4

Chiffrement ElGamal

ElGamal



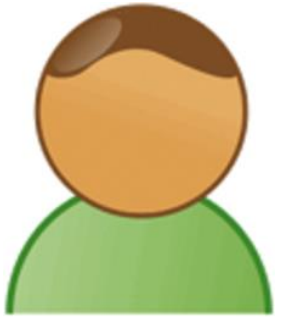
b

m

$t = d^b$ [p]

$k = s^b$ [p]

$c = mk$ [p]



p, a, d

$s = d^a$ [p]

$k = t^a$ [p]

$u = k^{-1}$[p]

$m = cu$ [p]

Logarithme modulaire

$$s = d^{a}\ [p]$$

$$s = d^{a}$$

$$\log(s) = \log(d^{a})$$

$$= a * \log(d)$$

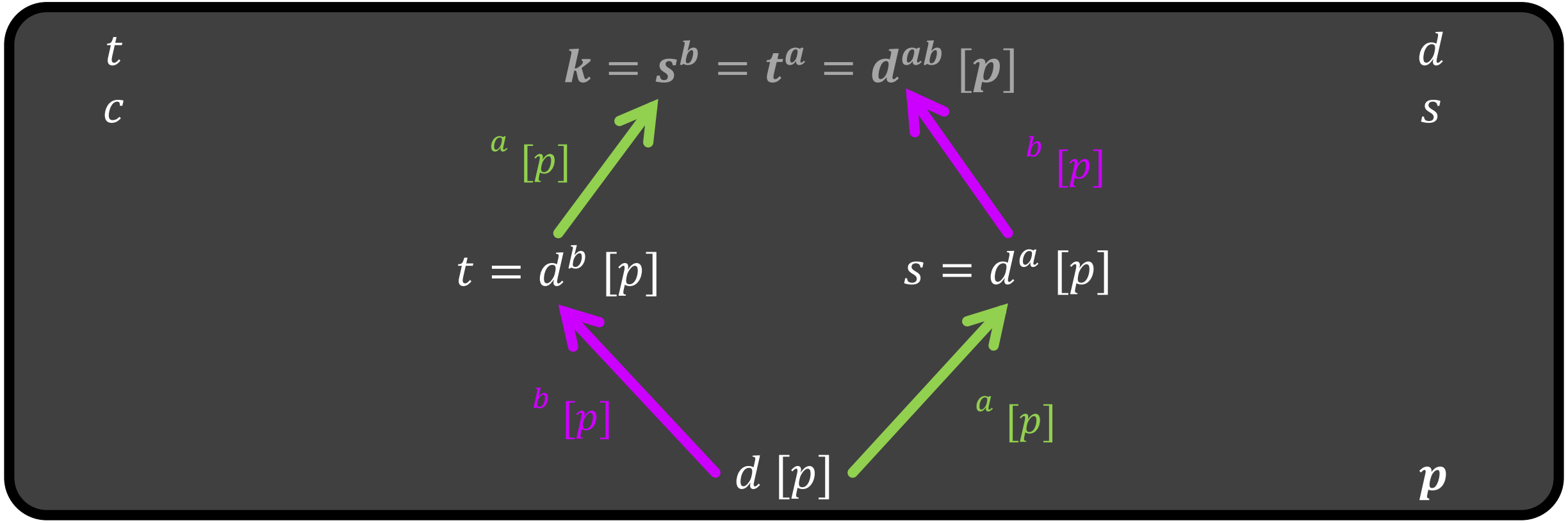
$$a = \frac{\log(s)}{\log(d)}$$

$$= \log(s - d)$$

Calculatrice Modulaire

https://pauldubois98.github.io/AsymmetricCryptographyTalk/tools/mod_calculator.html

Do it yourself



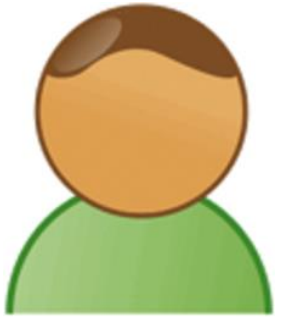
b

m

$t = d^b$ [p]

$k = s^b$ [p]

$c = mk$ [p]



p, a, d

$s = d^a$ [p]

$k = t^a$ [p]

$u = k^{-1}$[p]

$m = cu$ [p]

Principales conclusions

- L'espion est **bloqué** par l'impossibilité de **calculer $\boldsymbol{k}$** (à partir des info publiques) & de trouver a ou b (logarithme modulaire).
- Chiffrement **symétrique**

« + »:

- **Pas** besoin d'une clef de **code inconnue par l'espion**

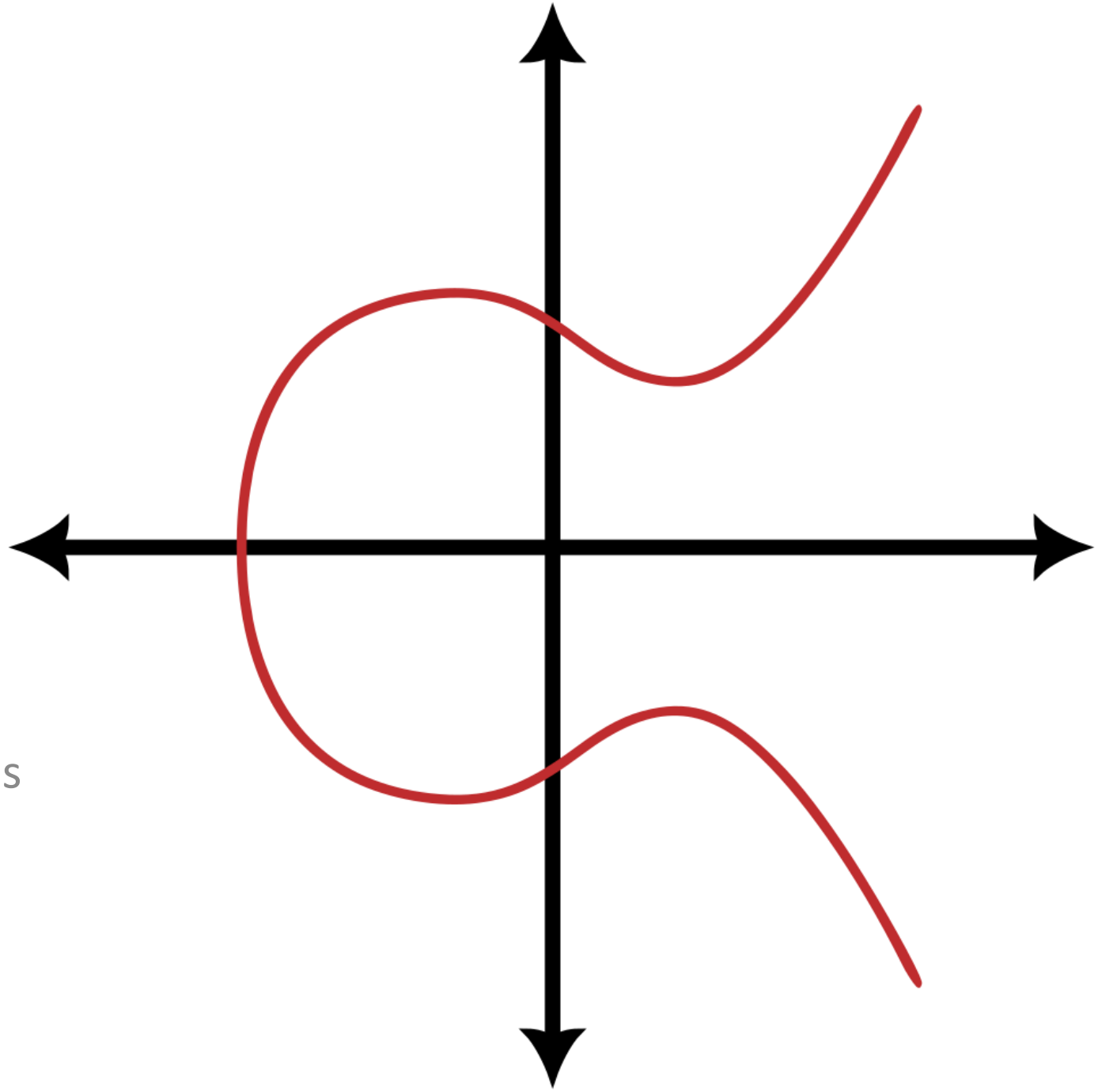
« - »:

- **Assez couteux** en terme de calculs
- Sujet a certaines **attaques algébrique** (complexe) permettant d'**altérer** le **message**

$\Rightarrow$ Le principe peut être réutiliser dans un autre contexte

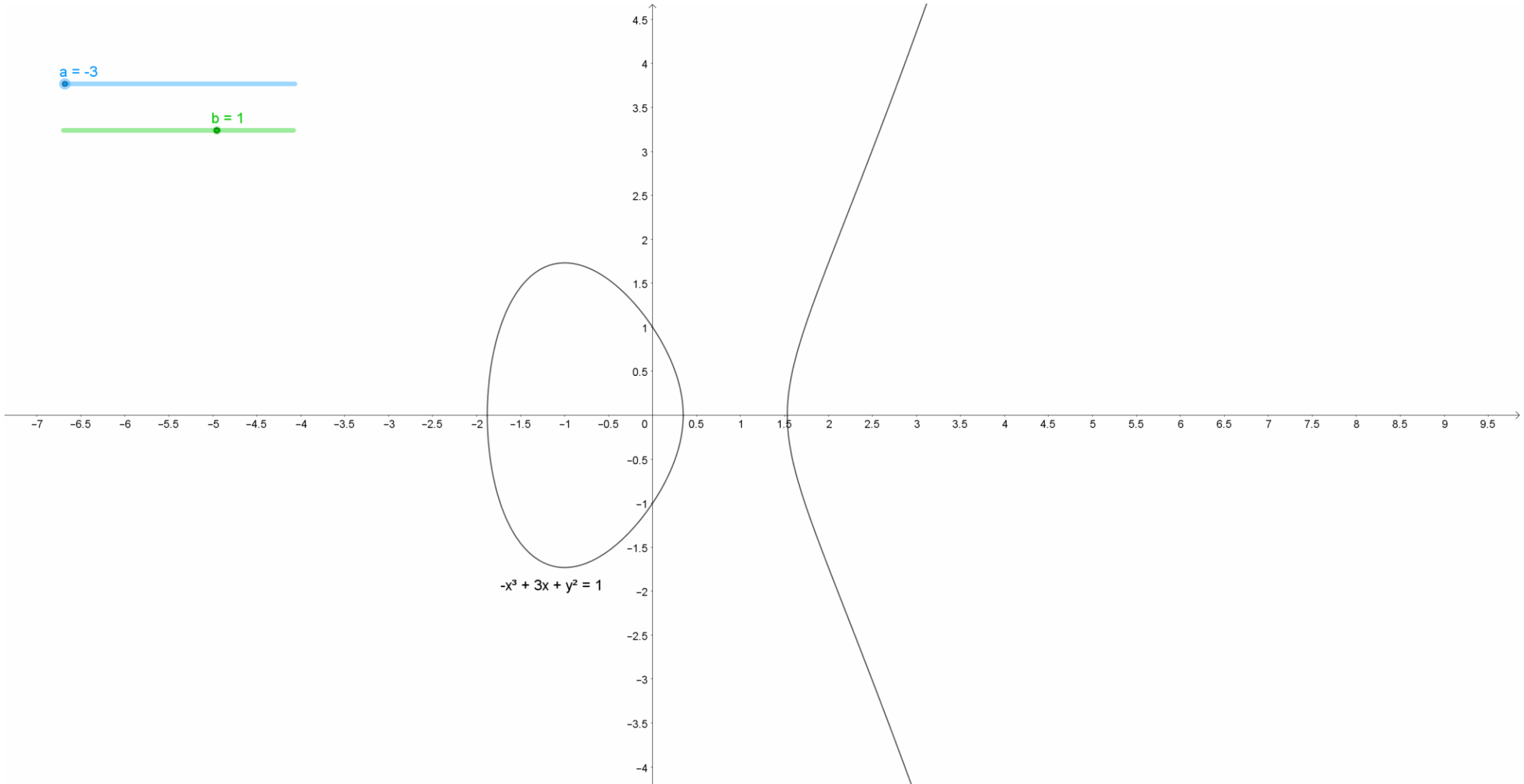
Niveau 5

Cryptographie sur Courbes Elliptiques



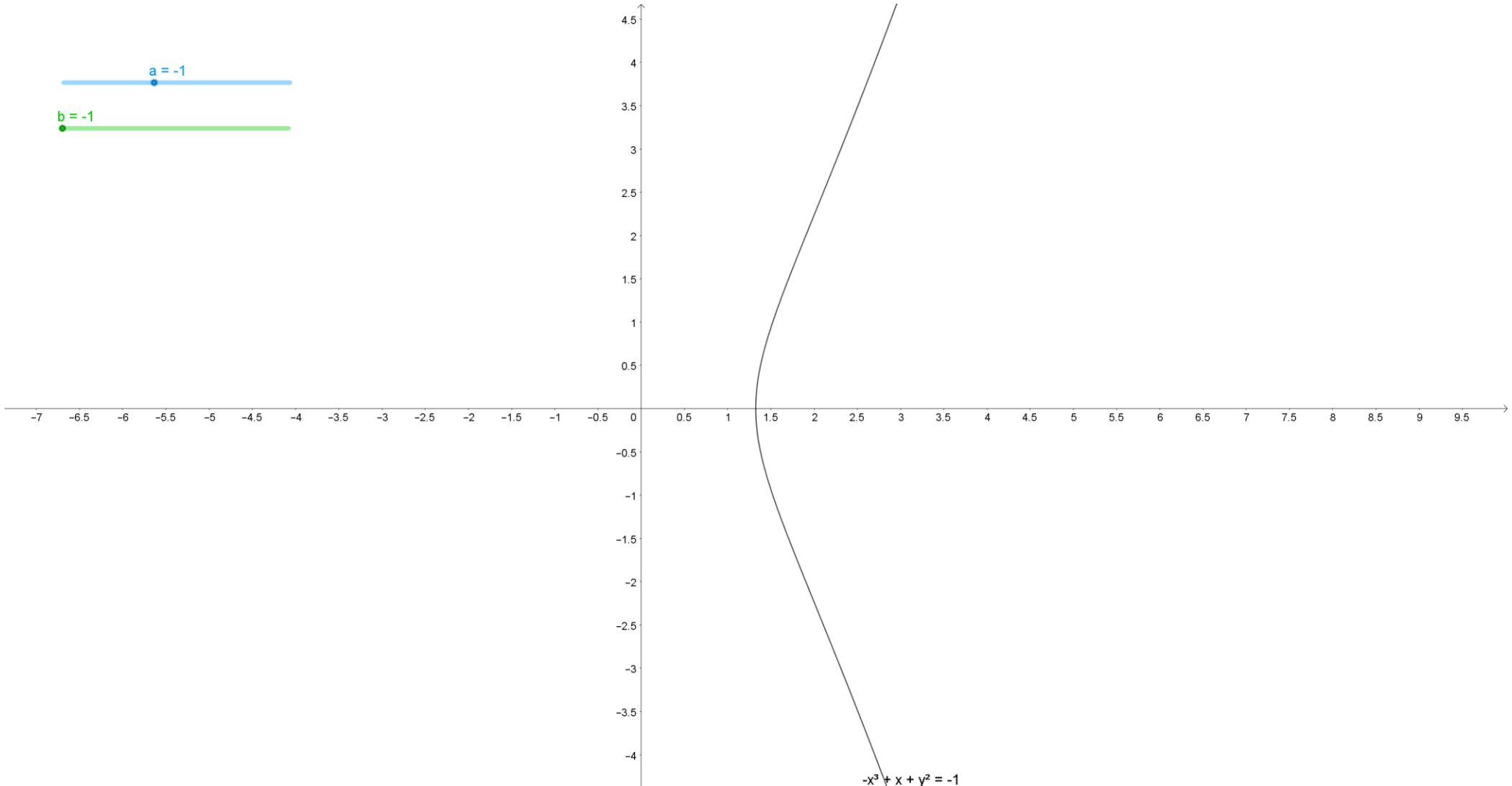
Une courbe elliptique, késaco?

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



Une courbe elliptique, késaco?

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



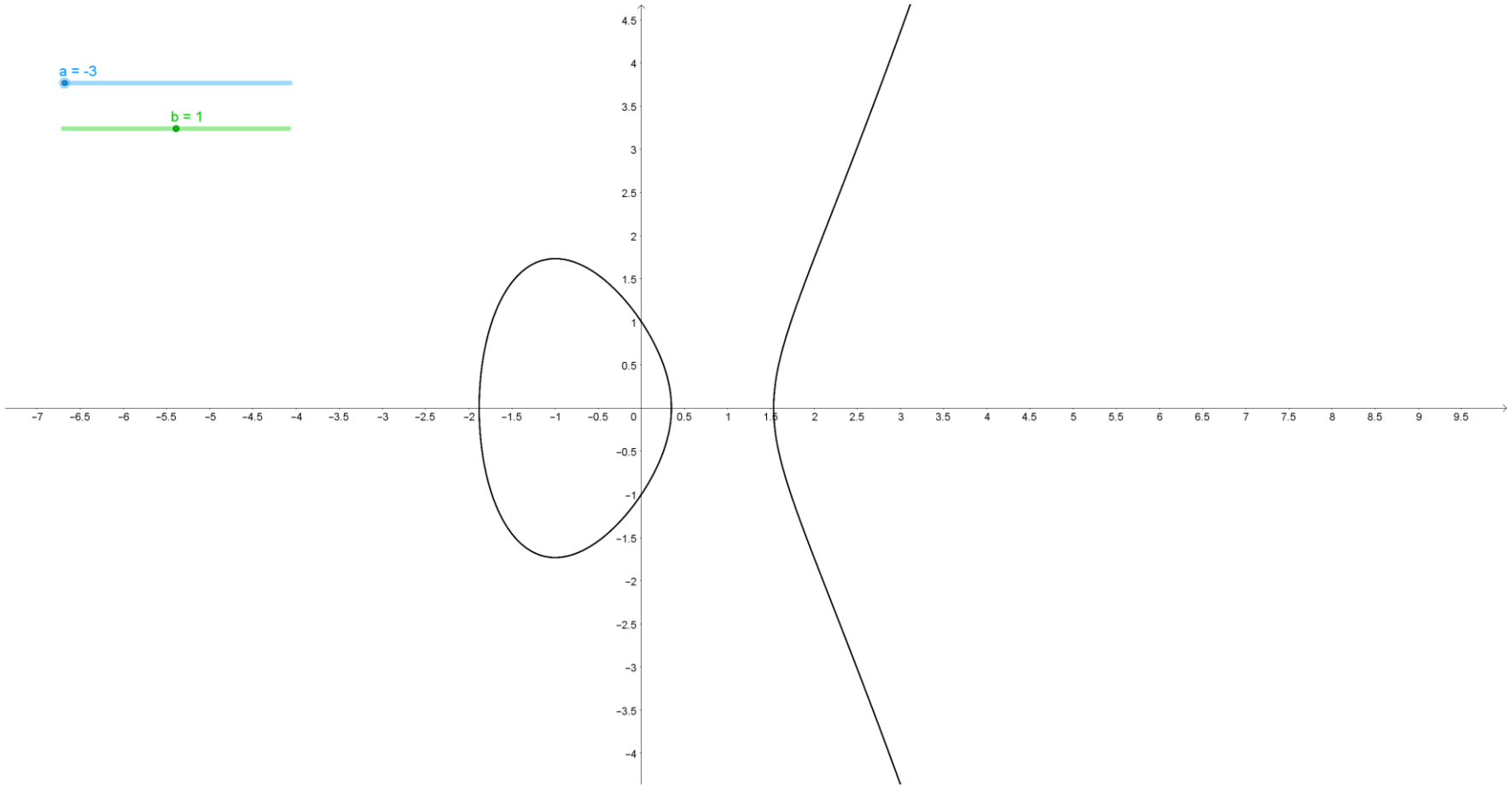
Une courbe elliptique, késaco?

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

https://pauldubois98.github.io/AsymmetricCryptographyTalk/tools/elliptic_curve.html

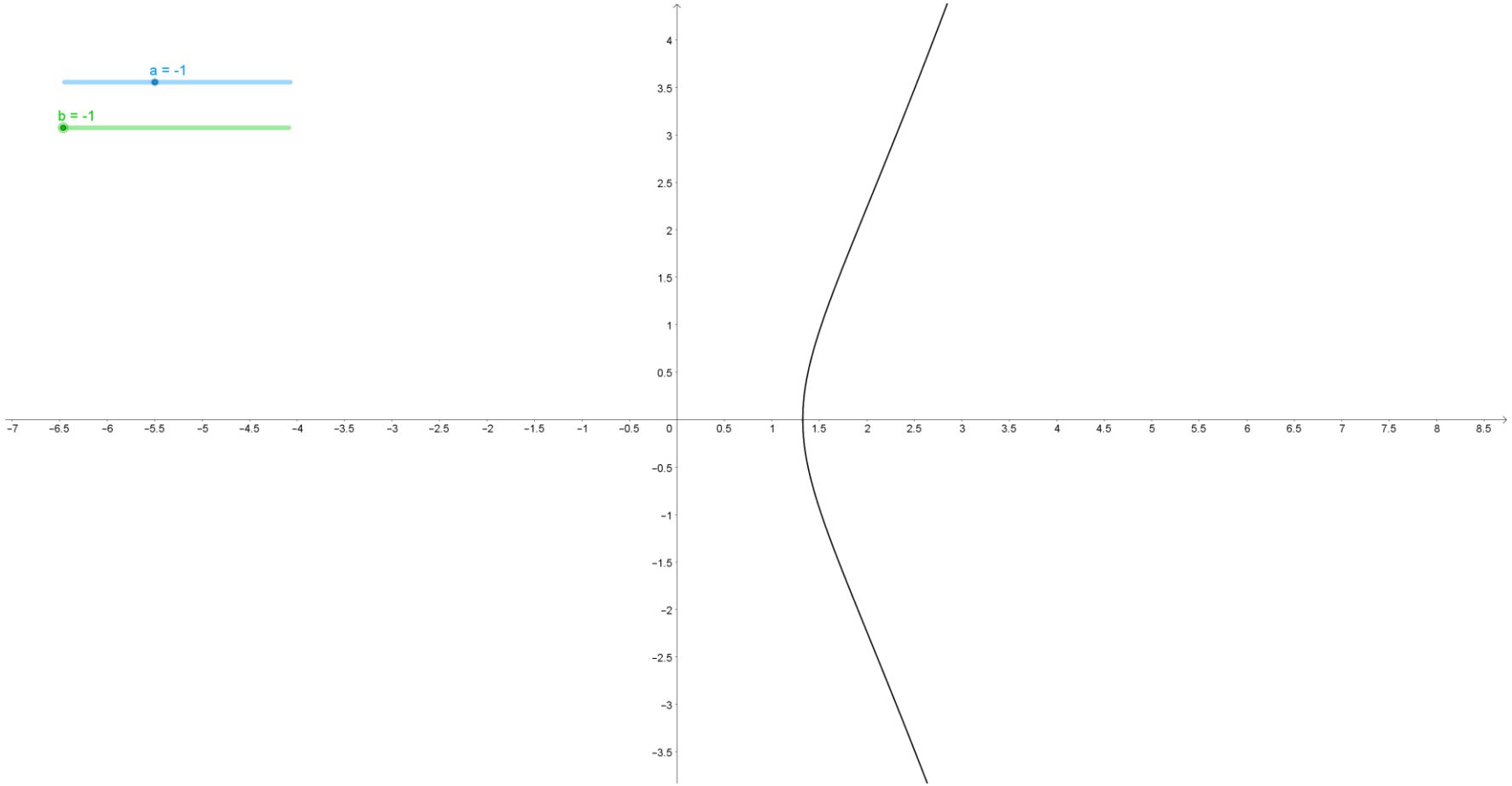
Une courbe elliptique, késaco?

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



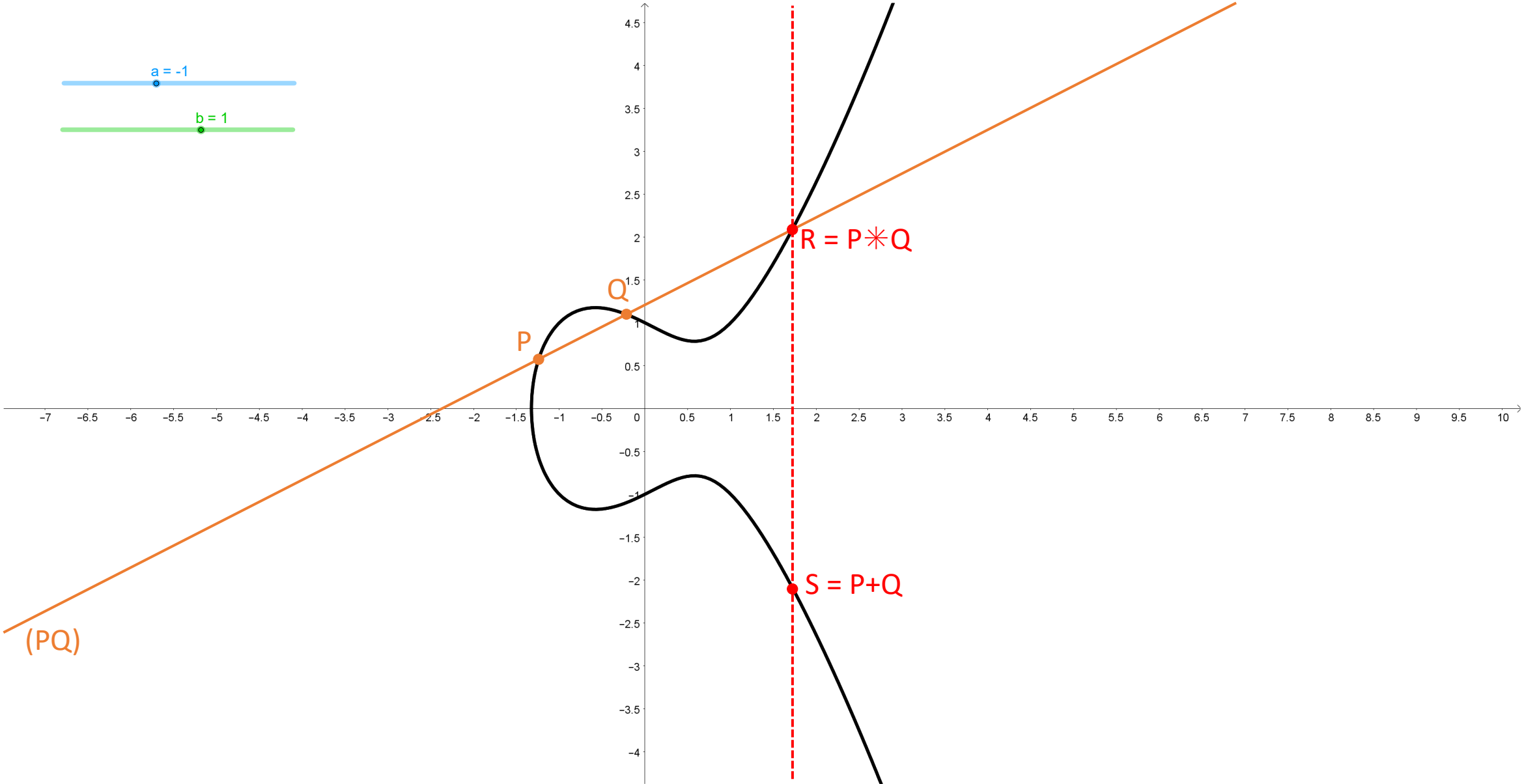
Une courbe elliptique, késaco?

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



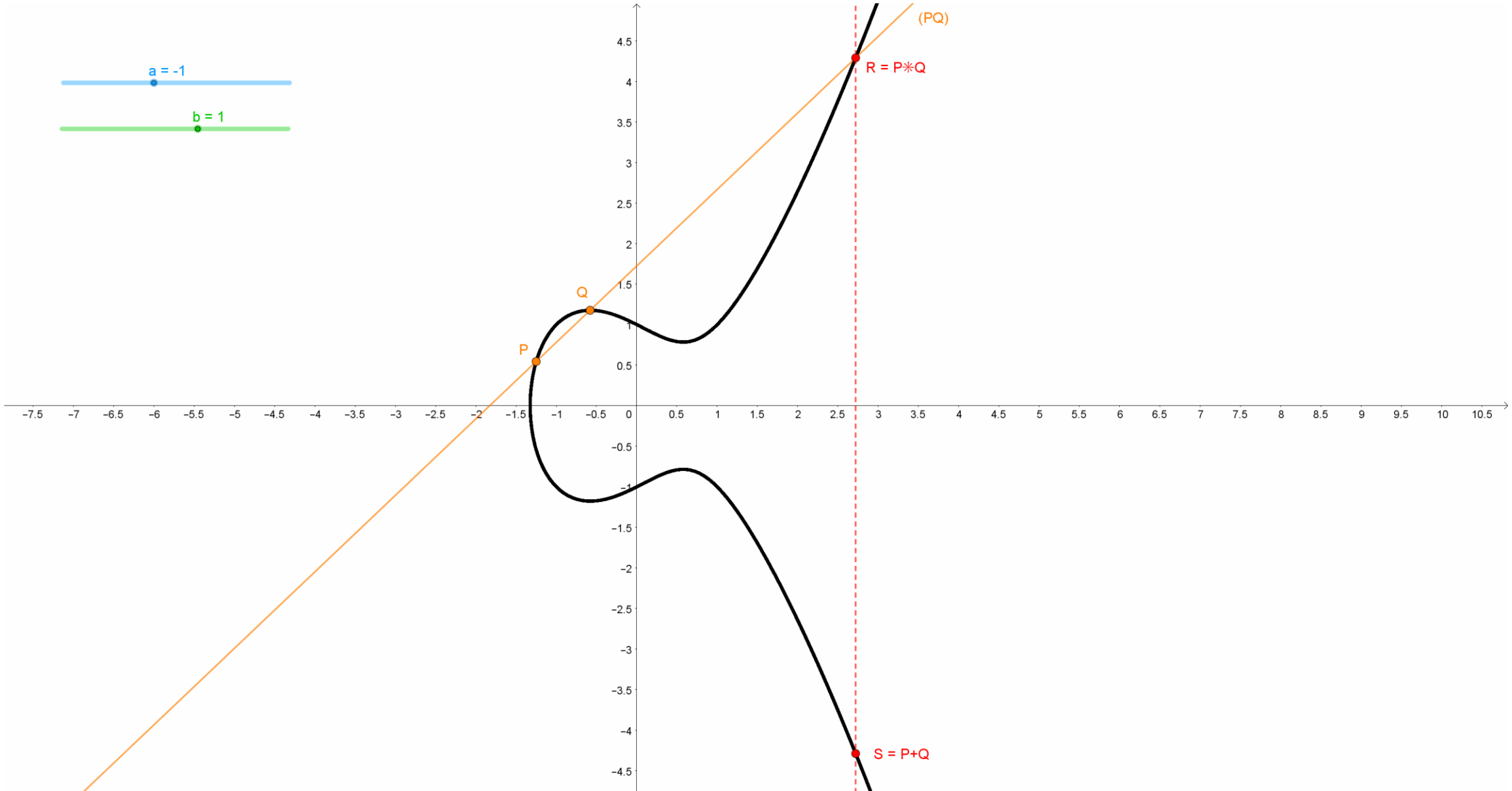
Courbe Elliptique: **Addition (P+Q)**

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



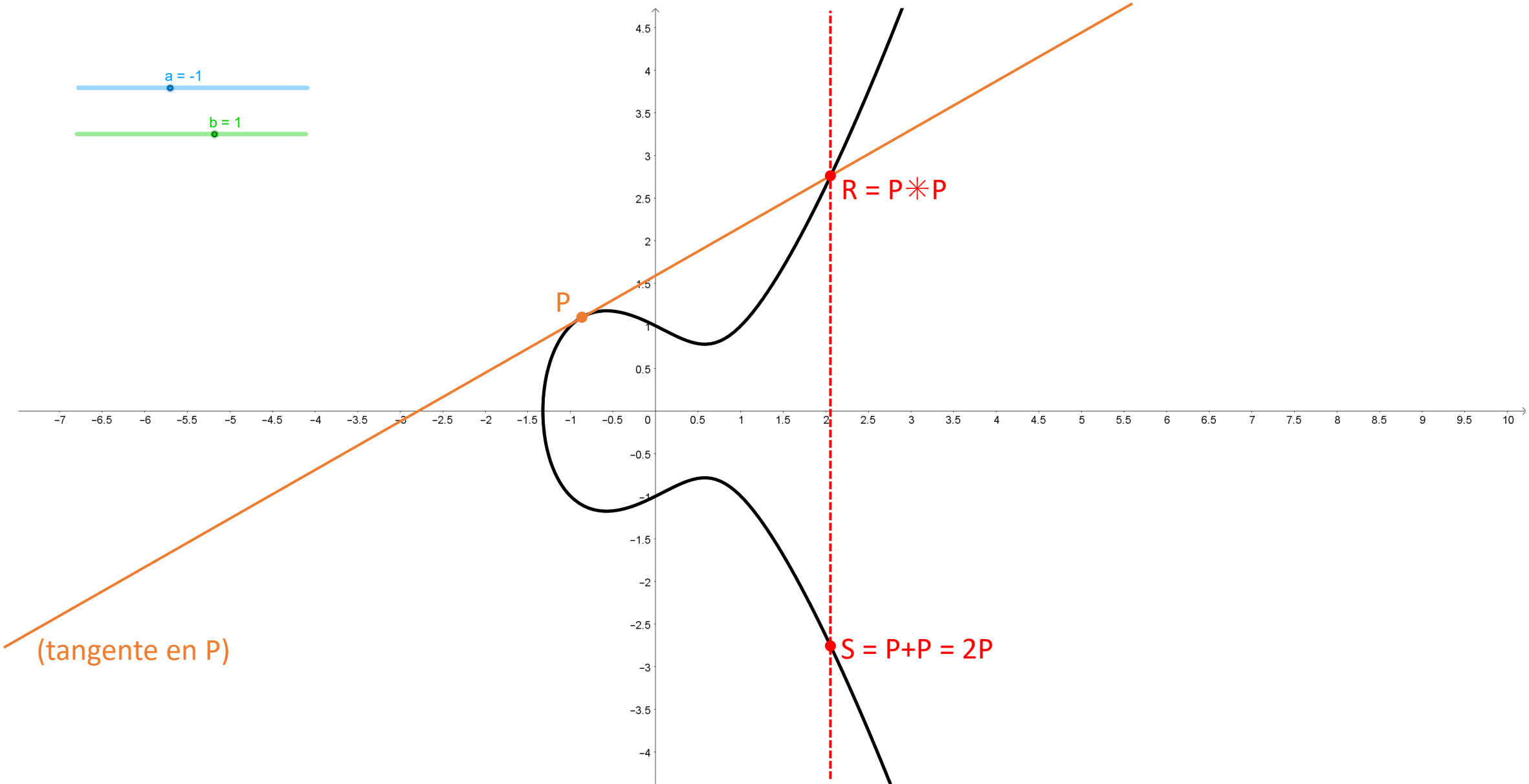
Courbe Elliptique: **Addition P+P?**

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



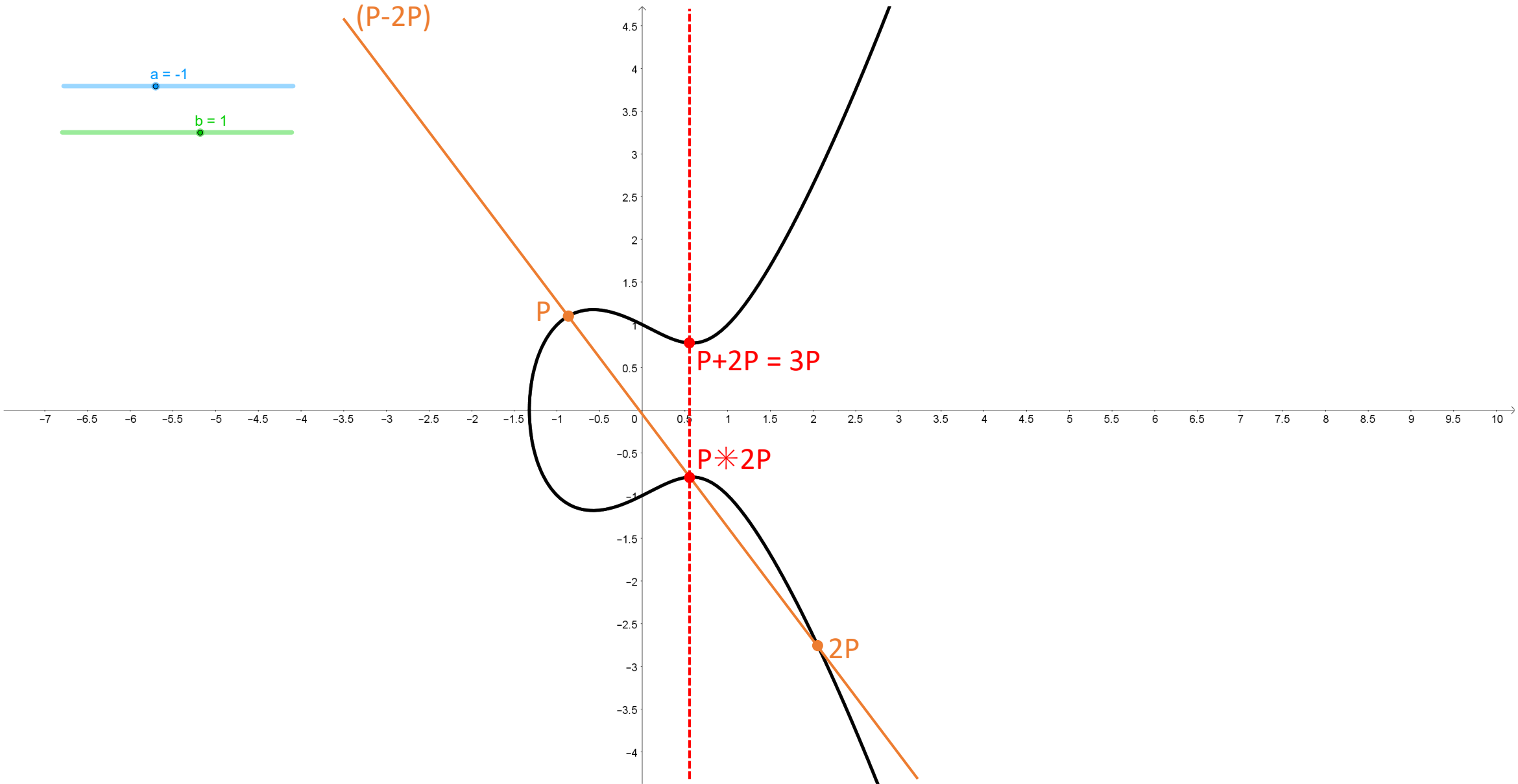
Courbe Elliptique: **Double (2P)**

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



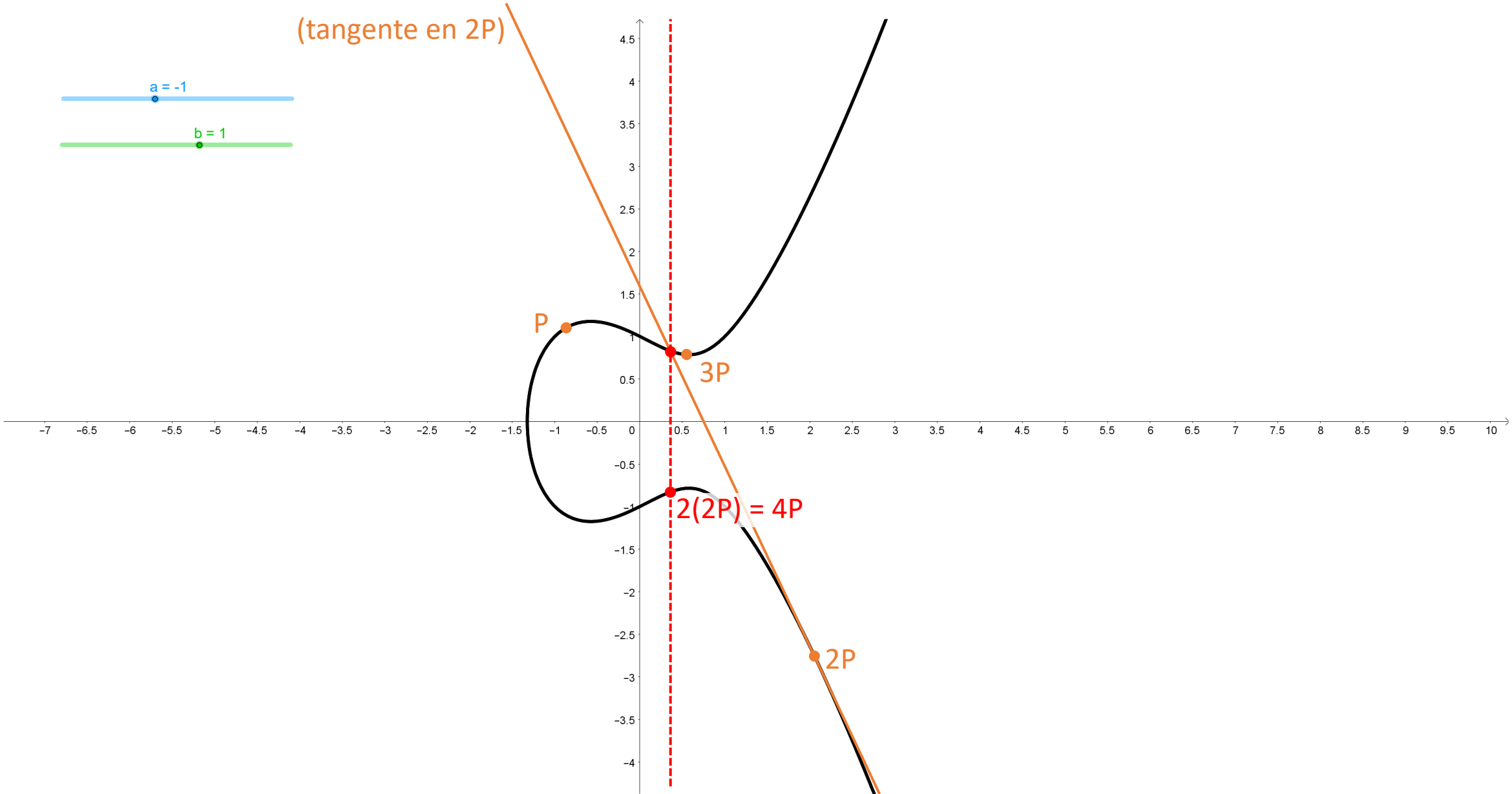
Courbe Elliptique: 3P = P+2P

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



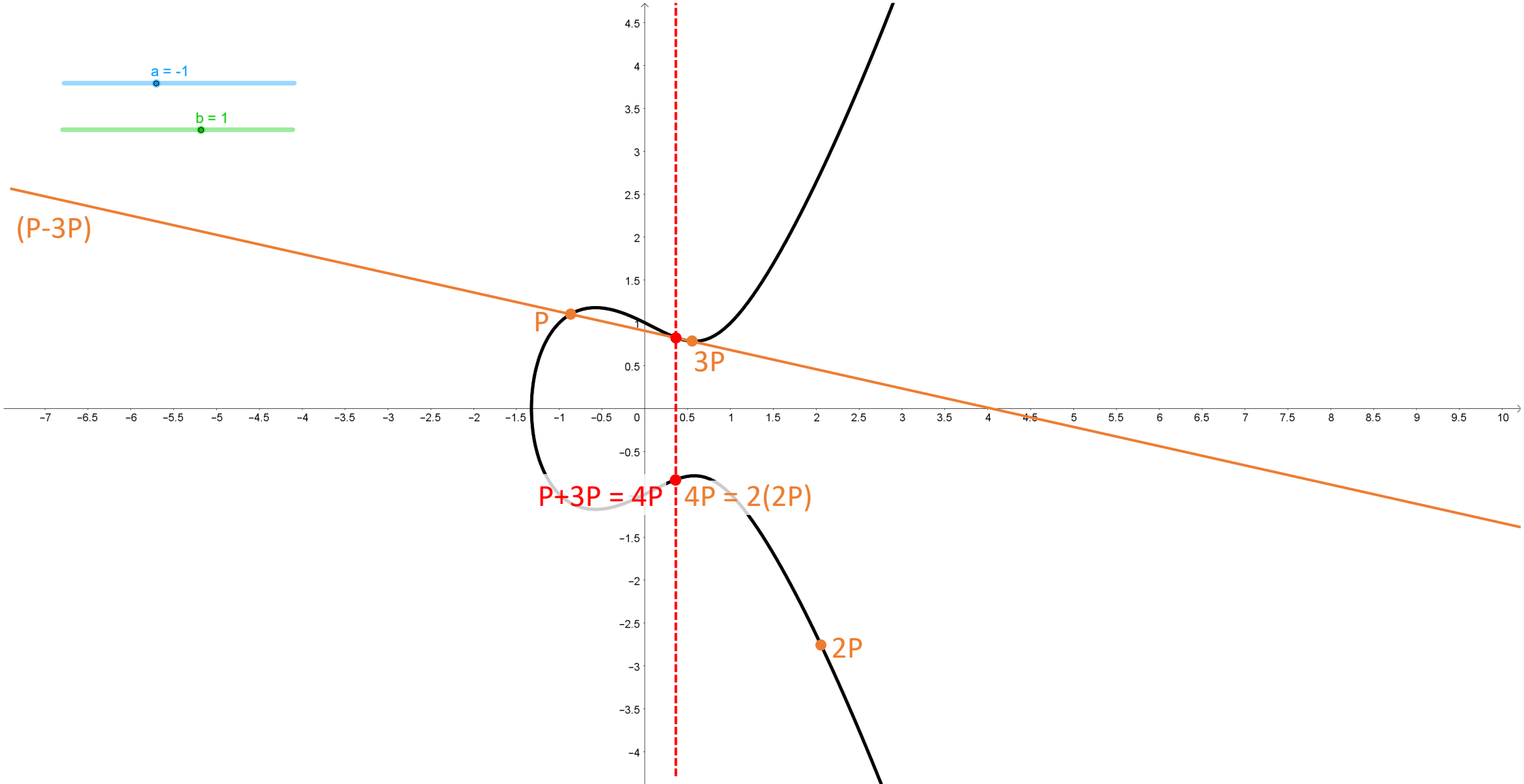
Courbe Elliptique: 4P = 2(2P) ou P+3P?

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



Courbe Elliptique: 4P = 2(2P) ou P+3P?

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



R
T

$$S = nR = kQ = nkP$$

P
Q

$* n$

$* k$

$R = kP$

$Q = nP$

$* k$

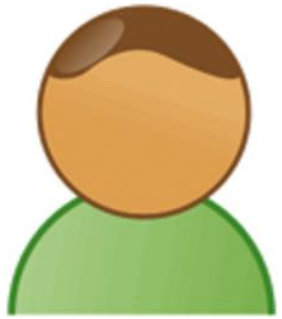
$* n$

P

$\boldsymbol{C}: y^2 = x^3 + ax + b$

$M \in C$ (le message)
$k \in \mathbb{N}$
$\mathrm{R} = kP$
$S = kQ$

$T = S + M$



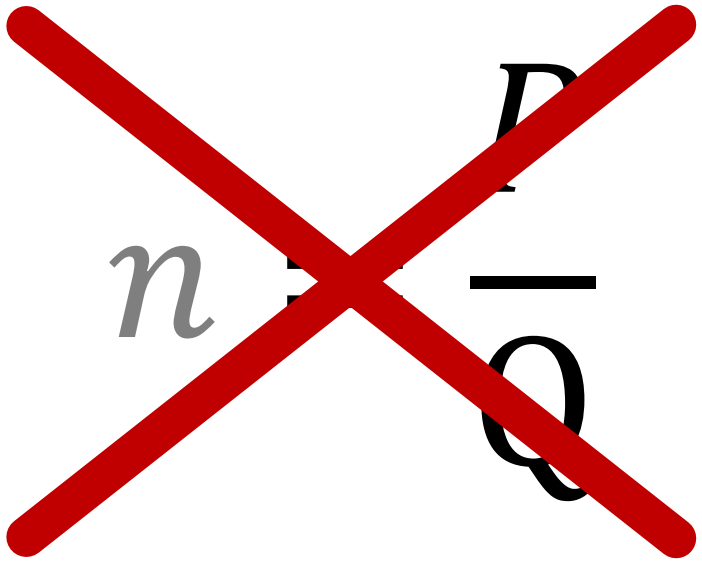
$n \in \mathbb{N}, P \in C$
$Q = nP$

$S = nR$

$M = T - S$

Division sur une Courbe Elliptique

$$nP = Q$$



Principales conclusions

- L'espion est **bloqué** par l'impossibilité de **calculer S** (à partir des info publiques) & de trouver n ou k.
- Chiffrement **symétrique**

« + »:

- **Pas** besoin d'une clef de **code inconnue par l'espion**

« - »:

- **Assez couteux** en terme de calculs
- (Très) **Difficile** à hacker par **force brute**
- Sujet aux **attaques par ordinateurs quantiques**


Aimez-vous Toulouse?

Aimez-vous les équations? ✓

Aimez-vous les protocoles sécurisés? ✓

Aimez-vous Toulouse? ✓

Aimez-vous l'argent? ✓

Fermat… un toulousain trop peu connu

« Petit théorème de Fermat »:

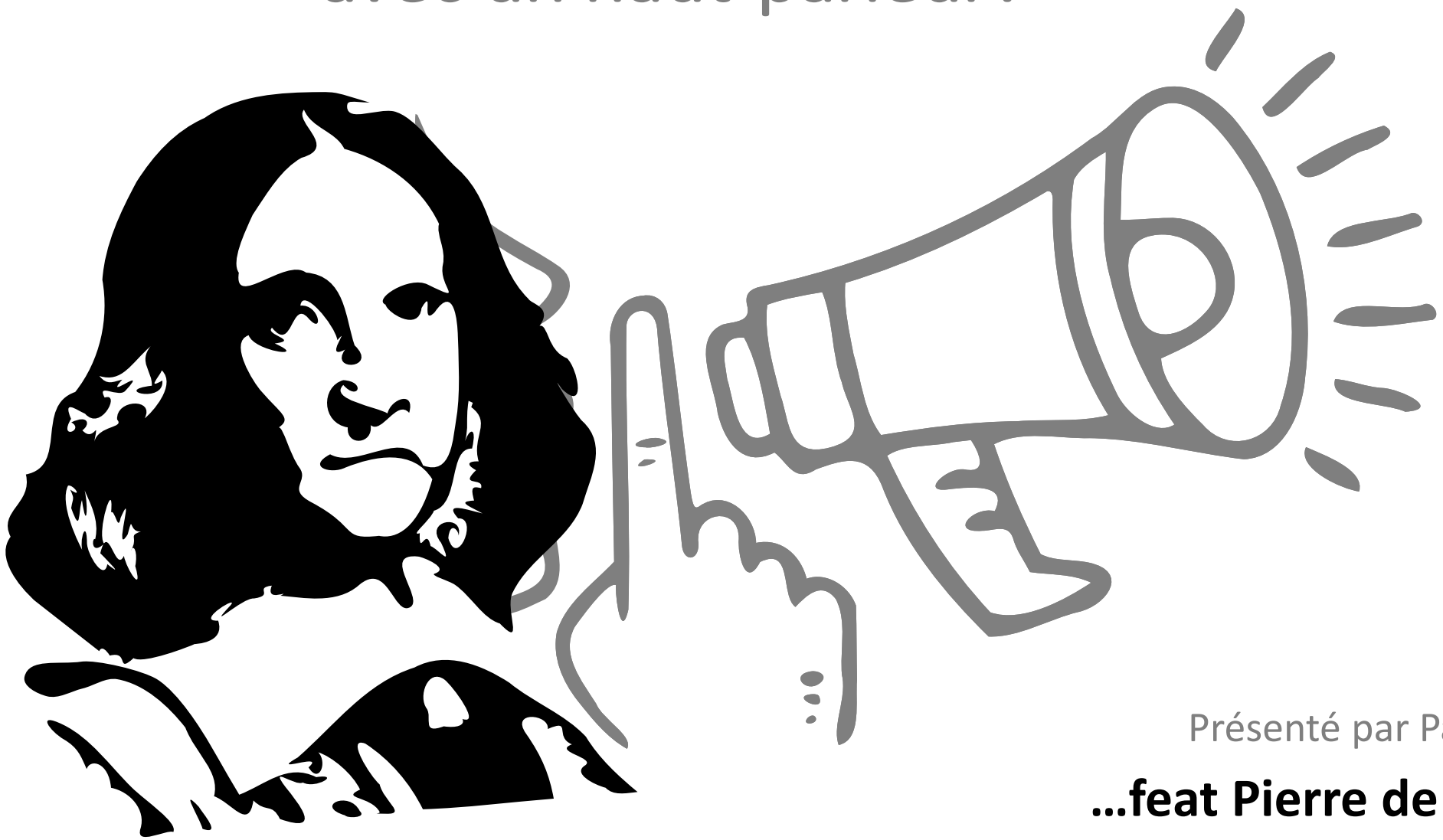
$$a^{p-1} \equiv 1\ [p]$$

« Grand théorème de Fermat »:

$$x^n + y^n = z^n$$

Pierre de Fermat

CRYPTOGRAPHIE ASYMETRIQUE:
Ou comment envoyer un secret avec un haut-parleur?



Présenté par Paul DUBOIS

…feat Pierre de FERMAT