

Sécurité de l'information et Cryptographie

Sylvain Duquesne

Université Rennes 1, laboratoire de Mathématiques

21 juin 2012

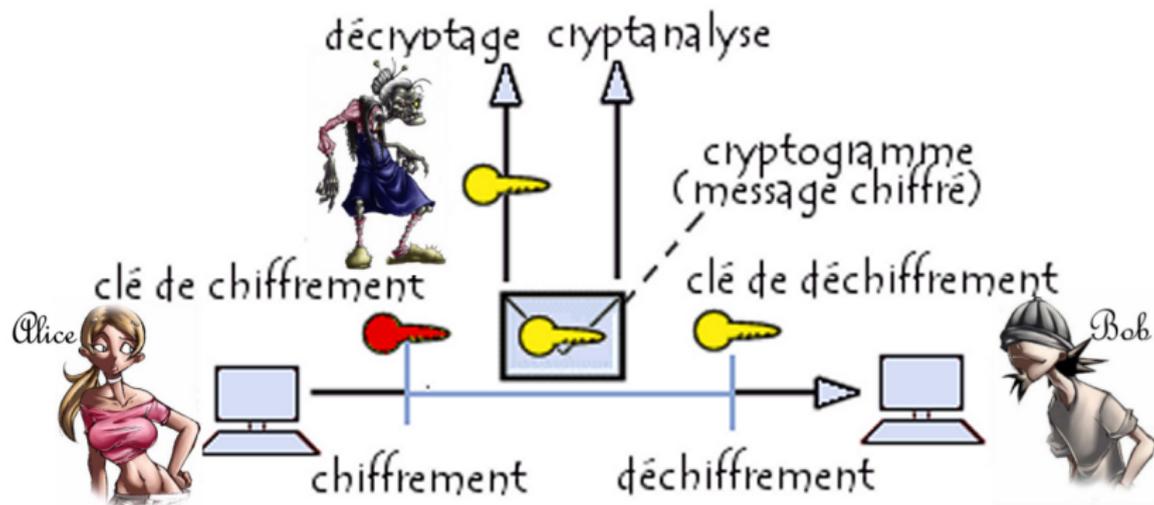
Journées MMS 2012, INSA Rennes



Qu'est ce que la cryptographie ?

cryptographie n. f.

Ensemble des principes, méthodes et techniques dont l'application assure le chiffrement et le déchiffrement des données, afin d'en préserver la confidentialité et l'authenticité.



Quelques repères historiques

Scytale : VIème siècle av JC, Grèce.

César : décalage de l'alphabet.

Par exemple de trois lettres vers la droite :

A T T A Q U E Z L E P A L A I S
D W W D T X H C O H S D O D L V

ou d'une lettre vers la gauche :

I B M W N T
H A L V M S

Enigma : 1939–45, Allemagne.



Enigma



Point commun à toutes ces méthodes : la méthode de chiffrage est secrète.

Inconvénient : elle n'est pas secrète pour tous ceux qui l'utilisent.

⇒ principes de Kerchoffs (19^{ème} siècle) dont :

la sécurité d'un système de chiffrement ne doit résider que dans la clé et non dans le procédé de chiffrement.

Démocratisation du secret.

La cryptographie à clé secrète (ou symétrique)

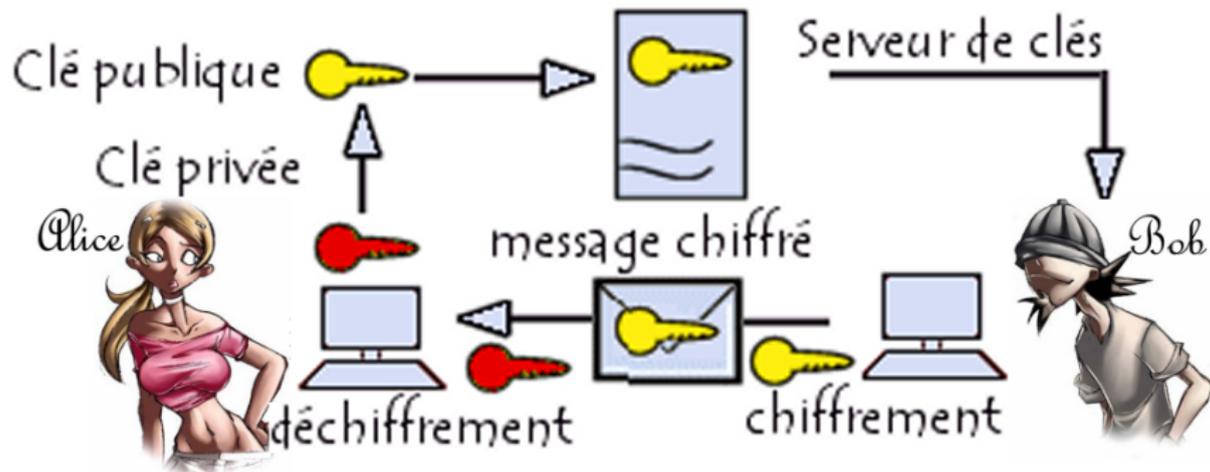


Les plus connus : DES, triple-DES, AES, masque jetable.

Inconvénients :

- il faut s'échanger la clé,
- il faut avoir une clé pour chaque correspondant.

La cryptographie à clé publique (ou asymétrique)



Principe introduit par Whitfield Diffie et Martin Hellman en 1976 (aussi introduit séparément par Ralph Merkle) utilisant une fonction à sens unique (**clé publique**) avec trappe (**clé privée**).

La cryptographie à clé publique (ou asymétrique)

⇒ permet de résoudre les problèmes de la cryptographie symétrique.

Les plus connus : RSA, DL, ECC, NTRU.

Inconvénient : 100 à 1000 fois plus lent.

En pratique on mélange les deux (SSL, SSH, PGP par exemple).



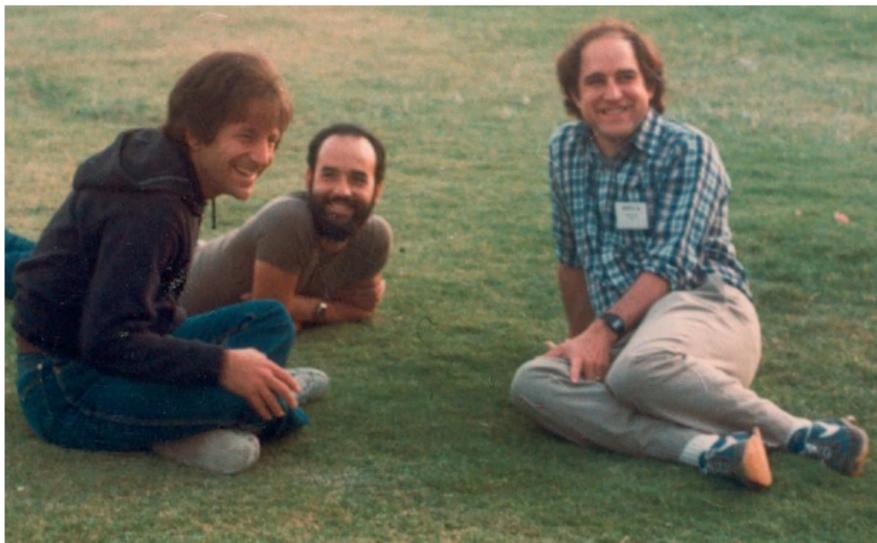
Whitfield Diffie

Les pères de la cryptographie à clé publique...



Martin Hellman

Système à clé publique introduit en 1977 très utilisé en pratique.



de gauche à droite : Adleman, Shamir et Rivest.

Il utilise le fait qu'il est difficile de factoriser un nombre.

Exemple : $2^{2^7} + 1 = 340282366920938463463374607431768211457 =$
 $59649589127497217 \times 5704689200685129054721$

Rappel : le calcul modulaire

a modulo b est le reste de la division de a par b .

- Un nombre est pair si il vaut 0 modulo 2.
- Nous sommes **jeudi**, 4^{ème} jour de la semaine. Si on veut savoir quel jour sera t'on dans 247 jours, on calcule $4+247$ modulo 7

$$251 = 35 \times 7 + 6, \text{ autrement écrit, } 250 \text{ modulo } 7 = 6.$$

On sera donc un **samedi**.

- Quand on fait du chiffrement de César, on travaille modulo 26 : si on veut decaler Y de 3 lettres, Y est la 25^{ème} lettre et $28 \text{ modulo } 26 = 2$, on obtient donc B.

Clé privé

p, q deux nombres premiers.

d un nombre premier avec $(p - 1) \times (q - 1)$.

Les données confidentielles à ne pas divulguer sont donc p, q et d .

Clé publique

$$n = p \times q$$

e un entier tel que $d \times e = 1$ modulo $(p - 1) \times (q - 1)$.

→ Autrement écrit, il existe un entier k tel que

$$d \times e = 1 + k \times (p - 1) \times (q - 1)$$

On dit que e est «l'inverse de d modulo $(p - 1) \times (q - 1)$ ».

Les données publiques à partager sont donc n et e .

Soit M le message (un nombre supposé premier à p et q) que B veut envoyer à A.

- **Étape 1** : B va chercher (sur le site web de A par exemple) le couple (n, e) (**clé publique de A**).
- **Étape 2** : B chiffre son message M par l'opération

$$C = M^e \text{ modulo } n$$

et envoie le message chiffré C à A (par mail par exemple).

- **Étape 3** : A déchiffre le message en calculant C^d modulo n .

En utilisant le fait que e et d sont inverses l'un de l'autre, on peut prouver que $C^d = M$ modulo n

RSA : un exemple simple

Clé privée de A :

$$p = 17, q = 11$$

$$d = 7$$

Clé publique de A :

$$n = p \times q = 187,$$

$$e = 23$$

Nous avons $(p - 1) \times (q - 1) = 160$ et ça donne bien

$$23 \times 7 = 161 = 1 \text{ modulo } 160$$

B veut envoyer le message $M = 123$ à A,

- il calcule 123^{23} modulo 187 ce qui donne 30,
- il envoie donc $C = 30$ à A.

Pour déchiffrer, A calcule $C^d = 30^7$ modulo 187

$$30^7 = 116951871 \times 187 + 123$$

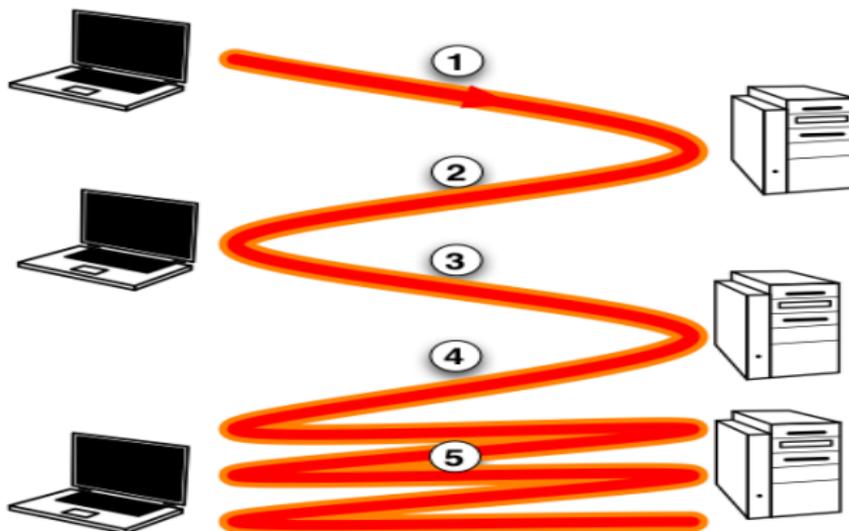
et retrouve bien 123.

La vraie vie : Achat en ligne sur Internet via le protocole SSL

Le protocole **SSL** (Secure Socket Layer) a été mis en place pour réaliser un canal sécurisé lors d'une connexion web.

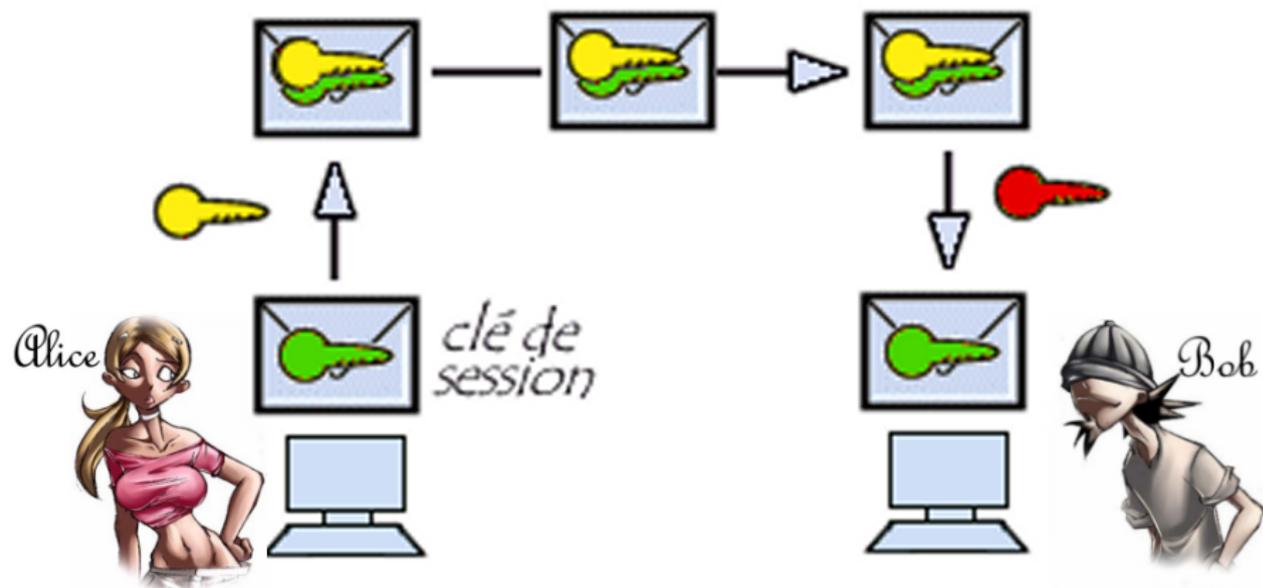
⇒ Cela permet alors d'avoir un canal entièrement sécurisé entre le navigateur et le site web.

Le principe de l'échange est schématisé par la figure ci-dessous :



- 1 Le navigateur envoie une requête de connexion sécurisée au site web.
- 2 Le site web envoie **son certificat** (i.e., une pièce d'identité délivrée par une autorité de confiance) et **sa clé publique**.
- 3 Le navigateur **vérifie le certificat**. Si le certificat est validé (i.e., le site web authentifié) alors le navigateur envoie **une clé secrète (pour être utilisé avec un chiffrement secret) générée «aléatoirement»** qui sera **chiffrée avec la clé publique du site web**.
- 4 Le site web déchiffre la clé secrète à l'aide de sa clé privée.
- 5 Le navigateur et le site web établissent alors un canal sécurisé chiffré avec la clé secrète (appelée **clé de session**).
Le navigateur et le site web peuvent échanger des données confidentielles grâce à la cryptographie symétrique .

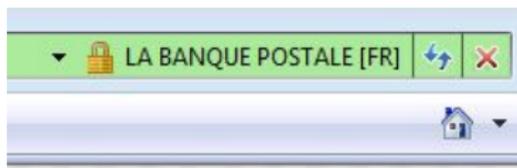
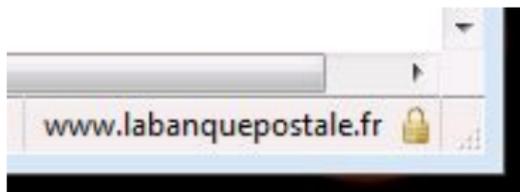
Résumons-nous !



La paire clé privée/clé publique est illustrée par **clé rouge**/clé **jaune**.

La clé de session (**clé verte**) représente le chiffrement symétrique.

SSL sur Internet



Informations sur la page - https://www.labanquepostale.fr/index/particuliers/banque_en_ligne/c...

Général Médias Flux Permissions Sécurité

Identité du site Web

Site Web : **www.labanquepostale.fr**
Propriétaire : **LA BANQUE POSTALE**
Vérfiée par : **VeriSign, Inc.**

Ce site Web fournit un certificat pour vérifier son identité. [Afficher le certificat](#)

Vie privée et historique

Ai-je déjà visité ce site Web auparavant ? **Oui, 105 fois**

Ce site Web collecte-t-il des informations (cookies) sur mon ordinateur ? **Oui** [Voir les cookies](#)

Ai-je un mot de passe enregistré pour ce site Web ? **Non** [Voir les mots de passe enregistrés](#)

Détails techniques

Connexion chiffrée : chiffrement de haut niveau (RC4 128 bit)
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.

[Charte d'utilisation](#)

[Accéder à votre compte](#)

Détails du certificat : "www.labanquepostale.fr"

Général Détails

Hiérarchie des certificats

- VeriSign Class 3 Public Primary Certification Authority - G5
 - VeriSign Class 3 Extended Validation SSL SGC CA
 - www.labanquepostale.fr

Champs du certificat

- Pas avant
- Pas après
- Sujet
- Info clé publique du sujet
 - Algorithme clé publique du sujet
 - Clé publique du sujet
- Extensions
 - Contraintes de base du certificat
 - Clé d'identification du sujet du certificat
 - Usage de la clé de certificat

Valeur du champ

Module (1024 bits) :

```
e9 5c 7e bf ef 96 6a 68 31 ab a6 75 e4 0e 8d fd
a0 0e 0e be 3f 0c 25 21 5c f6 47 b1 80 7e 2b 94
4e f2 64 72 fe f2 1f 83 e1 3a 04 b5 5d 86 c2 3b
85 da 20 98 4b 3f f7 1a c1 42 91 7c f7 b2 ed 17
fb 20 a3 e6 e4 b9 66 e5 d6 6a af 64 5c 00 04 00
30 e7 f7 dd 59 bf 46 80 43 86 d7 be 4e 5f cd b0
e5 bd e5 db 0d 10 8d od 42 57 01 d6 ba 24 ec d9
95 e2 84 56 10 6a f9 34 ac bf fe 3f bd e8 4a 07
```

Sécurité théorique \neq sécurité pratique

Les mathématiques fournissent des briques de base très solide...

Sécurité théorique \neq sécurité pratique

Les mathématiques fournissent des briques de base très solide...
.... encore faut il savoir faire du ciment.

Quelques exemples de mauvaise mise en pratique

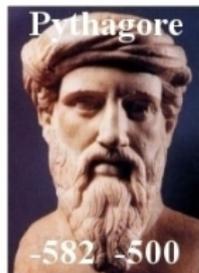
- Téléphonie mobile (GSM)
- Cartes bancaires
- Internet sans fil (WiFi, Wep)
- Canal sécurisé (SSH)
- DVD (CSS)

Enfin ca dépend du point de vue

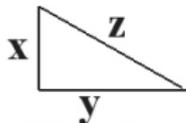
- Blue-Ray (AACS)
- Jeux vidéos (Xbox360, PS3)
- Musique (DRM)
- NSA

- RSA est en fin de vie, mais aura dominé durant 30 ans !
- Les mathématiques sont toujours de grands pourvoyeurs d'outils pour la cryptographie asymétrique.
 - ECC
 - NTRU
- La cryptographie est de plus en plus présente dans notre société
- Elle est aussi de plus en plus efficace

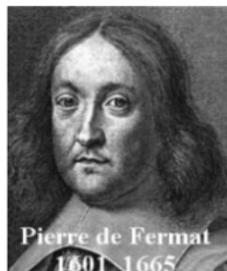
Recherche fondamentale : de l'inutile à l'indispensable



$$x^2 + y^2 = z^2$$



$$3^2 + 4^2 = 5^2$$

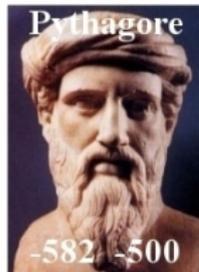


Grand théorème de Fermat

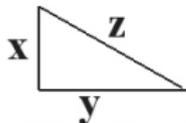
$$x^n + y^n = z^n$$

n'a pas de solutions
en nombres entiers
non nuls si $n > 2$

Recherche fondamentale : de l'inutile à l'indispensable



$$x^2 + y^2 = z^2$$



$$3^2 + 4^2 = 5^2$$



Grand théorème de Fermat

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

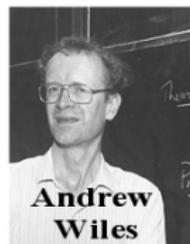
n'a pas de solutions
en nombres entiers
non nuls si $n > 2$

350 ans de recherche en
mathématique fondamentale

+

=

**Preuve
en 1994**



*courbes
elliptiques*



**Base de la cryptographie
à clé publique du
XXI eme siècle**

Recherche

- 4 chercheurs permanents, 5 à 8 doctorants ou post-doctorants
- Au sein du laboratoire de Mathématiques de Rennes
- Un séminaire hebdomadaire
- Collaboration avec le CELAR

Enseignements

- Master de Mathématiques spécialité Mathématiques de l'information, cryptographie.
 - Après une licence de Mathématiques
 - Double compétence en Mathématiques et en Informatique à la sortie
 - Débouchés : R&D, ingénieur d'études, recherche
- Master d'informatique spécialité Sécurité des Systèmes d'Information
 - Après un Master 1 d'informatique
 - Débouchés : audit de sécurité, développement, responsable sécurité