Sorbonne université — 16 avril 2019

Hackers vs équations diophantiennes

Razvan Barbulescu et Sébastien Canard

Déroulé de l'exposé

- La cryptologie est notre futur (Sébastien)
- Equations diophantiennes (Razvan)
- L'importance des accouplements en cryptologie (Sébastien)
- Et la recherche dans tout cela ? (Razvan)

Voici Alice…

- Elle travaille principalement avec deux collaborateurs
- Elle utilise un service de SMS signé pour valider ses contrats
- Elle utilise un cloud public pour stocker et partager ses documents sensibles
- La compagnie où elle travaille investit pour résister aux attaques cybernétiques

- Mais pas à n'importe quel prix…

Confidentialité des données de son entreprise

- Assurer la confidentialité d'une information signifie que cette information n'est jamais fourni aux entités non autorisées
- Les services utilisés par Alice doivent manipuler des données sensibles
  - documents administratifs
  - données sensibles relatives à la concurrence
- Comme un tel service peut-il redonner confiance à ses clients ?
  - par exemple en n'ayant pas accès aux données…
  - …tout en assurant la même qualité de service

Protection de la vie privée d'Alice

- En Europe, ces services doivent désormais se plier à la nouvelle Réglementation Générale sur la Protection des Données (RGPD)
  - l'utilisation des données doit être claire
  - transparence des données collectées
  - la collecte de données doit être pertinente
  - précision des données collectées
  - droit à l'oubli
- Comme un tel service peut-il redonner confiance à ses clients ?
  - vérifier la sensibilité des données, superviser le transfert de données
  - faire une analyse de risque
  - fournir des solutions pour protéger la vie privée des consommateurs…
  - … tout en maintenant la même qualité de service

Est-ce que la cryptographie peut être utile ?

- Objectifs historiques
  - confidentialité (le seul pendant très longtemps)
  - authentification des individus/données
  - intégrité
  - non répudiation
- Nouveaux objectifs
  - fournir des outils permettant de répondre à des besoins contradictoires
  - ceci inclut la protection des données

- Possédons-nous les bons outils pour aider Alice ?

Voici les collaborateurs d'Alice

- Alice travaille avec Bob et Eve
  - Alice vit à Paris
  - Bob vit à London
  - Eve vit à New York
- Ils utilisent What's app pour communiquer ensemble
  - mais ils échangent des données sensibles
  - et ils ne font pas confiance dans What's app
- Ils peuvent utiliser un système de chiffrement pour ça
  - mais ils doivent être les seuls à pouvoir déchiffrer
  - la cryptographie repose sur la possession d'une clé de déchiffrement
  - Alice, Bob et Eve doivent partager la même clé

Diffie-Hellman : utile pour Alice et Bob

a

A = [a]P

B = [b]P

b

K = [a]B = [ab]P

K = [b]A = [ab]P

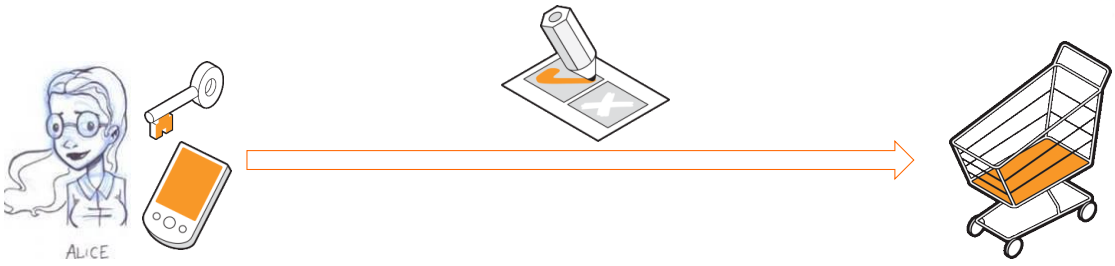
Ils obtiennent la même clé

- [a]P signifie P+P+…+P (a fois)
- A partir de [a]P, il est difficile de retrouver a

Mais si on rajoute Eve…

Comment pouvons-nous le faire simplement ?

Signature numérique d'un SMS

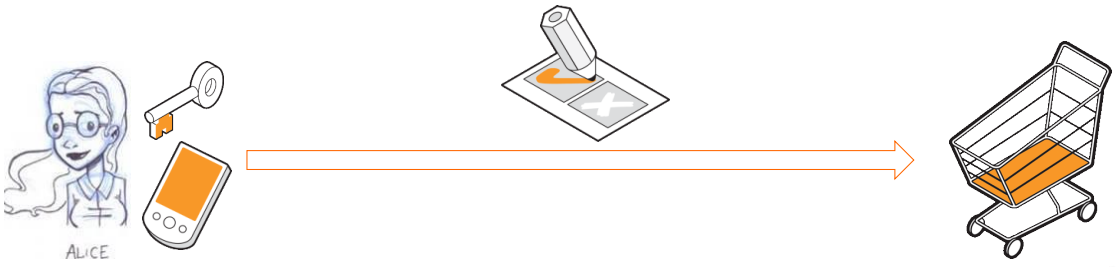


- Signature numérique
  - difficile à falsifier sans la connaissance d'une clé secrète
  - équivalente juridique d'une signature manuscrite

- La longueur standard d'un SMS est de 160 caractères de 7 bits

  $\Rightarrow$ 1120 bits
- Standard de signature RSA
  - taille d'une signature RSA : 2048 bits!

Signature numérique d'un SMS



- Signature numérique
  - difficile à falsifier sans la connaissance d'une clé secrète
  - équivalente juridique d'une signature manuscrite
- La longueur standard d'un SMS est de 160 caractères de 7 bits

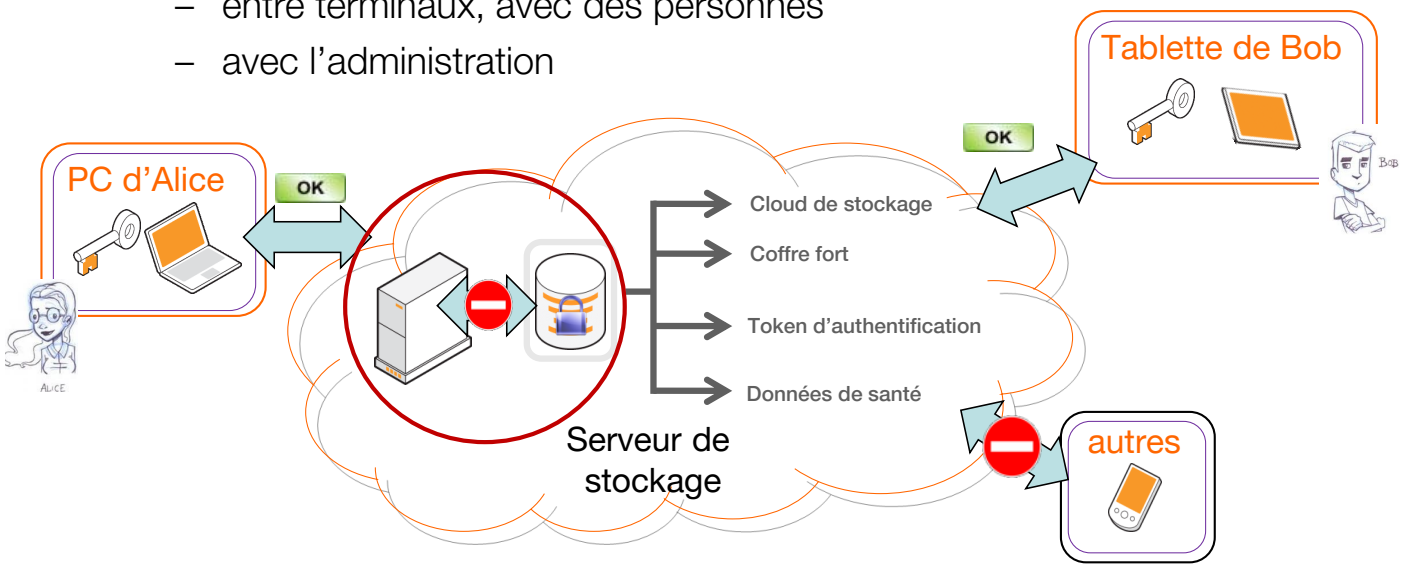
  ⇒ 1120 bits
- Standard de signature RSA
  - taille d'une signature RSA : 2048 bits!

SIGNATURE TROP LONGUE !!!

Comment obtenir une signature plus courte ?

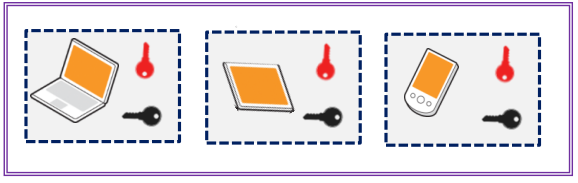
Stockage et partage de données sensibles

- Stockage de données
  - documents confidentiels, documents administratifs
  - coffres forts, cloud de storage, …
- Confidentialité des données ⇒ chiffrement
- Partage de données
  - entre terminaux, avec des personnes
  - avec l'administration



Solutions possibles pour partager des données

PARTAGE DE LA CLE



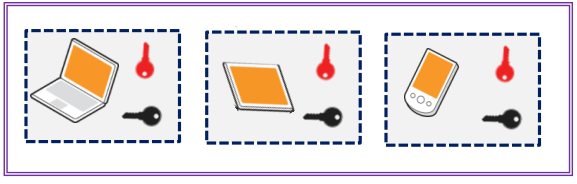
- Trou de sécurité si la clé est compromise
- Une telle compromission nécessite de mettre à jour toutes les clés

DUPLICATION DE LA DONNEE

- Bonne sécurité, peu de flexibilité
- Problème de l'augmentation de l'espace de stockage
- Dynamique des droits d'accès complexe

Solutions possibles pour partager des données

PARTAGE DE LA CLE



- Trou de sécurité si la clé est compromise
- Une telle compromission nécessite de mettre à jour toutes les clés

DUPLICATION DE LA DONNEE

- Bonne sécurité, peu de flexibilité
- Problème de l'augmentation de l'espace de stockage
- Dynamique des droits d'accès complexe

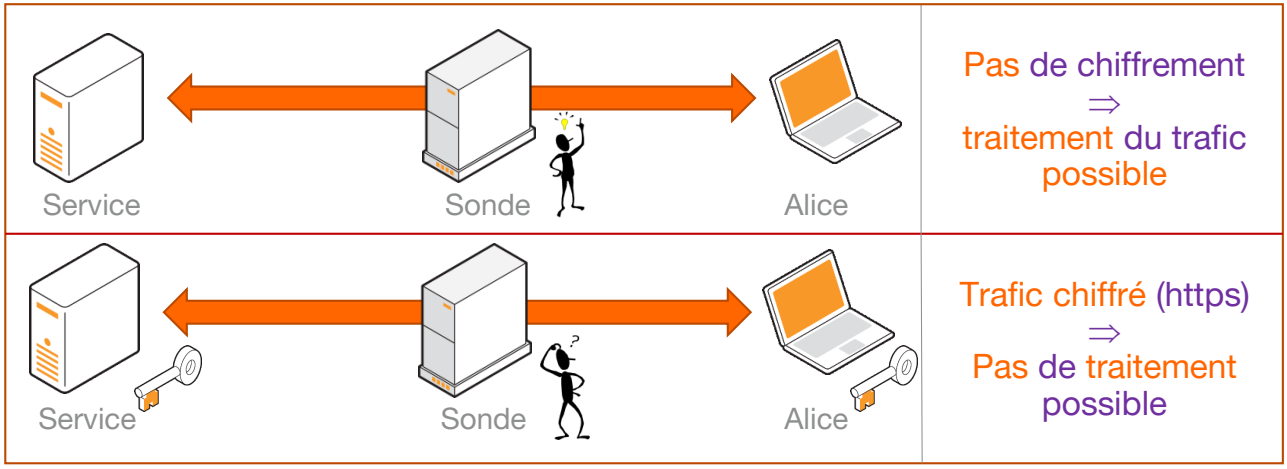
PAS ASSEZ SUR OU FLEXIBLE!!!

Quelle solution sûre et flexible peut-on utiliser ?

Le chiffrement est notre futur…

- Le groupe de travail IETF HTTPbis en charge des spécifications de la nouvelle génération HTTP 2.0 pour l'accès à Internet propose que le chiffrement soit proposé par défaut
- D'après une étude de l'Institut Ponemon, à laquelle participent Thales et Vormetric Data Security, le trafic chiffré Internet mondial a augmenté de 15% en 2005 et de plus de 40% en 2015. La proportion de trafic Internet chiffré devrait atteindre les 80% d'ici à 2020
- Les services Internet majeurs passent tous au chiffrement de bout-en-bout, comme par exemple What's app, Google, etc.
- La Commission Européenne, via son programme Horizon H2020, et notamment ses appels à proposition dans le domaine de la cybersecurité, prône pour plus de vie privée sur le trafic des individus
- …

Confidentialité ne rime pas avec sécurité



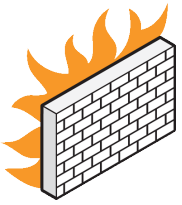
Avec les standards actuels, il est difficile de choisir entre confidentialité des données and utilité/sécurité !


01net › Actualités › Sécurité

Pourquoi les antivirus et les proxy SSL rendent le web moins sûr

⊙ 03/03/2017 à 08h11 Mis à jour le 03/03/2017 à 10h07

Le problème : intrusion via un trafic chiffré



- Intrusion Detection Systems
- Cas d'usage simple basé sur une injection SQL

- Requête légitime

```
http://localhost:9080/login?username=seb&password=1234
```

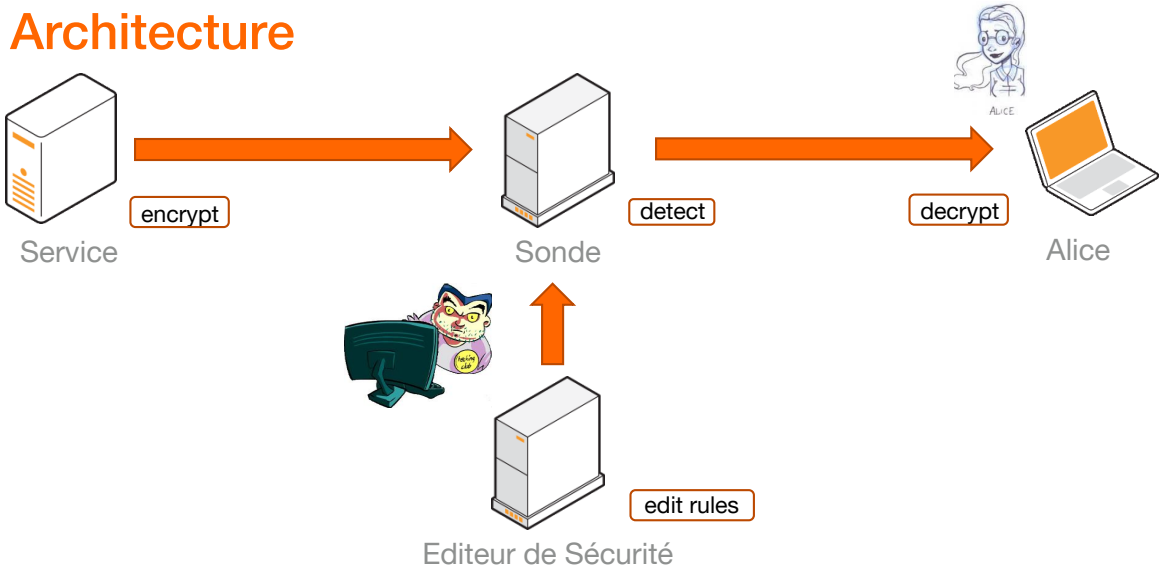
- Injection SQL ⇒ accès au service uniquement à partir du login

```
http://localhost:9080/login?username=seb&password='1111' or 'a' = 'a'
```

- Requête chiffrée

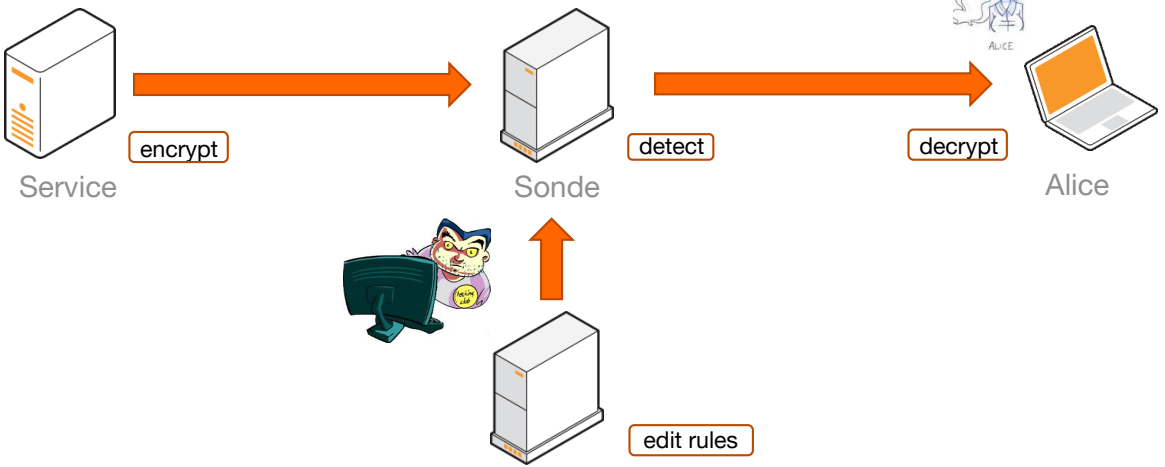
```
https://localhost:9080/login?DaeDFreffOJFldD[[|lmEZUjdLk6KL1kl{d
```

Architecture



- Deep Packet Inspection sur le contenu du paquet
- Utilisation de règles de détection pour analyser le contenu du trafic
  - Détection basée sur le comportement : fait sur les méta données
  - Détection basée sur les signatures : reconnaissance d'un pattern
- Solution actuelle: attaque de l'homme du milieu!

Architecture



- Deep Packet Inspection sur le contenu du paquet
- Utilisation de règles de détection pour analyser le contenu du trafic
  - Détection basée sur le comportement : fait sur les méta données
  - Détection basée sur les signatures : reconnaissance d'un pattern
- Solution actuelle: attaque de l'homme du milieu!

PAS ASSEZ SUR !!!

Comment obtenir une solution sécurisée ?

Est-ce la fin… (?)

- La cryptographie historique ne semble pas suffisamment puissante
- Il nous faudrait un outil mathématique puissant pour résoudre nos problèmes
- C'est là qu'intervient Diophante d'Alexandrie…

Déroulé de l'exposé

- La cryptologie est notre futur (Sébastien)
- Equations diophantiennes (Razvan)
- L'importance des accouplements en cryptologie (Sébastien)
- Et la recherche dans tout cela ? (Razvan)

Algorithme d'Euclide

Exemple

- entrée : $a = 1892$, $b = 144$
- sortie : $\text{pgcd}(a, b)$

On écrit deux équations triviales :

$$\begin{aligned} 1 \cdot a + 0 \cdot b &= 1892 \quad (0) \\ 0 \cdot a + 1 \cdot b &= 144 \quad (1) \end{aligned}$$

On combine de manière répétée les deux dernières équations pour rendre le membre droit non-négatif aussi petit que possible :

$$\begin{aligned} 1 \cdot a + (-13) \cdot b &= 20 \quad (2) := (0) - 13 \cdot (1) \\ (-7) \cdot a + 92 \cdot b &= 4 \quad (3) := (1) - 7 \cdot (2) \\ 36 \cdot a + (-473) \cdot b &= 0 \quad (4) := (2) - 5 \cdot (3) \end{aligned}$$

Theorem (Bezout)

Pour toute paire d'entiers a et b il existe $u, v \in \mathbb{Z}$ tels que

$$u \cdot a + v \cdot b = \text{pgcd}(a, b).$$

Algorithme d'Euclide

Exemple

- entrée : $a = 1892$, $b = 144$
- sortie : $\text{pgcd}(a, b)$

On écrit deux équations triviales :

$$\begin{aligned} 1 \cdot a + 0 \cdot b &= 1892 \quad (0) \\ 0 \cdot a + 1 \cdot b &= 144 \quad (1) \end{aligned}$$

On combine de manière répétée les deux dernières équations pour rendre le membre droit non-négatif aussi petit que possible :

$$\begin{aligned} 1 \cdot a + (-13) \cdot b &= 20 \quad (2) := (0) - 13 \cdot (1) \\ (-7) \cdot a + 92 \cdot b &= 4 \quad (3) := (1) - 7 \cdot (2) \\ 36 \cdot a + (-473) \cdot b &= 0 \quad (4) := (2) - 5 \cdot (3) \end{aligned}$$

Theorem (Bezout)

Pour toute paire d'entiers a et b il existe $u, v \in \mathbb{Z}$ tels que

$$u \cdot a + v \cdot b = \text{pgcd}(a, b).$$

Algorithme d'Euclide pour les polynômes

Exemple

- entrée : $a = x^5 + 2 * x^4 + 5x^3 + 8x^2 + 7x + 4,\ b = x^3 + 2x^2 + 2x + 1$
- sortie : $\text{pgcd}(a, b)$

On écrit deux équations triviales :

$$\begin{aligned} 1 \cdot a + 0 \cdot b &= x^5 + 2x^4 + 5x^3 + 8x^2 + 7x + 4 \quad (0) \\ 0 \cdot a + 1 \cdot b &= x^3 + 2x^2 + 2x + 1 \quad (1) \end{aligned}$$

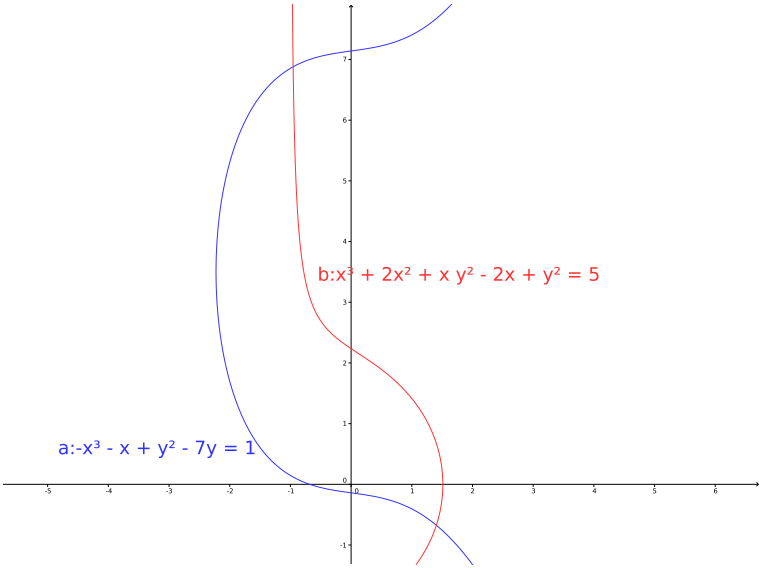
On combine de manière répétée les deux dernières équations pour rendre le membre droit de degré aussi petit que possible :

$$\begin{aligned} 1 \cdot a + (-x^2 + 3) \cdot b &= x^2 + x + 1 \quad (2) := (0) - (x^2 + 3) \cdot (1) \\ (-x + 1) \cdot a + (x^2 + 4) \cdot b &= 0 \quad (3) := (1) - (x + 1) \cdot (2) \end{aligned}$$

Theorem (Bezout)

Soient k un corps et $a, b \in k[x]$. Alors il existe $u, v \in k[x]$ tels que $u \cdot a + v \cdot b = \text{pgcd}(a, b)$.

Intersection de deux courbes



Application du théorème de Bezout pour $a(x, y)$ et $b(x, y)$

- $k = \mathbb{Q}(x)$
- $a = y^2 - 7y - (x^3 + x + 1)$ et $b = (x + 1)y^2 + (x^3 + 2x^2 - 2x - 5)$
- Th Bezout : $u \cdot a + v \cdot b =$
  $1/49x^8+4/49x^7+10/49x^6+12/49x5+50/49x^4+131/49x^3-24/49x^2-7x-229/49$
  où $u = xy/7 + \cdots$ et $v = -y/7 + \cdots$.

Construction à la règle et le compas

L'outillage du jardinier

Labergement-Foigney (Côte d'Or) 2012 - outillage Gallo-Romain I^{er} siècle

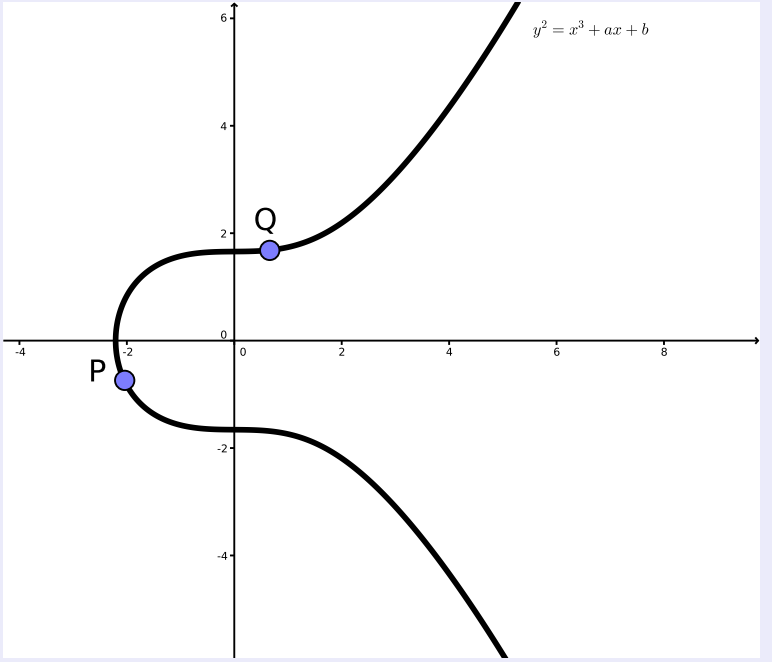
Langage moderne

Th de Bezout géométrique : une courbe de degrés m et n se coupent en au plus $m \times n$ points ou elle ont une composante infinie commune.

- une droite coupe un cercle en au plus 2 points
- une droite qui coupe une cubique dans 2 points la coupe aussi dans un 3e (on compte les multiplicités)
- Th. de Cayley-Bacharach : toutes les cubiques qui coupent une cubique fixée dans 8 points, la coupent nécessairement dans le même 9e point.

Construction aux courbes cubiques

Newton : loi d'addition sur une courbe elliptique

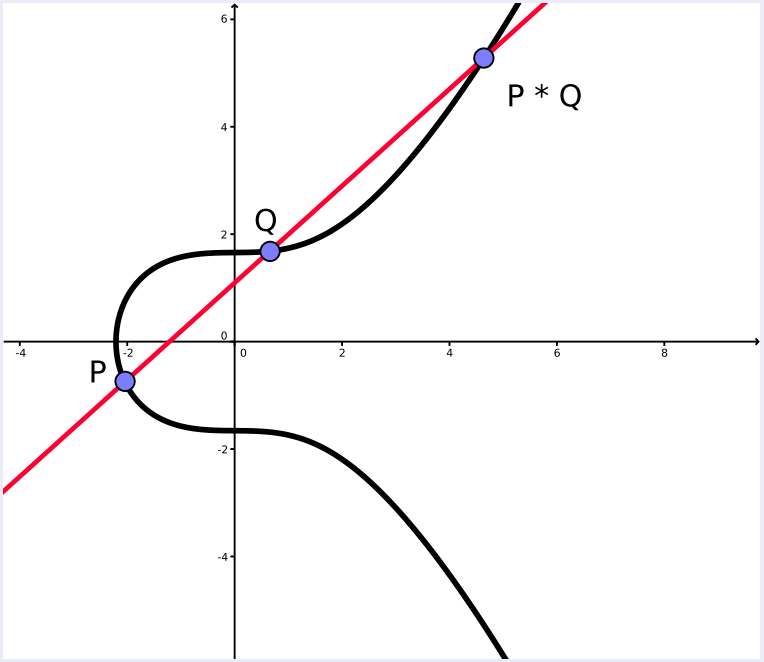


$k = \mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$ avec $p \geq 5$ premier

- $(\{(x, y) \in k : y^2 = x^3 + ax + b\} \bigcup \{\infty\}, +)$ est un groupe abélien ;
- formules : quotients de polynômes (rapides à calculer).

Construction aux courbes cubiques

Newton : loi d'addition sur une courbe elliptique

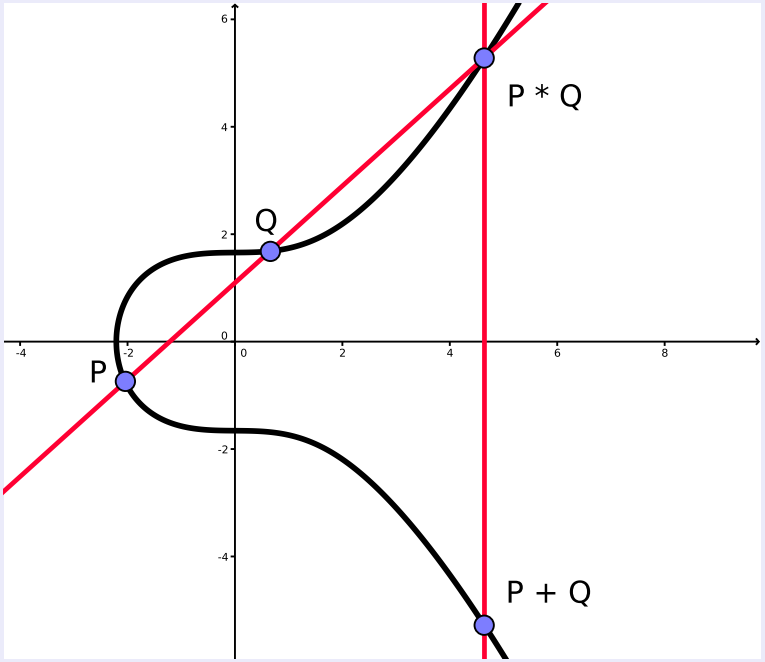


$k = \mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$ avec $p \geq 5$ premier

- $(\{(x, y) \in k : y^2 = x^3 + ax + b\} \bigcup \{\infty\}, +)$ est un groupe abélien ;
- formules : quotients de polynômes (rapides à calculer).

Construction aux courbes cubiques

Newton : loi d'addition sur une courbe elliptique



$k = \mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$ avec $p \geq 5$ premier

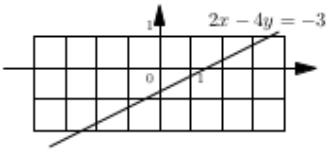
- $(\{(x, y) \in k : y^2 = x^3 + ax + b\} \bigcup \{\infty\}, +)$ est un groupe abélien ;
- formules : quotients de polynômes (rapides à calculer).

Équations diophantiennes

Definition

Une équation diophantienne est donnée par un polynôme $P(x, y)$. La résoudre consiste à trouver toutes les paires avec $x, y \in \mathbb{Z}$ (resp. $x, y \in \mathbb{Q}$) telles que $P(x, y) = 0$.

Étant donnés $a, b, c \in \mathbb{Z}$, trouver $x, y \in \mathbb{Z}$ tels que $x \cdot a + y \cdot b = c$



On résout en appliquant l'algorithme d'Euclide.

Équations diophantiennes de degré supérieur

- équation de Pell généralisée : $ax^2 + by^2 = c$ avec $x, y \in \mathbb{Z}$
- points rationnels des courbes elliptiques : $y^2 = x^2 + ax + b$ avec $x, y \in \mathbb{Q}$

Mordell, Weil et Faltings

Theorem (Mordell-Weil 1928)

Toute courbe elliptique à coefficients rationnels (définie par $y^2 = x^3 + ax + b$ avec $a, b \in \mathbb{Q}$) admet un nombre finis de points rationnels $P_1, \ldots, P_n$ pour un certain n tels que tout autre point rationnel est de la forme

$$[a_1]P_1 + [a_2]P_2 + \cdots + [a_n]P_n,$$

pour certains $a_1, \ldots, a_n \in \mathbb{Z}$.

Theorem (Faltings 1983, cas particulier)

Toute courbe de la forme $y^2 = P(x)$ avec $\deg P = 2g + 1$ pour un $g \geq 2$, sans racines multiples, a un nombre fini de points rationnels.

Accouplements de Weil 1940

Definition

Soit E une courbe elliptique à coefficients dans un corps k. Soient n un entier et P un point à coefficients dans une extension de k tels que $[n]P = \mathcal{O}$, où $\mathcal{O}$ est l'élément neutre. Le couplage de Weil (restreint aux multiples de P) est l'application

$$\begin{array}{rccc} e: & \mathbb{Z}/n\mathbb{Z} \cdot P \times \mathbb{Z}/n\mathbb{Z} \cdot P & \to & \zeta_n^{\mathbb{Z}/n\mathbb{Z}} \\ & ([a]P, [b]P) & \mapsto & \zeta_n^{ab}, \end{array}$$

où ζ_n est une solution de l'équation $x^n = 1$ dans une extension de k, qui n'est pas équation de $x^{n'} = 1$ pour aucun $n' < n$.

Propriétés des accouplements de Weil

- bilinéarité : $e([a_1]P + [a_2]P, [b]P) = e([a_1 + a_2]P, [b][P])$
- nondégénération : si a est tel que pour tout b on a $e([a]P, [b]P) = 1$, alors $a = 0$
- arithmétique rapide : pour calculer $e([a]P, [b]P)$ on a besoin des coordonnées x et y des points $[a]P$ et $[b]P$ et non pas de a et b.
- inversion difficile : étant donnés b et c, le calcul de a tel que $e([a]P, [b]P) = \zeta_n^c$ a une grande complexité

Déroulé de l'exposé

- La cryptologie est notre futur (Sébastien)
- Equations diophantiennes (Razvan)
- L'importance des accouplements en cryptologie (Sébastien)
- Et la recherche dans tout cela ? (Razvan)

Vous vous rappelez d'Alice?

- Elle travaille principalement avec deux collaborateurs
- Elle utilise un service de SMS signé pour valider ses contrats
- Elle utilise un cloud public pour stocker et partager ses documents sensibles
- La compagnie où elle travaille investit pour résister aux attaques cybernétiques

- Mais pas à n'importe quel prix…

Maintenant, vous connaissez Diophante d'Alexandrie

Comment peut-il aider Alice ?

Commençons par les collaborateurs d'Alice

[a]P

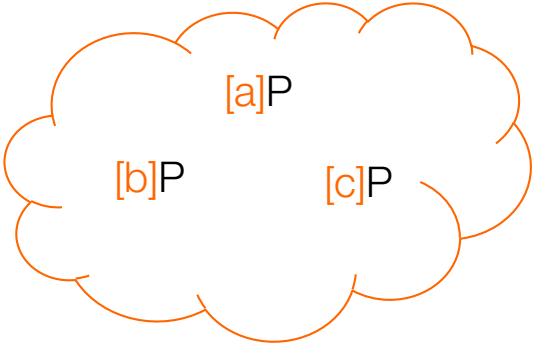
$e([b]P,[c]P)^a = e(P,P)^{abc}$

[c]P

$e([a]P,[b]P)^c = e(P,P)^{abc}$

[b]P

$e([a]P,[c]P)^b = e(P,P)^{abc}$



Commençons par les collaborateurs d'Alice

[a]P

$e([b]P,[c]P)^a = e(P,P)^{abc}$

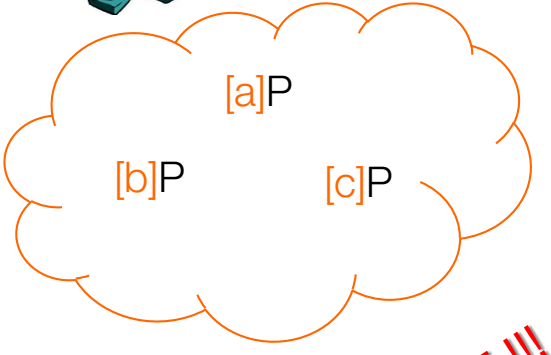
?

[c]P

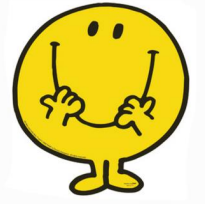
$e([a]P,[b]P)^c = e(P,P)^{abc}$

[b]P

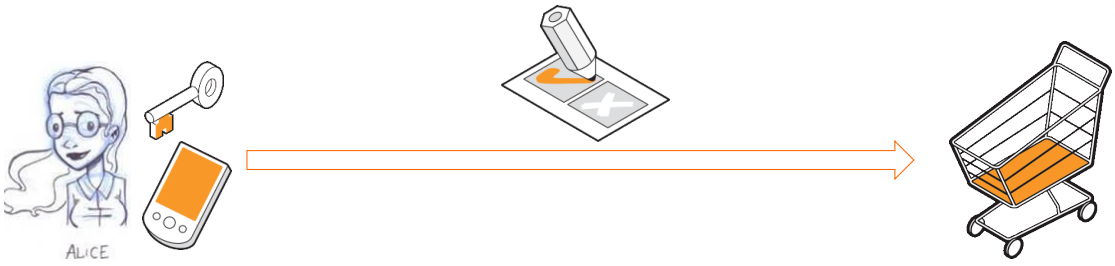
$e([a]P,[c]P)^b = e(P,P)^{abc}$



SOLUTION SIMPLE !!!



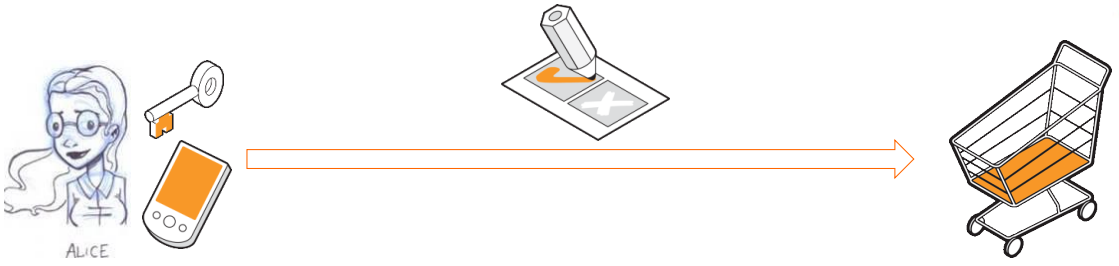
Et si Alice souhaite signer un SMS…



- Rappel : un SMS a une taille de 1120 bits

Taille de signature RSA	Taille d'une signature basée sur les accouplements
2048 bits	200 bits

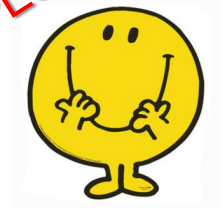
Et si Alice souhaite signer un SMS…



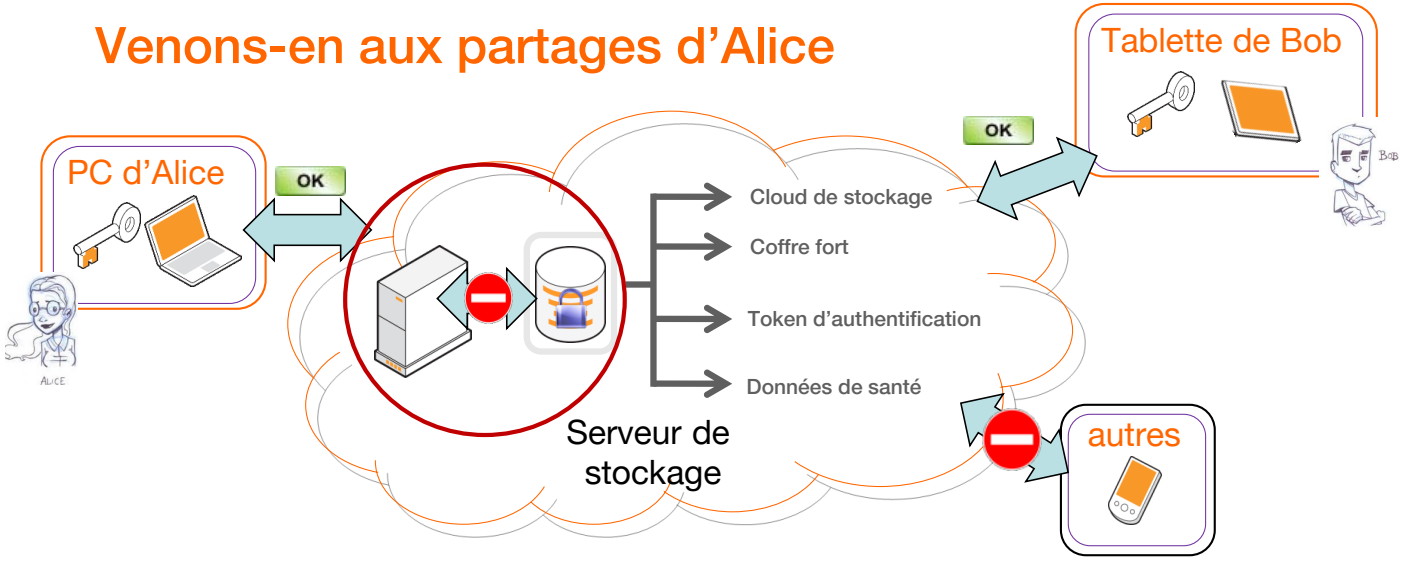
- Rappel : un SMS a une taille de 1120 bits

Taille de signature RSA	Taille d'une signature basée sur les accouplements
2048 bits	200 bits

BEAUCOUP PLUS PETIT !!!



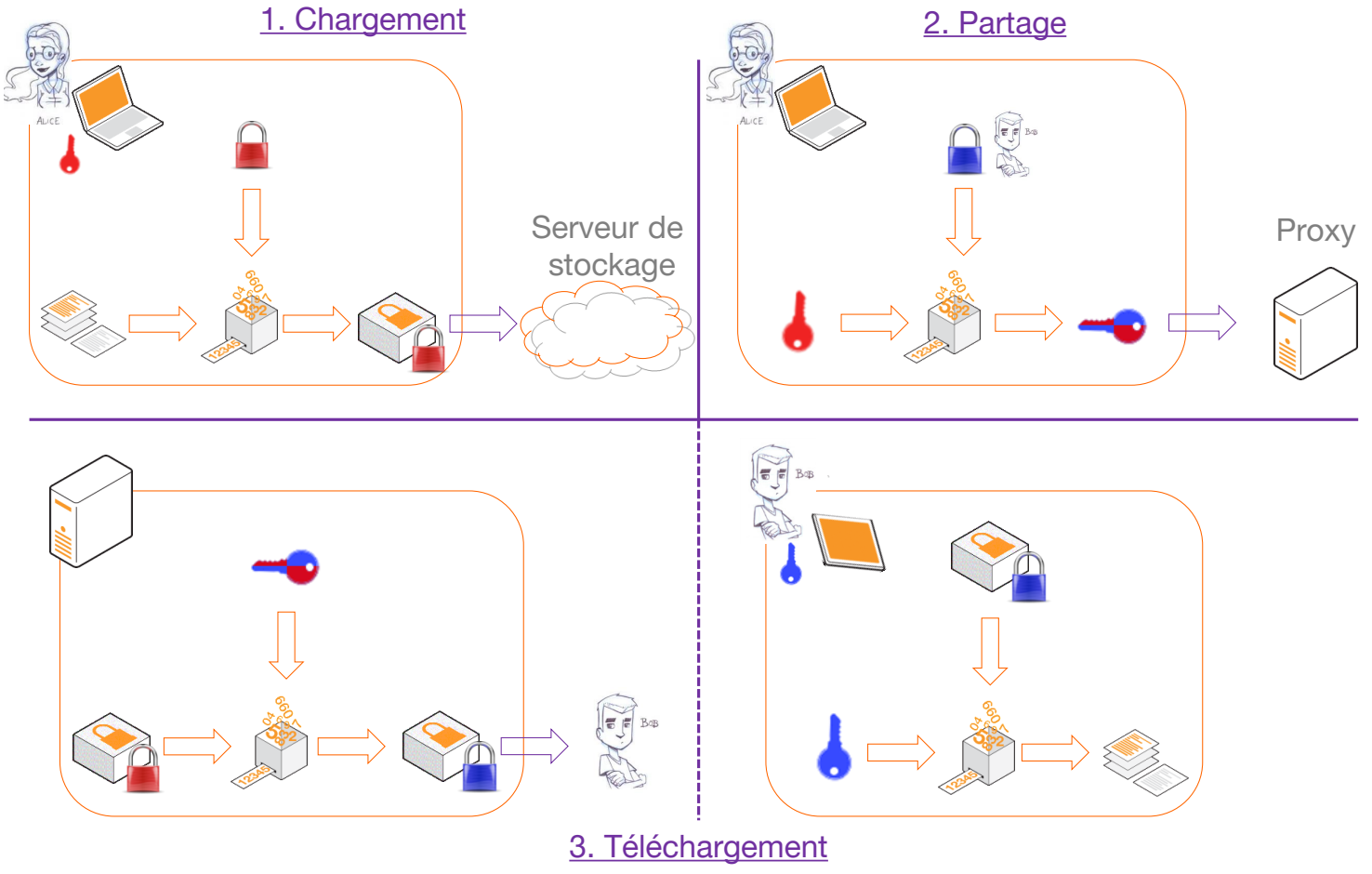
Venons-en aux partages d'Alice



- Transformation par le serveur de stockage d'un message chiffré pour Alice en le même message chiffré pour Bob
  - si Alice est d'accord
  - sans obtenir aucune connaissance sur les clés d'Alice ou Bob
  - sans obtenir aucune connaissance sur le message chiffré
- Utilisation d'une clé particulière dite de re-chiffrement

Chiffrement à clé publique : une clé publique pour chiffrer les données,, une clé privée pour déchiffrer la donnée

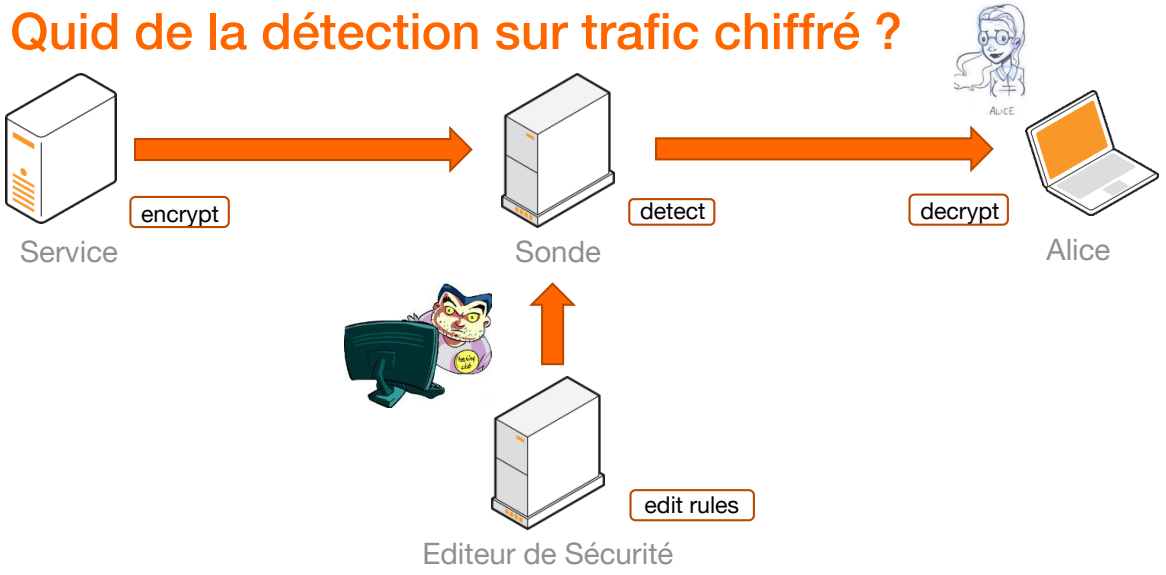
Notion de stockage aveugle



Propriétés obtenues

- La clé de déchiffrement n'est pas partagée
- Les données ne sont pas dupliquées sur les serveurs
- Alice n'est contactée qu'une seule fois pour la création de la clé de re-chiffrement
- Le service de stockage est aveugle des données manipulées
- Pas besoin de connaître a priori les personnes avec qui Alice va partager ses données
- Les accouplements permettent des constructions sûres et efficaces

Quid de la détection sur trafic chiffré ?



- Exemple de trafic

```
http://localhost:9080/login?username=seb&password=‘1111' or ‘a‘ = ‘a‘
```

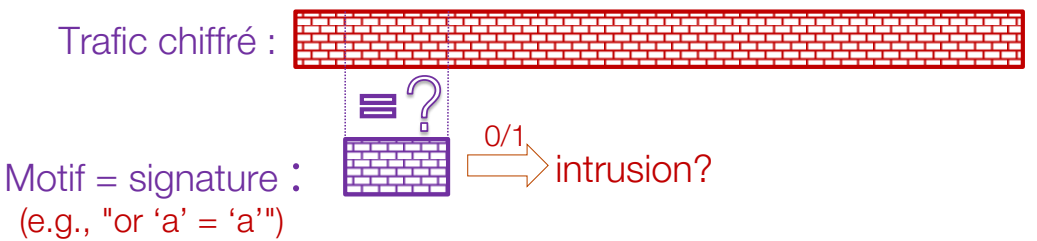
- Exemple de règle

```
alert tcp any any $->$ HOMENET PORTHTTP (msg: "SQL Injection Attempt - or a=a"; content: "GET"; httpmethod; uricontent: “or ‘a‘ = ‘a‘”; nocase; classtype:web-application-attack; sid:3000001; rev:1;)
```

Exigences sur le schéma de chiffrement

- Est-il possible de chercher un message spécifique dans un texte ?
  - filtrage par motif (cas simple) ou expression régulière (cas complexe)
  - comment faire si le texte est chiffré ?
- Nous avons besoin d'un schéma de chiffrement avec des fonctionnalités de recherche
  - Motif w recherché (Editeur de Sécurité) : Trap(w)
  - Trafic t chiffré (Service) : Encrypt(t)

  } Tester si w=t ou non



De la théorie à la pratique

1. Génération des règles (Editeur de sécurité)

- Clé privée x, Clé publique X = $[x]P_1$
- Pour tout motif w, calculer le token T=[x]F(w)

2. Chiffrement du trafic (Service)

- Pour chaque partie t du trafic, calculer
  - C = $[s]P_1$ pour un aléa s
  - U = e([s]X,F(t))

3. Détection (Sonde)

- A partir d'un token T, calculer
  - e(C,T) = e([s]P1,[x]F(w)) = e([sx]P1,F(w)) = e([s]X,F(w))
- Qui est égal à U ssi t = w !

De la théorie à la pratique

- BlindIDS est une implémentation de ce mécanisme
  - capacité de traiter 75% des règles
  - 700 µs de détection par token
- Utilisable dès maintenant dans des environnements fermés
- Un passage en standardisation est nécessaire pour une déploiement plus massif
- L'histoire est à suivre…

Quand Alice rencontre Diophante d'Alexandrie, les hackers sont défaits

Et nous n'allons pas nous arrêter là…

Déroulé de l'exposé

- La cryptologie est notre futur (Sébastien)
- Equations diophantiennes (Razvan)
- L'importance des accouplements en cryptologie (Sébastien)
- Et la recherche dans tout cela ? (Razvan)

Degré de plongement

Definition

Le degré de plongement de la courbe E à coefficients dans $\mathbb{F}_q$ par rapport à l'entier r est $\min\{k \in \mathbb{N}^* : q^k - 1 \equiv 0 \pmod{r}\}$

Theorem

Le degré de plongement est égal à
$\min\{k \in \mathbb{N} : \mathbb{F}_{q^k}$ *possède une racine r-ième primitive*$\}$

Ni trop chaud ni trop froid

Soit une courbe elliptique est définie sur $\mathbb{F}_q$ avec q tout juste assez grand pour assurer la sécurité (sur le côté de la courbe).

- Si k est trop petit le corps $\mathbb{F}_{q^k}$ est petit est sa sécurité n'est pas garantie.
- Si k est trop grand, le corps $\mathbb{F}_{q^k}$ est grand et les calculs de l'accouplement sont trop longs.

Il est nécessaire de construire des courbes de degré de plongement donné.

La construction des courbes adaptées aux couplages

Choix de q et r

Étant donné un entier k, on construit une courbe elliptique de degré de plongement k (et de taille $\log_2 q$ donné) en deux étapes :

1. on trouve q, r et t satisfaisant
   1.1 $\Phi_k(t-1) \equiv 0 \pmod{r}$
   1.2 $q + 1 - t \equiv 0 \pmod{r}$
   1.3 $\exists y,\ 4q = Dy^2 + t^2$
2. on applique la méthode à multiplication complexe pour construire une courbe elliptique E de degré de plongement k. La complexité est $O(h_D^{2+\epsilon})$ où h_D est le nombre de classes de $\mathbb{Q}(\sqrt{D})$ (dans le pire des cas, $h_D \simeq \sqrt{D}$). On obtient une courbe E telle que :
   - $\mathbb{F}_q$ est le corps des coefficients
   - E a $q + 1 - t$ points
   - E a un sousgroupe d'ordre r.

La famille MNT

Équations CM

1. $\Phi_k(t-1) \equiv 0 \pmod{r}$
2. $q+1-t \equiv 0 \pmod{r}$
3. $\exists y,\ 4q = Dy^2 + t^2$

Exemple quand $k = 3$ et $\varphi(k) = 2$

La famille MNT

Équations CM

1. ~~$\Phi_k(t-1) = 0 \pmod{r}$~~
2. $q + 1 - t \equiv 0 \pmod{r}$
3. $\exists y,\ 4q = Dy^2 + t^2$

Exemple quand $k = 3$ et $\varphi(k) = 2$

1. on pose $r = \Phi_k(t-1)$, qui satisfait (1)

La famille MNT

Équations CM

1. ~~$\Phi_k(t-1) = 0 \pmod{r}$~~
2. ~~$q+1-t = 0 \pmod{r}$~~
3. $\exists y,\ 4q = Dy^2 + t^2$

Exemple quand $k = 3$ et $\varphi(k) = 2$

1. on pose $r = \Phi_k(t-1)$, qui satisfait (1)
2. on pose $q = r + t - 1$, qui satisfait (2)

La famille MNT

Équations CM

1. ~~$\Phi_k(t-1) \equiv 0 \pmod{r}$~~
2. ~~$q+1-t \equiv 0 \pmod{r}$~~
3. équation de Pell généralisée (e.g. $X^2 - 3Dy^2 = 24$, où $X = 6x \pm 3$)

Exemple quand $k = 3$ et $\varphi(k) = 2$

1. on pose $r = \Phi_k(t-1)$, qui satisfait (1)
2. on pose $q = r + t - 1$, qui satisfait (2)
3. on substitue q par $q(t)$ dans (3), c'est une équation diophantienne en y et t (éq. de Pell généralisée)

La famille MNT

Équations CM

1. ~~$\Phi_k(t-1) \equiv 0 \pmod{r}$~~
2. ~~$q+1-t \equiv 0 \pmod{r}$~~
3. ~~équation de Pell généralisée (e.g. $X^2 - 3Dy^2 = 24$, où $X = 6x \pm 3$)~~

Exemple quand $k = 3$ et $\varphi(k) = 2$

1. on pose $r = \Phi_k(t-1)$, qui satisfait (1)
2. on pose $q = r + t - 1$, qui satisfait (2)
3. on substitue q par $q(t)$ dans (3), c'est une équation diophantienne en y et t (éq. de Pell généralisée)
4. on résout l'équation de Pell généralisée et on obtient y et t, ce qui donne q

Niveau de sécurité

Utilisation

- Les compagnies qui offrent des services de sécurité (stockage dans le cloud, vote par internet etc) obtiennent la certification ANSSI (France) ou NIST (É.-U.).
- Les chercheurs et les ingénieurs règlent les systèmes cryptologiques au même niveau de sécurité, ce qui permet de comparer les performances.

Calcul du niveau

- $\log_2 S$ où S est le nombre de clés possibles ;
- $\log_2 S$ où S est le nombre d'opérations (d'un processeur d'ordinateur classique) en utilisant le meilleur algorithme connu.

Challenge RSA et records

Un point de vue pragmatique

- En 1990 la compagnie RSA security a lancé une compétition pour factoriser des entiers (des clés RSA).
- Les chercheurs du secteur publique participent, le record est 232 chiffres décimaux (768 bits).

Compétition	Prix	Statut	Date de factorisation	Par
RSA-576	USD 10 000	Factorisé	3 décembre 2003	J. Franke et al.
RSA-640	USD 20 000	Factorisé	2 novembre 2005	F. Bahr et al.
RSA-704	USD 30 000	Annulé	2 juillet 2012	Shi Bai, Emmanuel Thomé et Paul Zimmermann[1]
RSA-768	USD 50 000	Factorisé	15 janvier 2010	Divers organismes[2]
RSA-896	USD 75 000	Annulé	-	-
RSA-1024	USD 100 000	Annulé	-	-

Le travail des chercheurs

- nouveaux théorèmes ou conjectures
- nouveaux algorithmes implantés en langages de haut niveau (python, Magma)
- implémentation dans des langages de bas niveau (C, CUDA)
- calculs à grande échelle, e.g. pour RSA 768 les chercheurs ont utilisé 1000 coeurs pendant 2 ans.

Avancées récentes

Avancées

remarque mathématique	corps $\mathbb{F}_p$ affectés
substituer P dans $x^p - x = \prod(x - a)$ B. Gaudry Joux Thomé (2014)	$p = 2$ et 3 (interdits par ENISA)
choix de polynômes dans l'algorithme B. Gaudry Guillevic Morain (2015)	n pair ou divisible par 3
remplacer l'anneau $\mathbb{Z}$ par d'autres e.g. $\mathbb{Z}[i]$ B. Gaudry Kleinjung (2015) et Kim et B. (2016)	$p = P(u)$ où $\lvert P\rvert_\infty$ est petit, $3 \leq P \leq 20$

Conséquence en petite caractéristique

- Gap Diffie–Hellman problem: Given g^x and g^y for hidden x and y compute $g^{x \cdot y}$, given an oracle which allows solution of the Decision Diffie–Hellman problem.

Clearly the ability to solve the DLP will also give one the ability to solve the above three problems, but the converse is not known to hold in general (although it is in many systems widely believed to be the case).

Finite Field DLP

The discrete logarithm problem in finite fields (which we shall refer to simply as DLP), and hence the Diffie–Hellman problem, Decision Diffie–Hellman problem and gap Diffie–Hellman problem, is parametrized by the finite field $\mathbb{F}_{p^n}$ and the subgroup size q, which should be prime. In particular this means that q divides $p^n - 1$. To avoid "generic attacks" the value q should be at least 160 bits in length for legacy applications and at least 256 bits in length for new deployments.

For the case of small prime characteristic, i.e. $p = 2, 3$ there is new algorithm was presented in early 2013 by Joux [184] which runs in time $L(1/4 + o(1))$, for when the extension degree n is composite (which are of relevance to pairing based cryptography). This algorithm was quickly supplanted by an algorithm which runs in quasi-polynomial time by Barbulescu and others [26]. Also in 2013 a series of record breaking calculations were performed by a French team and a Irish team for characteristic two fields, resulting in the records of $\mathbb{F}_{2^{6120}}$ [137] and $\mathbb{F}_{2^{6168}}$ [182]. For characteristic three the record is $\mathbb{F}_{3^{582}}$ [332]. For prime values of n the best result is a discrete logarithm calculation in the field $\mathbb{F}_{2^{809}}$ [61]. All of these results make use of special modification to the function field sieve algorithm [9]. **In light of these results no system should be deployed relying on the hardness of the DLP in small characteristic fields.**

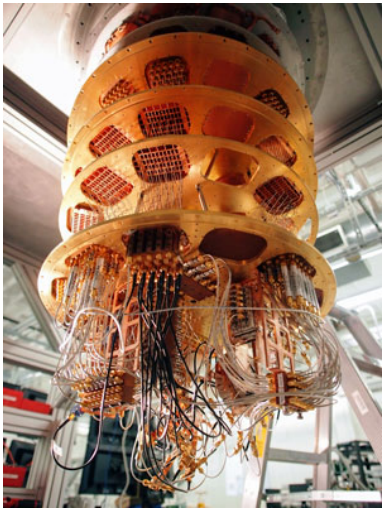
Conséquence si la caractéristique n'est pas petite

Conséquences sur les couplages

B. et Duquesne (2018, Journal of Cryptology) : les tailles des clés des accouplements utilisés en pratique doivent être augmentées entre 50% et 100%.

Ordinateur quantique

Google (72 qubits)



IBM (50 qubits)

Roetteler et al. 2017 (cité par ssl.com) : un éventuel ordinateur quantique de 2330 qubits (126 milliards de portes Tofolli) peut casser la cryptographie à base des courbes elliptiques et des accouplements de Weil au niveau de sécurité de 128 de bits.

Quand Alice rencontre Diophante d'Alexandrie, les hackers sont défaits

Questions ?

Références

1. N. Billerey et M. Rebolledo. Équations diophantiennes et courbes elliptques. Disponible en ligne à l'adresse `http://math.univ-bpclermont.fr/~billerey/Miscellaneous/mathsauvergne_NB_MR.pdf`

2. S. Canard. Cryptography for trust and data services. Disponible en ligne à l'adresse `http://confiance-numerique.clermont-universite.fr/SDTA-2014/slides/cryptography_for_trust_and_data_services.pdf`. 2014.

3. S. Galbraith. Mathematics of public key cryptography. Livre édité par Cambridge. 2012.