

# De la géométrie à la cryptographie

Alena Pirutka

CNRS et École Polytechnique

La coulée verte  
Jeudi 12 février 2015

## De l'année 1840...

*Le nombre est dans l'art comme dans la science.  
L'algèbre est dans l'astronomie, et l'astronomie touche à  
la poésie; l'algèbre est dans la musique, et la musique  
touche à la poésie. L'esprit de l'homme a trois clefs qui  
ouvrent tout : le chiffre, la lettre, la note. Savoir, penser,  
rêver. Tout est là.*

(Victor Hugo, «Les Rayons et les Ombres», préface)

à l'année 2015 :



# Connections Internet

The image shows a browser window displaying a search result for 'kafemath'. A security warning dialog box is overlaid on the page, indicating that the connection is encrypted. The search result includes the URL, a description of Kafemath as a mathematical cafe, and a list of related links and dates.

Vous vous trouvez sur **google.fr**  
Vérfié par : Google Inc  
La connexion vers ce site est chiffrée.

Plus d'informations...

**kafemath.fr/** ▼  
Le **Kafemath** est un essai de café mathématique. Un café mathématique est aux mathématiques ce que le "café-philos" est à la philosophie !  
Vous avez consulté cette page 2 fois. Dernière visite : 27/01/15

**2013-2014**  
avec André Deledicq, créateur du "concours Kangourou des ...

**Kafemath Pour transmettre l...**  
expérience kafemath.fr suites.  
Kafemath. Pour transmettre le...

**Sites à visiter**  
Sites mathématiques à visiter de toute urgence !

**2012-2013**  
Les séances du Kafemath en 2012-2013. "Cent ans de mathématique

kafemath - Recherche Go... x +

https://www.google.fr/search? Informations sur la page - https://www.google.fr/search?q=kafemath&ie=utf-8&oe=utf-8&gws...  
Général Médias Permissions Sécurité

Les plus visités Débuter avec Fire...  
kafemath

Web Maps In

Environ 1 170 résultats

**kafemath**  
kafemath.fr /  
Le Kafemath est un es  
mathématiques ce que  
Vous avez consulté ce  
2013-2014  
avec André Deled  
"concours Kangou  
Kafemath Po  
expérience kafem  
Kafemath. Pour tr  
Autres résultats s

**Identité du site web**

Site web : **www.google.fr**  
Propriétaire : **Ce site web ne fournit pas d'informations sur son propriétaire.**  
Vérfiée par : **Google Inc**

[Afficher le certificat](#)

**Vie privée et historique**

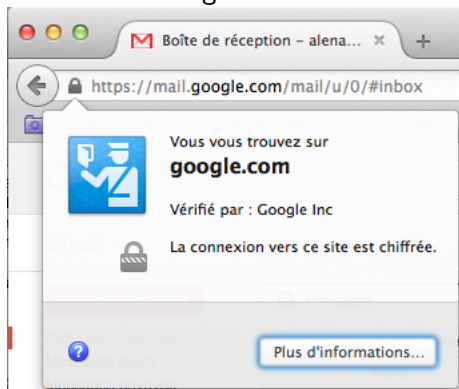
Ai-je déjà visité ce site web auparavant ?	Oui, 104 fois
Ce site web collecte-t-il des informations (cookies) sur mon ordinateur ?	Oui <a href="#">Voir les cookies</a>
Ai-je un mot de passe enregistré pour ce site web ?	Non <a href="#">Voir les mots de passe enregistrés</a>

**Détails techniques**

**Connexion chiffrée : chiffrement de haut niveau (clés TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256, 128 bits)**  
La page que vous voyez a été chiffrée avant sa transmission sur Internet.  
Le chiffrement rend très difficile aux personnes non autorisées la visualisation de la page durant son transit entre ordinateurs. Il est donc très improbable que quelqu'un puisse lire cette page durant son transit sur le réseau.

**Le Kafemath - La Coulée Douce**  
www.lacouleedouce.fr/le-kafemath /  
Tout en restant ouvert à tous, au Kafemath, on parle de maths, on en découvre l'  
histoire, on en fait un peu, on en débat, on en apprend si on veut. On y rit et ...

Ou encore avec gmail:



# Plan

# Plan

1. Quelques principes et algorithmes.

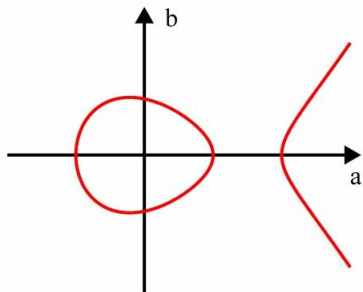


# Plan

1. Quelques principes et algorithmes.
2. Les méthodes du siècle précédent : nombres entiers, divisibilité et RSA.

# Plan

1. Quelques principes et algorithmes.
2. Les méthodes du siècle précédent : nombres entiers, divisibilité et RSA.
3. Les méthodes modernes : courbes elliptiques.



# Contexte cryptographique

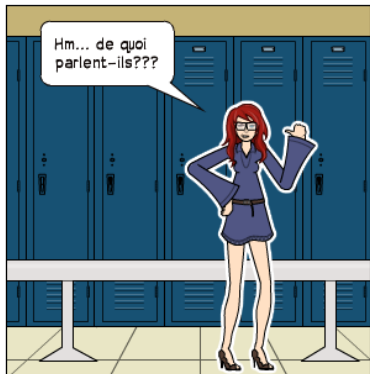
# Contexte cryptographique



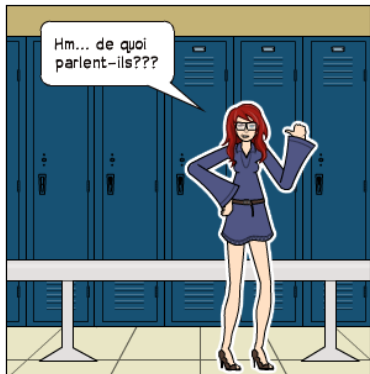
# Contexte cryptographique



# Eva

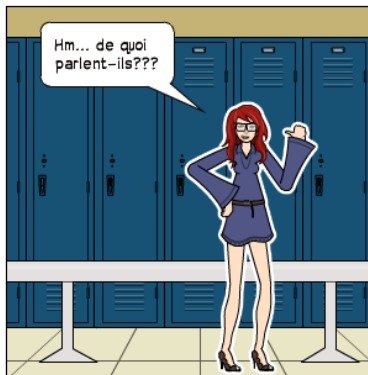


# Eva



- ▶ Eva veut lire le message privé d'Alice;

## Eva



- ▶ Eva veut lire le message privé d'Alice;
- ▶ Elle peut accéder au canal public de transmission des messages.



# Chiffrement



# Chiffrement



- ▶ Alice et Bob se mettent d'accord sur le système de chiffrement qu'ils utilisent

# Chiffrement



- ▶ Alice et Bob se mettent d'accord sur le système de chiffrement qu'ils utilisent
- ▶ et aussi sur la **clé publique** nécessaire pour chiffrer le message.

# Déchiffrement



# Déchiffrement

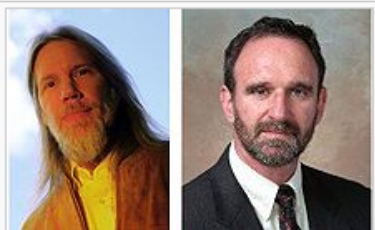


- ▶ Bob choisit la clé **privée** pour déchiffrer le message.

Principe : tout le monde peut chiffrer (avec la clé publique), mais il n'y a que Bob qui peut déchiffrer (avec sa clé privée).

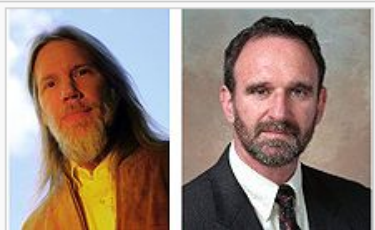


Cette méthode a été proposée en 1976 par Whitfield Diffie et Martin Hellman :



On l'appelle la **cryptographie à clé publique**.

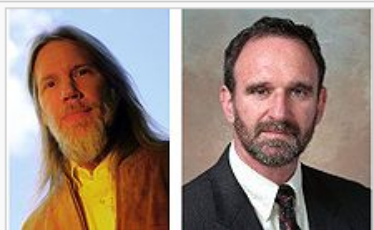
Cette méthode a été proposée en 1976 par Whitfield Diffie et Martin Hellman :



On l'appelle la **cryptographie à clé publique**.  
Propriétés :



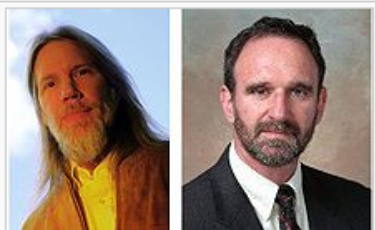
Cette méthode a été proposée en 1976 par Whitfield Diffie et Martin Hellman :



On l'appelle la **cryptographie à clé publique**.  
Propriétés :

- ▶ C'est «facile» de coder le message.

Cette méthode a été proposée en 1976 par Whitfield Diffie et Martin Hellman :



On l'appelle la **cryptographie à clé publique**.

Propriétés :

- ▶ C'est «facile» de coder le message.
- ▶ Il est très difficile de déchiffrer le message *sans connaître la clé privée* .

# Signature numérique

# Signature numérique



# Signature numérique

Principe : il n'y a qu'Alice qui peut signer (avec sa clé privée), mais tout le monde peut vérifier (avec la clé publique).

## Signature numérique

Principe : il n'y a qu'Alice qui peut signer (avec sa clé privée), mais tout le monde peut vérifier (avec la clé publique).



# Algorithme RSA

Proposé par Ronald Rivest, Adi Shamir et Leonard Adleman

# Algorithmme RSA

Proposé par Ronald Rivest, Adi Shamir et Leonard Adleman



en 1978 dans l'article "A Method for Obtaining Digital Signatures and Public-key Cryptosystems".



# Algorithmme RSA

Proposé par Ronald Rivest, Adi Shamir et Leonard Adleman



en 1978 dans l'article "A Method for Obtaining Digital Signatures and Public-key Cryptosystems".

- ▶ Les «messages» sont des nombres entiers;

# Algorithme RSA

Proposé par Ronald Rivest, Adi Shamir et Leonard Adleman



en 1978 dans l'article "A Method for Obtaining Digital Signatures and Public-key Cryptosystems".

- ▶ Les «messages» sont des nombres entiers;
- ▶ Pour coder un message, on utilise les opérations arithmétiques: sommes, produits, divisions.

# Bases arithmétiques

- ▶ On dit qu'un entier  $d$  divise un entier  $n$  si l'on peut écrire

$$n = d \cdot q$$

avec  $q$  un entier. Si c'est le cas, on écrit  $d|n$ .

# Bases arithmétiques

- ▶ On dit qu'un entier  $d$  divise un entier  $n$  si l'on peut écrire

$$n = d \cdot q$$

avec  $q$  un entier. Si c'est le cas, on écrit  $d|n$ .

Exemples:  $3|12$  car  $12 = 3 \cdot 4$ ;  $5|2015$  car  $2015 = 5 \cdot 403$ ,

## Bases arithmétiques

- ▶ On dit qu'un entier  $d$  **divise** un entier  $n$  (ou que  $d$  est un **facteur** de  $n$ ) si l'on peut écrire

$$n = d \cdot q$$

avec  $q$  un entier. Si c'est le cas, on écrit  $d|n$ .

Exemples:  $3|12$  car  $12 = 3 \cdot 4$ ;  $5|2015$  car  $2015 = 5 \cdot 403$

## Bases arithmétiques

- ▶ On dit qu'un entier  $d$  **divise** un entier  $n$  (ou que  $d$  est un **facteur** de  $n$ ) si l'on peut écrire

$$n = d \cdot q$$

avec  $q$  un entier. Si c'est le cas, on écrit  $d|n$ .

Exemples:  $3|12$  car  $12 = 3 \cdot 4$ ;  $5|2015$  car  $2015 = 5 \cdot 403$   
aussi  $1|n$  pour tout  $n$  et  $n|n$ .

## Bases arithmétiques

- ▶ On dit qu'un entier  $d$  **divise** un entier  $n$  (ou que  $d$  est un **facteur** de  $n$ ) si l'on peut écrire

$$n = d \cdot q$$

avec  $q$  un entier. Si c'est le cas, on écrit  $d|n$ .

Exemples:  $3|12$  car  $12 = 3 \cdot 4$ ;  $5|2015$  car  $2015 = 5 \cdot 403$   
aussi  $1|n$  pour tout  $n$  et  $n|n$ .

- ▶ Un entier  $p$  est **premier** s'il n'y a que deux nombres distincts qui divisent  $p$  : 1 et  $p$ .

## Bases arithmétiques

- ▶ On dit qu'un entier  $d$  **divise** un entier  $n$  (ou que  $d$  est un **facteur** de  $n$ ) si l'on peut écrire

$$n = d \cdot q$$

avec  $q$  un entier. Si c'est le cas, on écrit  $d|n$ .

Exemples:  $3|12$  car  $12 = 3 \cdot 4$ ;  $5|2015$  car  $2015 = 5 \cdot 403$   
aussi  $1|n$  pour tout  $n$  et  $n|n$ .

- ▶ Un entier  $p$  est **premier** s'il n'y a que deux nombres distincts qui divisent  $p$  : 1 et  $p$ . Exemples: 2, 3, 5, 7, 11, 13...



# Congruences

- ▶ Si  $n$  et  $m$  sont des entiers et  $d|(n - m)$  on dit que  $n$  est **congru à  $m$  modulo  $d$** :

$$n \equiv m \pmod{d}.$$

# Congruences

- ▶ Si  $n$  et  $m$  sont des entiers et  $d|(n - m)$  on dit que  $n$  est **congru à  $m$  modulo  $d$** :

$$n \equiv m \pmod{d}.$$

Exemple :  $10 \equiv 4 \pmod{3}$ ,  $2 \equiv 8 \pmod{3}$ .

# Congruences

- ▶ Si  $n$  et  $m$  sont des entiers et  $d|(n - m)$  on dit que  $n$  est **congru à  $m$  modulo  $d$** :

$$n \equiv m \pmod{d}.$$

Exemple :  $10 \equiv 4 \pmod{3}$ ,  $2 \equiv 8 \pmod{3}$ .

- ▶ Multiplication : si

$$n \equiv m \pmod{d}$$

et  $a \equiv b \pmod{d}$  alors

$$an \equiv bm \pmod{d}.$$

# Congruences

- ▶ Si  $n$  et  $m$  sont des entiers et  $d|(n - m)$  on dit que  $n$  est **congru à  $m$  modulo  $d$** :

$$n \equiv m \pmod{d}.$$

Exemple :  $10 \equiv 4 \pmod{3}$ ,  $2 \equiv 8 \pmod{3}$ .

- ▶ Multiplication : si

$$n \equiv m \pmod{d}$$

et  $a \equiv b \pmod{d}$  alors

$$an \equiv bm \pmod{d}.$$

Exemple :  $20 \equiv 32 \pmod{3}$ .

# Congruences

- ▶ Si  $n$  et  $m$  sont des entiers et  $d|(n - m)$  on dit que  $n$  est **congru à  $m$  modulo  $d$** :

$$n \equiv m \pmod{d}.$$

Exemple :  $10 \equiv 4 \pmod{3}$ ,  $2 \equiv 8 \pmod{3}$ .

- ▶ Multiplication : si

$$n \equiv m \pmod{d}$$

et  $a \equiv b \pmod{d}$  alors

$$an \equiv bm \pmod{d}.$$

Exemple :  $20 \equiv 32 \pmod{3}$ .

- ▶ Si  $d|n$  et  $d|m$  on dit que  $d$  est un **diviseur commun** de  $n$  et  $m$ . Si  $n$  et  $m$  n'ont pas de diviseurs communs (sauf 1) on dit que  $n$  et  $m$  sont **premiers entre eux**.

# Congruences

- ▶ Si  $n$  et  $m$  sont des entiers et  $d|(n - m)$  on dit que  $n$  est **congru à  $m$  modulo  $d$** :

$$n \equiv m \pmod{d}.$$

Exemple :  $10 \equiv 4 \pmod{3}$ ,  $2 \equiv 8 \pmod{3}$ .

- ▶ Multiplication : si

$$n \equiv m \pmod{d}$$

et  $a \equiv b \pmod{d}$  alors

$$an \equiv bm \pmod{d}.$$

Exemple :  $20 \equiv 32 \pmod{3}$ .

- ▶ Si  $d|n$  et  $d|m$  on dit que  $d$  est un **diviseur commun** de  $n$  et  $m$ . Si  $n$  et  $m$  n'ont pas de diviseurs communs (sauf 1) on dit que  $n$  et  $m$  sont **premiers entre eux**.

Exemples: 5 et 7, 10 et 27.

- ▶ Division euclidienne : on peut toujours diviser un entier  $n$  par un entier  $d$  avec le reste :

$$n = d \cdot q + r$$

où  $r$  est le reste,  $0 \leq r < d$ .

- ▶ Division euclidienne : on peut toujours diviser un entier  $n$  par un entier  $d$  avec le reste :

$$n = d \cdot q + r$$

où  $r$  est le reste,  $0 \leq r < d$ .

Exemples:  $12 = 3 \cdot 4 + 0$ ,  $12 = 7 \cdot 1 + 5$ ,  $2015 = 100 \cdot 20 + 15$ .

On a

$$n \equiv r \pmod{d}.$$

On a  $12 \equiv 5 \pmod{7}$ ,  $2015 \equiv 15 \pmod{100}$ .



## Division et puissances

Question : quels restes vont donner  $n, n^2, n^3 \dots$  modulo  $d$ ?

Peut-on avoir  $r = 1$ ?

## Division et puissances

Question : quels restes vont donner  $n$ ,  $n^2$ ,  $n^3 \dots$  modulo  $d$ ?

Peut-on avoir  $r = 1$ ?

- ▶ si  $d = p$  est un nombre premier et  $p$  ne divise pas  $n$ , alors

$$n^{p-1} \equiv 1 \pmod{p}.$$

(petit théorème de Fermat).

## Division et puissances

Question : quels restes vont donner  $n, n^2, n^3 \dots$  modulo  $d$ ?

Peut-on avoir  $r = 1$ ?

- ▶ si  $d = p$  est un nombre premier et  $p$  ne divise pas  $n$ , alors

$$n^{p-1} \equiv 1 \pmod{p}.$$

(petit théorème de Fermat).

ou encore (en multipliant par  $n$ ) :  $n^p \equiv n \pmod{p}$ .

- ▶ Si  $d = pq$  est le produit de deux nombres premiers distincts et ni  $p$ , ni  $q$  ne divise  $n$ , alors

$$n^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

- ▶ Si  $d = pq$  est le produit de deux nombres premiers distincts et ni  $p$ , ni  $q$  ne divise  $n$ , alors

$$n^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

Ou encore, on multiplie  $a$  fois cette congruence par elle-même :

$$n^{(p-1)(q-1)a} \equiv 1^a = 1 \pmod{pq}.$$

- ▶ Si  $d = pq$  est le produit de deux nombres premiers distincts et ni  $p$ , ni  $q$  ne divise  $n$ , alors

$$n^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

Ou encore, on multiplie  $a$  fois cette congruence par elle-même :

$$n^{(p-1)(q-1)a} \equiv 1^a = 1 \pmod{pq}.$$

et

$$n^{(p-1)(q-1)a+1} \equiv n \pmod{pq}.$$

# Fonctionnement de RSA

- ▶ On choisit  $N$  un entier tel que  $N = pq$  est le produit de deux (très grands) nombres premiers.

## Fonctionnement de RSA

- ▶ On choisit  $N$  un entier tel que  $N = pq$  est le produit de deux (très grands) nombres premiers.
- ▶ Un «message» sera un entier  $m$  tel que  $1 \leq m < N$ .



## Fonctionnement de RSA

- ▶ On choisit  $N$  un entier tel que  $N = pq$  est le produit de deux (très grands) nombres premiers.
- ▶ Un «message» sera un entier  $m$  tel que  $1 \leq m < N$ .
- ▶ Le chiffrement : le reste  $r$  de  $m^e$  modulo  $N$ .

## Fonctionnement de RSA

- ▶ On choisit  $N$  un entier tel que  $N = pq$  est le produit de deux (très grands) nombres premiers.
- ▶ Un «message» sera un entier  $m$  tel que  $1 \leq m < N$ .
- ▶ Le chiffrement : le reste  $r$  de  $m^e$  modulo  $N$ .
- ▶ Pour déchiffrer... encore des puissances : on calcule le reste de  $r^f$  de modulo  $N$ . Comment choisit-on  $f$ ?

## Fonctionnement de RSA

- ▶ On choisit  $N$  un entier tel que  $N = pq$  est le produit de deux (très grands) nombres premiers.
- ▶ Un «message» sera un entier  $m$  tel que  $1 \leq m < N$ .
- ▶ Le chiffrement : le reste  $r$  de  $m^e$  modulo  $N$ .
- ▶ Pour déchiffrer... encore des puissances : on calcule le reste de  $r^f$  de modulo  $N$ . Comment choisit-on  $f$ ? On a

$$r \equiv m^e \pmod{pq}$$

En multipliant  $f$  fois cette congruence par elle-même:

$$r^f \equiv (m^e)^f = m^{ef} \pmod{pq}$$

## Fonctionnement de RSA

- ▶ On choisit  $N$  un entier tel que  $N = pq$  est le produit de deux (très grands) nombres premiers.
- ▶ Un «message» sera un entier  $m$  tel que  $1 \leq m < N$ .
- ▶ Le chiffrement : le reste  $r$  de  $m^e$  modulo  $N$ .
- ▶ Pour déchiffrer... encore des puissances : on calcule le reste de  $r^f$  de modulo  $N$ . Comment choisit-on  $f$ ? On a

$$r \equiv m^e \pmod{pq}$$

En multipliant  $f$  fois cette congruence par elle-même:

$$r^f \equiv (m^e)^f = m^{ef} \pmod{pq} \equiv m?$$

Comment avoir  $m^{ef} \equiv m \pmod{pq}$ ?

Comment avoir  $m^{ef} \equiv m \pmod{pq}$ ?

Petit théorème de Fermat : il faut prendre  $f$  tel que  
 $ef = (p-1)(q-1)a + 1$ , i.e. que

$$ef \equiv 1 \pmod{(p-1)(q-1)}.$$

(rappel :  $n^{(p-1)(q-1)a+1} \equiv n \pmod{pq}$ .)

## Récapitulatif

Paramètres :  $p, q$  deux nombres premiers,  $N = pq$ ,  $e, f$  tels que  $ef \equiv 1 \pmod{(p-1)(q-1)}$ .

# Récapitulatif

Paramètres :  $p, q$  deux nombres premiers,  $N = pq$ ,  $e, f$  tels que  $ef \equiv 1 \pmod{(p-1)(q-1)}$ .

Données publiques  $N, e$ .



# Récapitulatif

Paramètres :  $p, q$  deux nombres premiers,  $N = pq$ ,  $e, f$  tels que  $ef \equiv 1 \pmod{(p-1)(q-1)}$ .

Données publiques  $N, e$ . **Clé privée de Bob** :  $f$ .

## Récapitulatif

Paramètres :  $p, q$  deux nombres premiers,  $N = pq$ ,  $e, f$  tels que  $ef \equiv 1 \pmod{(p-1)(q-1)}$ .

Données publiques  $N, e$ . **Clé privée de Bob** :  $f$ .



## Récapitulatif

Paramètres :  $p, q$  deux nombres premiers,  $N = pq$ ,  $e, f$  tels que  $ef \equiv 1 \pmod{(p-1)(q-1)}$ .

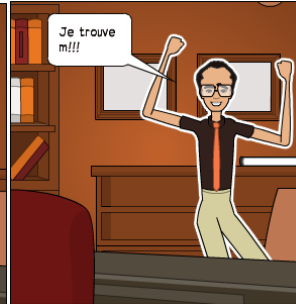
Données publiques  $N, e$ . **Clé privée de Bob** :  $f$ .



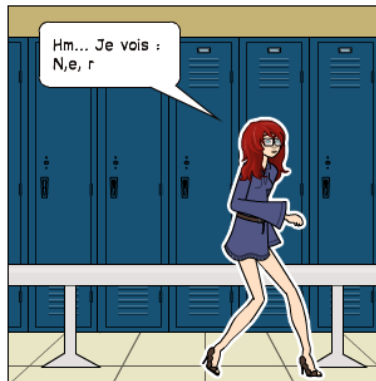
## Récapitulatif

Paramètres :  $p, q$  deux nombres premiers,  $N = pq$ ,  $e, f$  tels que  $ef \equiv 1 \pmod{(p-1)(q-1)}$ .

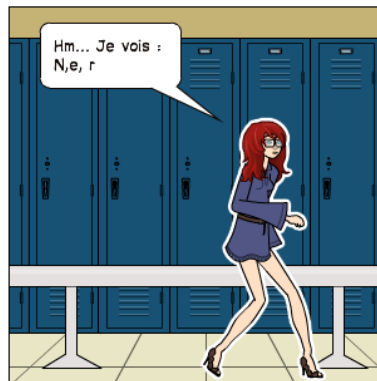
Données publiques  $N, e$ . **Clé privée de Bob** :  $f$ .



# La sécurité du système

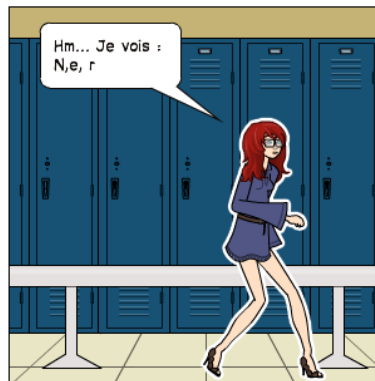


## La sécurité du système



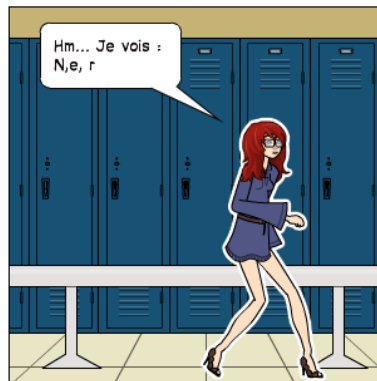
- ▶ On connaît  $r = m^e$  (modulo N), comment trouver  $m$ ?

## La sécurité du système



- ▶ On connaît  $r = m^e$  (modulo  $N$ ), comment trouver  $m$ ?
- ▶ Pour déchiffrer il faut connaître  $f$  tel que  $ef \equiv 1 \pmod{(p-1)(q-1)}$ .

## La sécurité du système



- ▶ On connaît  $r = m^e$  (modulo  $N$ ), comment trouver  $m$ ?
- ▶ Pour déchiffrer il faut connaître  $f$  tel que  $ef \equiv 1 \pmod{(p-1)(q-1)}$ .
- ▶ On peut le trouver si l'on connaît  $p$  et  $q$  (problème de **factorisation**).

Ce sont des problèmes très difficiles (techniquement)!!!



## Un exemple

- ▶ Le message : la note au BAC (entre  $1 = D$  et  $4 = A$ ).
- ▶  $p = 5, q = 7, N = 35, (p - 1)(q - 1) = 24, e = 5$ .
- ▶ On chiffre  $m = 4$

## Un exemple

- ▶ Le message : la note au BAC (entre  $1 = D$  et  $4 = A$ ).
- ▶  $p = 5, q = 7, N = 35, (p - 1)(q - 1) = 24, e = 5$ .
- ▶ On chiffre  $m = 4$  :  $4^5 \equiv$

## Un exemple

- ▶ Le message : la note au BAC (entre  $1 = D$  et  $4 = A$ ).
- ▶  $p = 5, q = 7, N = 35, (p - 1)(q - 1) = 24, e = 5$ .
- ▶ On chiffre  $m = 4$  :  $4^5 \equiv 9 \pmod{35}$ .

## Un exemple

- ▶ Le message : la note au BAC (entre  $1 = D$  et  $4 = A$ ).
- ▶  $p = 5, q = 7, N = 35, (p - 1)(q - 1) = 24, e = 5$ .
- ▶ On chiffre  $m = 4 : 4^5 \equiv 9 \pmod{35}$ .
- ▶ Déchiffrement :  $e \cdot 5 \equiv 1 \pmod{24}$ , ici  $f = 5$ .

## Un exemple

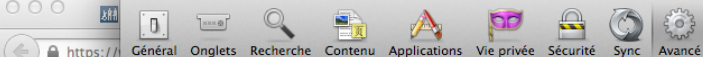
- ▶ Le message : la note au BAC (entre  $1 = D$  et  $4 = A$ ).
- ▶  $p = 5, q = 7, N = 35, (p - 1)(q - 1) = 24, e = 5$ .
- ▶ On chiffre  $m = 4 : 4^5 \equiv 9 \pmod{35}$ .
- ▶ Déchiffrement :  $e \cdot 5 \equiv 1 \pmod{24}$ , ici  $f = 5$ .
- ▶ On calcule  $9^5 \equiv$

## Un exemple

- ▶ Le message : la note au BAC (entre  $1 = D$  et  $4 = A$ ).
- ▶  $p = 5, q = 7, N = 35, (p - 1)(q - 1) = 24, e = 5$ .
- ▶ On chiffre  $m = 4$  :  $4^5 \equiv 9 \pmod{35}$ .
- ▶ Déchiffrement :  $e \cdot 5 \equiv 1 \pmod{24}$ , ici  $f = 5$ .
- ▶ On calcule  $9^5 \equiv 3^3 \cdot 3^3 \cdot 3^3 \cdot 3 \equiv (-8) \cdot (-8) \cdot (-8) \cdot 3 \equiv (-6) \cdot (-8) \cdot 3 \equiv -6 \cdot 11 \equiv 4 \pmod{35}$ .

## En réalité





Lorsqu'un serveur demande mon certificat personnel :

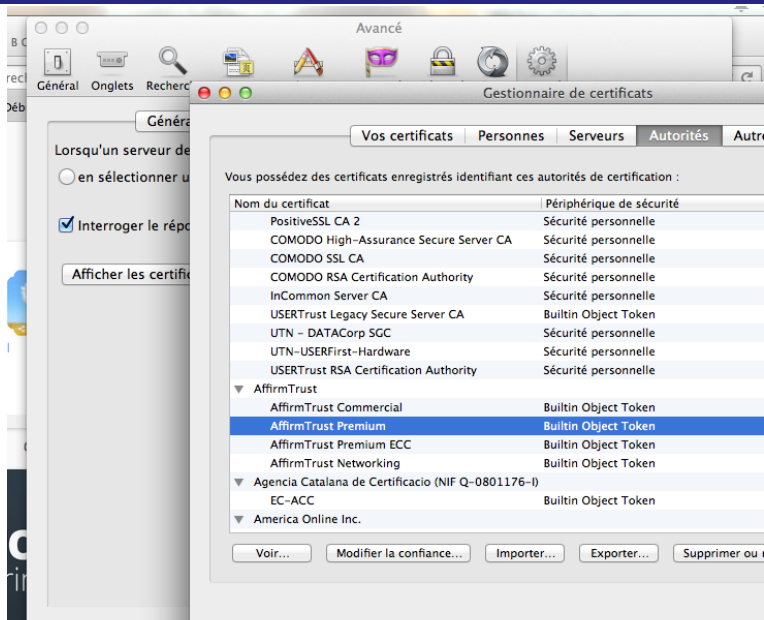
en sélectionner un automatiquement  me demander à chaque fois

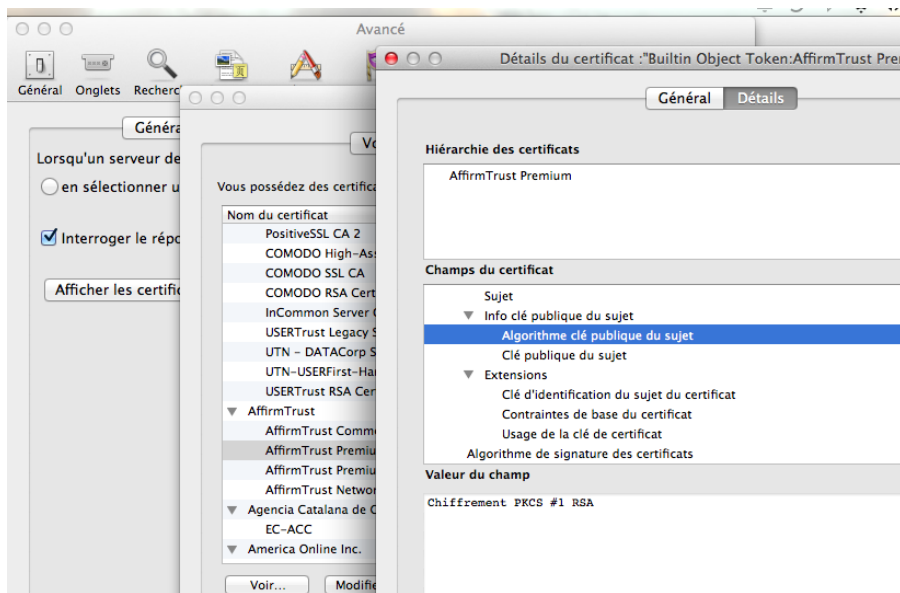
Interroger le répondeur OCSP pour confirmer la validité de vos certificats

Afficher les certificats

Périphériques de sécurité







Détails du certificat : "Builtin Object Token:AffirmTrust Premium"

Général Détails

**Hiérarchie des certificats**

AffirmTrust Premium

**Champs du certificat**

Sujet

- ▼ Info clé publique du sujet
  - Algorithme clé publique du sujet
  - Clé publique du sujet**
- ▼ Extensions
  - Clé d'identification du sujet du certificat
  - Contraintes de base du certificat
  - Usage de la clé de certificat
  - Algorithme de signature des certificats

**Valeur du champ**

Module (4096 bits) :

```
c4 12 df a9 5f fe 41 dd dd f5 9f 8a e3 f6 ac e1
3c 78 9a bc d8 f0 7f 7a a0 33 2a dc 8d 20 5b ae
2d 6f e7 93 d9 36 70 6a 68 cf 8e 51 a3 85 5b 67
04 a0 10 24 6f 5d 28 82 c1 97 57 d8 48 29 13 b6
e1 be 91 4d df 85 0c 53 18 9a 1e 24 a2 4f 8f f0
a2 85 0b cb f4 29 7f d2 a4 58 ee 26 4d c9 aa a8
7b 9a d9 fa 38 de 44 57 15 e5 f8 8c c8 d9 48 e2
0d 16 27 1d 1e c8 83 85 25 b7 ba aa 55 41 cc 03
22 4b 2d 91 8d 8b e6 89 af 66 c7 e9 ff 2b e9 3c
```

Exporter...

Vous possédez des certificats

Nom du certificat

- PositiveSSL CA 2
- COMODO High-As...
- COMODO SSL CA
- COMODO RSA Cert...
- InCommon Server C...
- USERTrust Legacy S...
- UTN - DATACorp S...
- UTN - USERFirst-Ha...
- USERTrust RSA Cer...
- ▼ AffirmTrust
  - AffirmTrust Comm...
  - AffirmTrust Premi...**
  - AffirmTrust Premi...
  - AffirmTrust Networ...
- ▼ Agencia Catalana de C...
  - EC-ACC
- ▼ America Online Inc.

Voir... Modifier

# Cryptographie avec les courbes elliptiques

Question : est-ce qu'on peut faire de l'arithmétique avec d'autres objets que les nombres?

# Cryptographie avec les courbes elliptiques

Question : est-ce qu'on peut faire de l'arithmétique avec d'autres objets que les nombres?

Oui! On peut additionner les points de certaines courbes (dites elliptiques).

# Cryptographie avec les courbes elliptiques

Question : est-ce qu'on peut faire de l'arithmétique avec d'autres objets que les nombres?

Oui! On peut additionner les points de certaines courbes (dites elliptiques).



(N. Koblitz, V. Miller, 1985)

# Cryptographie avec les courbes elliptiques

Question : est-ce qu'on peut faire de l'arithmétique avec d'autres objets que les nombres?

Oui! On peut additionner les points de certaines courbes (dites elliptiques).



(N. Koblitz, V. Miller, 1985)

Avantages : plus rapide, nécessite moins de mémoire d'ordinateur.

## Premier exemple : pyramide

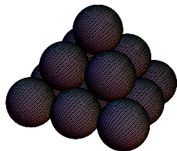
Problème : on a une pyramide de boules...





## Premier exemple : pyramide

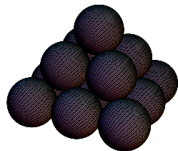
Problème : on a une pyramide de boules...



qui s'écrase...

## Premier exemple : pyramide

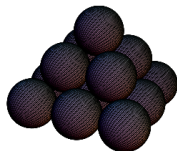
Problème : on a une pyramide de boules...



qui s'écrase... Peut-on arranger les boules dans un carré?

## Premier exemple : pyramide

Problème : on a une pyramide de boules...



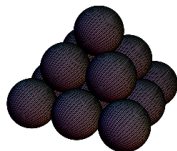
qui s'écrase... Peut-on arranger les boules dans un carré?

Si  $x$  est la hauteur de la pyramide et  $y$  est la longueur d'un côté du carré, on doit avoir:

$$y^2 = 1 + 2^2 + 3^2 + \dots + x^2 = \frac{x(x+1)(2x+1)}{6}.$$

## Premier exemple : pyramide

Problème : on a une pyramide de boules...



qui s'écrase... Peut-on arranger les boules dans un carré?

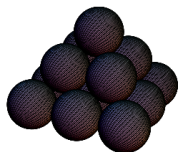
Si  $x$  est la hauteur de la pyramide et  $y$  est la longueur d'un côté du carré, on doit avoir:

$$y^2 = 1 + 2^2 + 3^2 + \dots + x^2 = \frac{x(x+1)(2x+1)}{6}.$$

Les seuls solutions entières sont (1, 1) et

## Premier exemple : pyramide

Problème : on a une pyramide de boules...



qui s'écrase... Peut-on arranger les boules dans un carré?

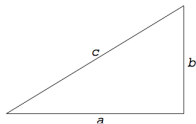
Si  $x$  est la hauteur de la pyramide et  $y$  est la longueur d'un côté du carré, on doit avoir:

$$y^2 = 1 + 2^2 + 3^2 + \dots + x^2 = \frac{x(x+1)(2x+1)}{6}.$$

Les seules solutions entières sont  $(1, 1)$  et  $(24, 70)$ .

## Deuxième exemple : triangle

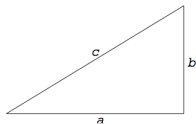
Problème : trouver tous les entiers  $n$  tels qu'il existe un triangle rectangle d'aire  $n$



dont tous les côtés sont des nombres rationnels.

## Deuxième exemple : triangle

Problème : trouver tous les entiers  $n$  tels qu'il existe un triangle rectangle d'aire  $n$

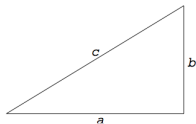


dont tous les côtés sont des nombres rationnels.

On appelle un tel entier  $n$  un nombre **congruent**.

## Deuxième exemple : triangle

Problème : trouver tous les entiers  $n$  tels qu'il existe un triangle rectangle d'aire  $n$



dont tous les côtés sont des nombres rationnels.

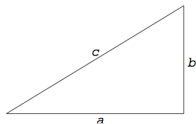
On appelle un tel entier  $n$  un nombre **congruent**.

Exemple :  $a = \frac{20}{3}$ ,  $b = \frac{3}{2}$ ,  $c = \frac{41}{6}$  et  $n = 5$ .



## Deuxième exemple : triangle

Problème : trouver tous les entiers  $n$  tels qu'il existe un triangle rectangle d'aire  $n$



dont tous les côtés sont des nombres rationnels.

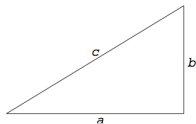
On appelle un tel entier  $n$  un nombre **congruent**.

Exemple :  $a = \frac{20}{3}$ ,  $b = \frac{3}{2}$ ,  $c = \frac{41}{6}$  et  $n = 5$ .

Fait:  $n$  est congruent si et seulement si l'équation  $y^2 = x^3 - n^2x$  admet d'autres solutions rationnelles que

## Deuxième exemple : triangle

Problème : trouver tous les entiers  $n$  tels qu'il existe un triangle rectangle d'aire  $n$



dont tous les côtés sont des nombres rationnels.

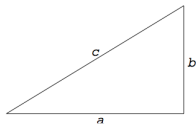
On appelle un tel entier  $n$  un nombre **congruent**.

Exemple :  $a = \frac{20}{3}$ ,  $b = \frac{3}{2}$ ,  $c = \frac{41}{6}$  et  $n = 5$ .

Fait:  $n$  est congruent si et seulement si l'équation  $y^2 = x^3 - n^2x$  admet d'autres solutions rationnelles que  $(0, 0)$ ,  $(n, 0)$ ,  $(-n, 0)$ .

## Deuxième exemple : triangle

Problème : trouver tous les entiers  $n$  tels qu'il existe un triangle rectangle d'aire  $n$



dont tous les côtés sont des nombres rationnels.

On appelle un tel entier  $n$  un nombre **congruent**.

Exemple :  $a = \frac{20}{3}$ ,  $b = \frac{3}{2}$ ,  $c = \frac{41}{6}$  et  $n = 5$ .

Fait:  $n$  est congruent si et seulement si l'équation  $y^2 = x^3 - n^2x$  admet d'autres solutions rationnelles que  $(0, 0)$ ,  $(n, 0)$ ,  $(-n, 0)$ .

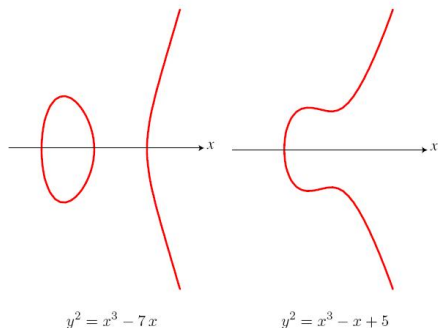
Conjecturalement, c'est le cas pour  $n \equiv 5, 6$  ou  $7 \pmod{8}$ .

# Courbes elliptiques

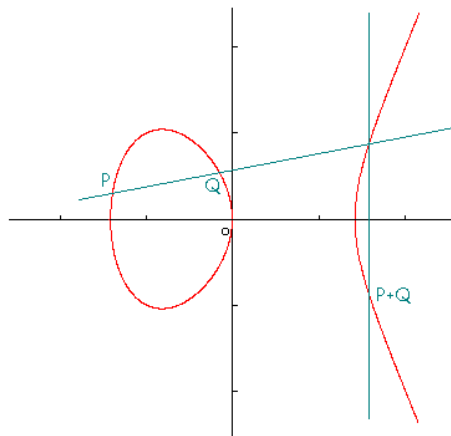
Une **courbe elliptique** est une courbe plane donnée par une équation

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

où  $a, b$  sont des nombres entiers (ou rationnels),  $4a^3 + 27b^2 \neq 0$  :



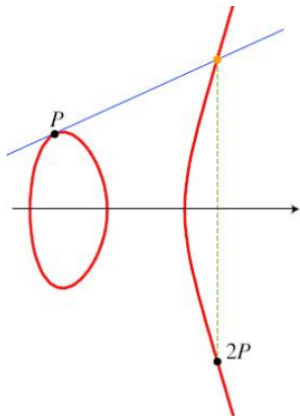
## La somme des points



Courbe elliptique et opération sur cette courbe

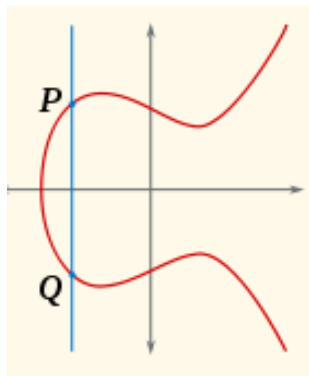
Si  $P, Q$  sont deux points de  $E$ , la droite qui les joint intersecte  $E$  en troisième point  $R$ . La somme  $P + Q$  et le point symétrique à  $R$  par rapport à l'axe des abscisses.

Si  $P = Q...$



On prend la droite tangente.

## Le point à l'infini



On dit que la droite qui joint  $P$  et  $Q$  intersecte  $E$  «à l'infini». La somme  $P + Q$  est alors le point «à l'infini»  $O_E$ .

## Et modulo $p$

- ▶ On prend  $p$  un nombre premier et  $a, b$  des nombres entiers tels que  $p$  ne divise pas  $4a^3 + 27b^2$ .



## Et modulo $p$

- ▶ On prend  $p$  un nombre premier et  $a, b$  des nombres entiers tels que  $p$  ne divise pas  $4a^3 + 27b^2$ .
- ▶ Un **point « modulo  $p$ »** est donné par  $x, y$  avec

$$y^2 - (x^3 + ax + b) \equiv 0 \pmod{p}, 0 \leq x < p, 0 \leq y < p.$$

## Et modulo $p$

- ▶ On prend  $p$  un nombre premier et  $a, b$  des nombres entiers tels que  $p$  ne divise pas  $4a^3 + 27b^2$ .
- ▶ Un **point « modulo  $p$ »** est donné par  $x, y$  avec

$$y^2 - (x^3 + ax + b) \equiv 0 \pmod{p}, 0 \leq x < p, 0 \leq y < p.$$

- ▶ On peut aussi faire la somme des points « modulo  $p$ ».

## Et modulo $p$

- ▶ On prend  $p$  un nombre premier et  $a, b$  des nombres entiers tels que  $p$  ne divise pas  $4a^3 + 27b^2$ .
- ▶ Un **point « modulo  $p$ »** est donné par  $x, y$  avec

$$y^2 - (x^3 + ax + b) \equiv 0 \pmod{p}, 0 \leq x < p, 0 \leq y < p.$$

- ▶ On peut aussi faire la somme des points « modulo  $p$ ».

## Exemple

▶  $p = 5, E : y^2 = x^3 - x + 1;$

## Exemple

- ▶  $p = 5, E : y^2 = x^3 - x + 1;$
- ▶  $P = (1, 1), Q = (-2, 0)$

## Exemple

- ▶  $p = 5$ ,  $E : y^2 = x^3 - x + 1$ ;
- ▶  $P = (1, 1)$ ,  $Q = (-2, 0)$ .
- ▶ La droite qui joint  $P$  et  $Q$  :  $y = 2(x + 2)$  (pour  $x = 1$  on a  $2 \cdot 3 = 6 \equiv 1 \pmod{5}$ ).
- ▶ Le troisième point d'intersection :  $4(x + 2)^2 = x^3 - x + 1$ , on trouve

## Exemple

- ▶  $p = 5$ ,  $E : y^2 = x^3 - x + 1$ ;
- ▶  $P = (1, 1)$ ,  $Q = (-2, 0)$ .
- ▶ La droite qui joint  $P$  et  $Q$  :  $y = 2(x + 2)$  (pour  $x = 1$  on a  $2 \cdot 3 = 6 \equiv 1 \pmod{5}$ ).
- ▶ Le troisième point d'intersection :  $4(x + 2)^2 = x^3 - x + 1$ , on trouve  $x = 0$ ,  $y = 1$ .
- ▶  $P + Q =$

## Exemple

- ▶  $p = 5$ ,  $E : y^2 = x^3 - x + 1$ ;
- ▶  $P = (1, 1)$ ,  $Q = (-2, 0)$ .
- ▶ La droite qui joint  $P$  et  $Q$  :  $y = 2(x + 2)$  (pour  $x = 1$  on a  $2 \cdot 3 = 6 \equiv 1 \pmod{5}$ ).
- ▶ Le troisième point d'intersection :  $4(x + 2)^2 = x^3 - x + 1$ , on trouve  $x = 0$ ,  $y = 1$ .
- ▶  $P + Q = (0, -1)$ .



## Un avantage

- ▶ Le nombre  $N$  des points de  $E$  modulo  $p$  vérifie :

$$p + 1 - 2\sqrt{p} < N < p + 1 + 2\sqrt{p}$$

(c'est le théorème de Hasse)  
et varie si l'on change la courbe  $E$ .

- ▶ Quand on fait l'arithmétique « modulo  $pq$  » (comme dans le système RSA), le nombre d'entiers (restes modulo  $pq$ ) est fixe!  
On a plus de flexibilité avec les courbes elliptiques.

## Exemple: système ElGamal avec les courbes elliptiques



- ▶ On choisit  $p$  un premier,  $E$  une courbe elliptique  $y^2 = x^3 + ax + b$  et un point  $P$  de  $E$  (modulo  $p$ ).

## Exemple: système ElGamal avec les courbes elliptiques



- ▶ On choisit  $p$  un premier,  $E$  une courbe elliptique  $y^2 = x^3 + ax + b$  et un point  $P$  de  $E$  (modulo  $p$ ).
- ▶ Bob choisit sa clé privée  $s$  et calcule modulo  $p$  la somme  $B = sP = P + P + \dots + P$  ( $s$  fois).

- ▶ Les données publiques sont  $p, E, P, B$ , la clé privée est  $s$ .

- ▶ Les données publiques sont  $p, E, P, B$ , la clé privée est  $s$ .
- ▶ Alice représente son «message» comme un point  $M$  de  $E$ .

- ▶ Les données publiques sont  $p, E, P, B$ , la clé privée est  $s$ .
- ▶ Alice représente son «message» comme un point  $M$  de  $E$ .
- ▶ Chiffrement : Alice choisit un entier  $k$  et calcule  $Q = kP, R = M + kB$ .

- ▶ Les données publiques sont  $p, E, P, B$ , la clé privée est  $s$ .
- ▶ Alice représente son «message» comme un point  $M$  de  $E$ .
- ▶ Chiffrement : Alice choisit un entier  $k$  et calcule  $Q = kP, R = M + kB$ .
- ▶ Déchiffrement  $R - sQ$ .

- ▶ Les données publiques sont  $p, E, P, B$ , la clé privée est  $s$ .
- ▶ Alice représente son «message» comme un point  $M$  de  $E$ .
- ▶ Chiffrement : Alice choisit un entier  $k$  et calcule  $Q = kP, R = M + kB$ .
- ▶ Déchiffrement  $R - sQ$ .
- ▶ Ça marche!

$$R - sQ = M + kB - s(kP) = M + k(sP) - ksP = M + ksP - ksP = M.$$



# Récapitulatif

Paramètres :  $p$  un nombre premier,  $E$  une courbe elliptique.

# Récapitulatif

Paramètres :  $p$  un nombre premier,  $E$  une courbe elliptique.  
Données publiques  $p, E, P, B$ .

# Récapitulatif

Paramètres :  $p$  un nombre premier,  $E$  une courbe elliptique.  
Données publiques  $p, E, P, B$ . **Clé privée de Bob** :  $s$ .

## Récapitulatif

Paramètres :  $p$  un nombre premier,  $E$  une courbe elliptique.  
Données publiques  $p, E, P, B$ . Clé privée de Bob :  $s$ .



## Récapitulatif

Paramètres :  $p$  un nombre premier,  $E$  une courbe elliptique.  
Données publiques  $p, E, P, B$ . Clé privée de Bob :  $s$ .

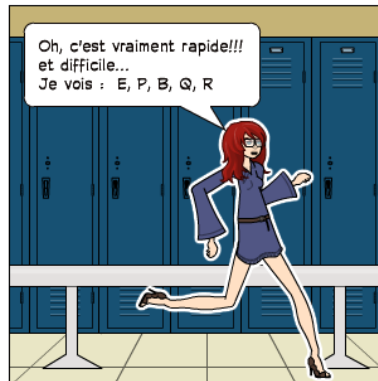


## Récapitulatif

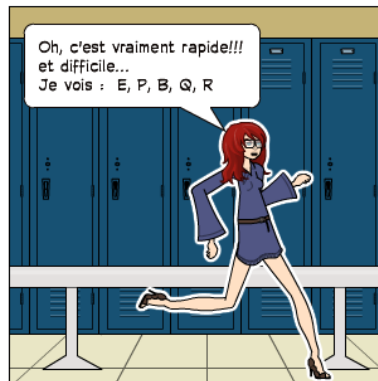
Paramètres :  $p$  un nombre premier,  $E$  une courbe elliptique.  
Données publiques  $p, E, P, B$ . Clé privée de Bob :  $s$ .



# La sécurité du système



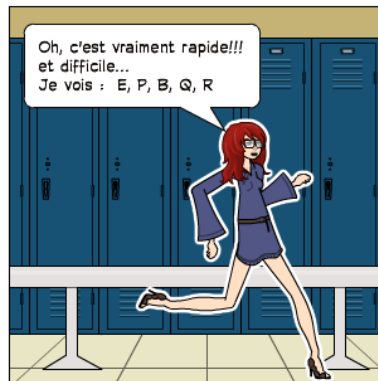
## La sécurité du système



- ▶ On connaît  $P, B$  (modulo  $N$ ), comment trouver  $s$  tel que  $P = sB$  (problème de **logarithme discret**)?



## La sécurité du système



- ▶ On connaît  $P, B$  (modulo  $N$ ), comment trouver  $s$  tel que  $P = sB$  (problème de **logarithme discret**)? C'est un problème très difficile techniquement!!!

# Problème de factorisation

- ▶ On dispose d'un entier  $N$ . **Problème** : trouver un (ou des) facteurs de  $N$ .

# Problème de factorisation

- ▶ On dispose d'un entier  $N$ . **Problème** : trouver un (ou des) facteurs de  $N$ .
- ▶ Rappel : dans l'algorithme RSA on a  $N = pq$ . Si l'on peut trouver  $p$  et  $q$ , alors il est facile de déterminer la clé privée.

# Méthodes élémentaires

- ▶ Tester tous les entiers  $2 \leq d \leq \sqrt{N}$ ...

# Méthodes élémentaires

- ▶ Tester tous les entiers  $2 \leq d \leq \sqrt{N}$ ...
- ▶ Rappel (petit théorème de Fermat) : si  $p$  est premier, alors  $p$  divise  $a^{p-1} - 1$ ,

# Méthodes élémentaires

- ▶ Tester tous les entiers  $2 \leq d \leq \sqrt{N}$ ...
- ▶ Rappel (petit théorème de Fermat) : si  $p$  est premier, alors  $p$  divise  $a^{p-1} - 1$ , plus généralement,  $p$  divise  $a^{(p-1)m} - 1$  pour tout entier  $m$ .

# Méthodes élémentaires

- ▶ Tester tous les entiers  $2 \leq d \leq \sqrt{N}$ ...
- ▶ Rappel (petit théorème de Fermat) : si  $p$  est premier, alors  $p$  divise  $a^{p-1} - 1$ , plus généralement,  $p$  divise  $a^{(p-1)m} - 1$  pour tout entier  $m$ .  
Conséquence : si  $p|N$ , alors on peut trouver  $p$  comme diviseur commun de  $N$  et  $a^{(p-1)m} - 1$

# Méthodes élémentaires

- ▶ Tester tous les entiers  $2 \leq d \leq \sqrt{N}$ ...
- ▶ Rappel (petit théorème de Fermat) : si  $p$  est premier, alors  $p$  divise  $a^{p-1} - 1$ , plus généralement,  $p$  divise  $a^{(p-1)m} - 1$  pour tout entier  $m$ .  
Conséquence : si  $p|N$ , alors on peut trouver  $p$  comme diviseur commun de  $N$  et  $a^{(p-1)m} - 1$  (il est «facile» de calculer les diviseurs communs).



- ▶ **Une difficulté** : on ne connaît pas  $p$ , comment trouver  $(p - 1)m$ ?

- ▶ **Une difficulté** : on ne connaît pas  $p$ , comment trouver  $(p - 1)m$ ?
- ▶ Réponse : on espère que les facteurs premiers de  $p - 1$  ne sont pas trop grands, on a alors  $(p - 1) | B!$  où

$$B! = 1 \cdot 2 \cdot 3 \dots \cdot (B - 1) \cdot B.$$

pour un entier  $B$  (pas trop grand) i.e.  $(p - 1)m = B!$

- ▶ **Une difficulté** : on ne connaît pas  $p$ , comment trouver  $(p - 1)m$ ?
- ▶ Réponse : on espère que les facteurs premiers de  $p - 1$  ne sont pas trop grands, on a alors  $(p - 1) | B!$  où

$$B! = 1 \cdot 2 \cdot 3 \dots \cdot (B - 1) \cdot B.$$

pour un entier  $B$  (pas trop grand) i.e.  $(p - 1)m = B!$

- ▶ Exemple :  $p = 19$ ,  $p - 1 = 18 = 2 \cdot 3 \cdot 3$ , on a donc

$$p - 1 | 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6.$$

## Algorithme $p - 1$ de Pollard

- ▶ On fixe un très grand entier  $M$  et  $a$  tel que  $a < N$ . On calcule, pour tout  $i = 1, 2, 3, \dots, M$  :

$$b = a^{i!} - 1 \pmod{N}$$

## Algorithme $p - 1$ de Pollard

- ▶ On fixe un très grand entier  $M$  et  $a$  tel que  $a < N$ . On calcule, pour tout  $i = 1, 2, 3, \dots, M$  :

$$b = a^{i!} - 1 \pmod{N}$$

- ▶ et on cherche des diviseurs communs de  $b$  et  $N$ .

## Algorithme $p - 1$ de Pollard

- ▶ On fixe un très grand entier  $M$  et  $a$  tel que  $a < N$ . On calcule, pour tout  $i = 1, 2, 3, \dots, M$  :

$$b = a^{i!} - 1 \pmod{N}$$

- ▶ et on cherche des diviseurs communs de  $b$  et  $N$ .



## Avec les courbes elliptiques

- ▶ L'algorithme **ECM** ("Elliptic Curve Method") a été introduit par H. Lenstra dans les années 1980 et développé par R. Brent, P. Montgomery et autres.

## Avec les courbes elliptiques

- ▶ L'algorithme **ECM** ("Elliptic Curve Method") a été introduit par H. Lenstra dans les années 1980 et développé par R. Brent, P. Montgomery et autres.
- ▶ Un des derniers facteurs trouvés : le facteur suivant de  $12^{284} + 1$



## Avec les courbes elliptiques

- ▶ L'algorithme **ECM** ("Elliptic Curve Method") a été introduit par H. Lenstra dans les années 1980 et développé par R. Brent, P. Montgomery et autres.
- ▶ Un des derniers facteurs trouvés : le facteur suivant de  $12^{284} + 1$

26721194531973848954767772351114152203083577206813943149484875628623309473

(B. Dodson, 26 Octobre 2014.)

- ▶ Rappel : si  $E$  est une courbe elliptique, et si  $P, Q$  sont deux points de  $E$ , pour trouver le point  $P + Q$ , il faut
  1. trouver l'équation de la droite  $L$  qui joint  $P$  et  $Q$ ,
  2. trouver le troisième point d'intersection  $R$  de  $L$  et  $E$ ,
  3. trouver le point symétrique à  $R$  par rapport à l'axe des abscisses.

- ▶ Rappel : si  $E$  est une courbe elliptique, et si  $P, Q$  sont deux points de  $E$ , pour trouver le point  $P + Q$ , il faut
  1. trouver l'équation de la droite  $L$  qui joint  $P$  et  $Q$ ,
  2. trouver le troisième point d'intersection  $R$  de  $L$  et  $E$ ,
  3. trouver le point symétrique à  $R$  par rapport à l'axe des abscisses.
- ▶ Exemple :  $y^2 = x^3 - 8x + 1$ ,

- ▶ Rappel : si  $E$  est une courbe elliptique, et si  $P, Q$  sont deux points de  $E$ , pour trouver le point  $P + Q$ , il faut
  1. trouver l'équation de la droite  $L$  qui joint  $P$  et  $Q$ ,
  2. trouver le troisième point d'intersection  $R$  de  $L$  et  $E$ ,
  3. trouver le point symétrique à  $R$  par rapport à l'axe des abscisses.
- ▶ Exemple :  $y^2 = x^3 - 8x + 1$ ,  $P : x = 0, y = 1$ ,  
 $Q : x = 3, y = 2$ . La droite  $L$  :

- ▶ Rappel : si  $E$  est une courbe elliptique, et si  $P, Q$  sont deux points de  $E$ , pour trouver le point  $P + Q$ , il faut
  1. trouver l'équation de la droite  $L$  qui joint  $P$  et  $Q$ ,
  2. trouver le troisième point d'intersection  $R$  de  $L$  et  $E$ ,
  3. trouver le point symétrique à  $R$  par rapport à l'axe des abscisses.
- ▶ Exemple :  $y^2 = x^3 - 8x + 1$ ,  $P : x = 0, y = 1$ ,  
 $Q : x = 3, y = 2$ . La droite  $L : y = \frac{1}{3}x + 1\dots$

- ▶ Rappel : si  $E$  est une courbe elliptique, et si  $P, Q$  sont deux points de  $E$ , pour trouver le point  $P + Q$ , il faut
  1. trouver l'équation de la droite  $L$  qui joint  $P$  et  $Q$ ,
  2. trouver le troisième point d'intersection  $R$  de  $L$  et  $E$ ,
  3. trouver le point symétrique à  $R$  par rapport à l'axe des abscisses.
- ▶ Exemple :  $y^2 = x^3 - 8x + 1$ ,  $P : x = 0, y = 1$ ,  
 $Q : x = 3, y = 2$ . La droite  $L : y = \frac{1}{3}x + 1\dots$   
**Observation** : on doit inverser 3!

- ▶ Rappel : si  $E$  est une courbe elliptique, et si  $P, Q$  sont deux points de  $E$ , pour trouver le point  $P + Q$ , il faut
  1. trouver l'équation de la droite  $L$  qui joint  $P$  et  $Q$ ,
  2. trouver le troisième point d'intersection  $R$  de  $L$  et  $E$ ,
  3. trouver le point symétrique à  $R$  par rapport à l'axe des abscisses.
- ▶ Exemple :  $y^2 = x^3 - 8x + 1$ ,  $P : x = 0, y = 1$ ,  
 $Q : x = 3, y = 2$ . La droite  $L : y = \frac{1}{3}x + 1\dots$   
**Observation** : on doit inverser 3!
- ▶ Utilisation : si l'on regarde une courbe elliptique « modulo »  $N$ , on peut trouver les diviseurs de  $N$  parmi les dénominateurs.

# ECM





# ECM



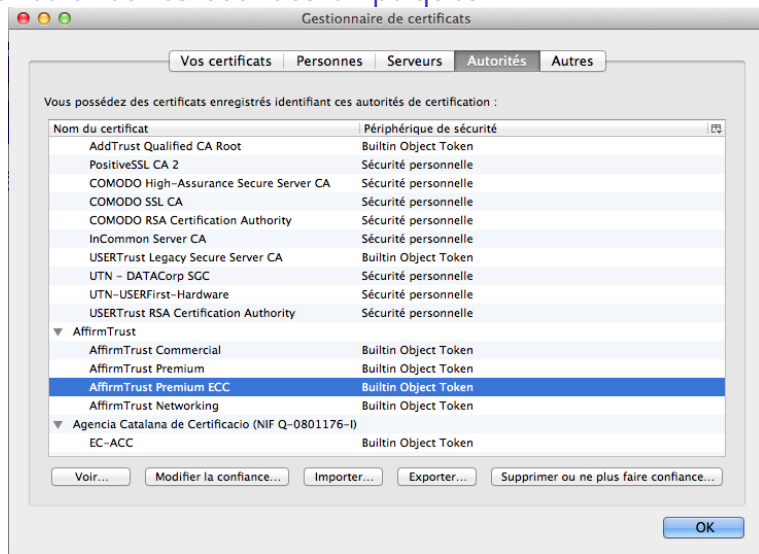
- ▶ On prend une courbe elliptique  $E$  et un point  $P$  de  $E$ .
- ▶ On fixe un très grand entier  $M$ . On calcule modulo  $N$ , pour tout  $i = 1, 2, 3, \dots, M$  :  $i!P = P + P + \dots + P$  ( $i!$  fois).

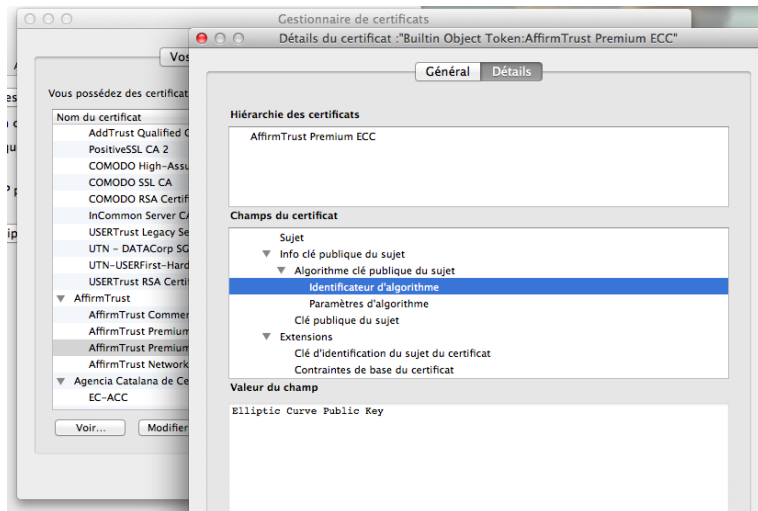
# ECM

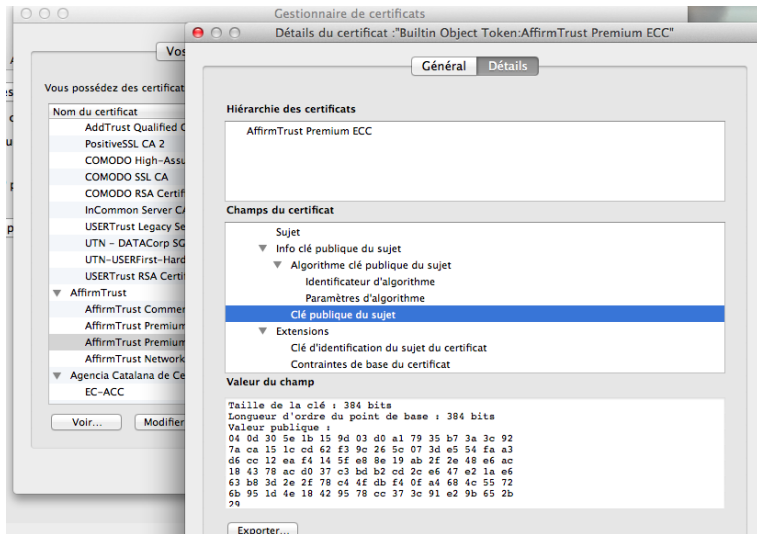


- ▶ On prend une courbe elliptique  $E$  et un point  $P$  de  $E$ .
- ▶ On fixe un très grand entier  $M$ . On calcule modulo  $N$ , pour tout  $i = 1, 2, 3, \dots, M$  :  $i!P = P + P + \dots + P$  ( $i!$  fois).
- ▶ On trouve des diviseurs communs de  $N$  quand on n'arrive pas à effectuer une division.

# Réalité avec les courbes elliptiques







NSA Suite B Cryptography ... x +

https://www.nsa.gov/ia/programs/suiteb\_cryptography/ Rechercher

Les plus visités ▾ Débuter avec Fire... Apple Disney Les Echos Yahoo! YouTube Lesson 1: Home ... France Info - direct Graduate Studies ... Tpa

NATIONAL SECURITY AGENCY  CENTRAL SECURITY SERVICE 

*Defending Our Nation. Securing The Future.*

HOME ABOUT NSA ACADEMIA BUSINESS CAREERS **INFORMATION ASSURANCE** RESEARCH PUBLIC INFORMATION CIVIL LIBERTIES

Home > Information Assurance > Programs > NSA Suite B Cryptography

## Suite B Cryptography

Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting National Security Systems (NSS). Suite B includes cryptographic algorithms for encryption, key exchange, digital signature, and hashing.

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Encryption	<a href="#">FIPS Pub 197</a>	128 bit keys for SECRET  256 bit keys for TOP SECRET

**Information Assurance**

- About IA at NSA
- IA Client and Partner Support
- IA News
- IA Events
- IA Mitigation Guidance
- IA Academic Outreach
- IA Business and Research
- IA Programs
  - Commercial Solutions for Classified Program
  - Global Information Grid
  - High Assurance Platform

Merci de votre attention!<sup>1</sup>



<sup>1</sup>Je remercie Benjamin Smith et François Morain pour des références sur l'utilisation des courbes elliptiques

