De la cryptographie

Tanguy Ortolo

18 avril 2010

Licence

Ce document est mis à disposition selon les termes de la licence Creative Commons paternité – partage des conditions initiales à l'identique 3.0.

Table des matières

1 Une brève histoire de la cryptographie **3**

1.1 Antiquité : naissance de la cryptographie 3

1.1.1 Aparté : la stéganographie 3

1.1.2 La cryptographie 4

1.2 La course au chiffre 4

1.2.1 Le chiffrement humain 4

1.2.2 La mécanisation 5

1.3 La révolution informatique 5

1.3.1 Chiffres symétriques 5

1.3.2 Échange de clefs 6

1.3.3 Chiffres asymétriques 6

2 Principes de la cryptographie asymétrique **8**

2.1 Fondements mathématiques 8

2.1.1 Principes généraux 8

2.1.2 L'algorithme RSA 9

2.2 Transmission des clefs 10

2.3 Chiffrement 10
2.4 Signature 11
2.5 Problème 11

3 La certification **12**
3.1 Organisation de base : la confiance directe 12
3.1.1 Fonctionnement 12
3.1.2 Limites 13
3.2 Modèle simple : les autorités de certification 13
3.2.1 Fonctionnement 13
3.2.2 Limites 14
3.3 Le réseau de confiance 15
3.3.1 Fonctionnement 15
3.3.2 Forces 15
3.3.3 Limites 16

4 Le système OpenPGP **17**
4.1 Origine 17
4.1.1 Les restrictions d'usage de la cryptographie . . 17
4.1.2 L'idée de Zimmermann 17
4.1.3 Le système PGP 18
4.1.4 OpenPGP et GnuPG 19
4.2 Notions 19
4.2.1 Clef 19
4.2.2 Identité 20
4.2.3 Signature de clef 20
4.2.4 Serveur de clefs 21
4.3 Utilisation 21
4.3.1 Génération de clefs 21

4.3.2 Signature de clef 22
4.3.3 Logiciels 23

Vocabulaire

Clair texte lisible.

Chiffre algorithme de chiffrement.

Chiffré texte illisible sans connaître les informations de déchiffrement.

Chiffrer appliquer un algorithme pour rendre un texte illisible.

Déchiffrer remettre un texte chiffré en clair à l'aide des informations de déchiffrement.

Décrypter remettre un texte chiffré en clair sans connaître les informations de déchiffrement, par analyse cryptographique.

Code convention de remplacement de mots ou de phrases par d'autres : « les carottes sont cuites ».

Crypter, **encrypter**, **cryptage**, **encryption**... barbarismes inutiles.

(b) l'importer : `gpg2 --import FICHIER`.

(c) la publier à nouveau sur les serveurs : `gpg2 --send-key ID`.

Des logiciels pour automatiser cela : `caff`, du paquet `signing-party`.

4.3.3 Logiciels

GPG (GnuPG, GNU Privacy Guard) est aujourd'hui l'implémentation la plus répandue d'OpenPGP. Il est intégré à toutes les bonnes distributions et installé par défaut. Il dispose d'interfaces graphiques pour les bureaux GNOME et KDE.

FireGPG est une extension pour Mozilla Firefox qui prend en charge le système de chiffrement OpenPGP au sein du navigateur. Cela permet de déchiffrer et de vérifier les signatures de textes présents sur le web, et de signer ou de chiffrer les textes que l'on envoie dans des formulaires. Il est surtout utile avec des webmails.

Enigmail est une extension de Mozilla Thunderbird (entre autres) qui prend en charge le système de chiffrement OpenPGP pour le courrier électronique.

La plupart des bons logiciels de messagerie instantanée, comme Pidgin et Gajim, prennent en charge OpenPGP pour chiffrer les messages envoyés et signer les messages de présence. Gajim essaie chiffre systématiquement les communications lorsque c'est possible, quitte à utiliser un chiffrement sans confiance qui est toujours mieux qu'une transmission en clair.

4.3.2 Signature de clef

Signer la clef de quelqu'un :

1. Sur place :
   (a) rencontrer quelqu'un ;
   (b) prendre sa carte d'identité et un papier avec son empreinte de clef (idéalement, une carte de visite) ;
   (c) contrôler son identité et noter son nom ;
   (d) lui rendre sa carte d'identité en gardant sa carte de visite.
2. De retour chez soi :
   (a) récupérer sa clef : `gpg2 --recv-key KEYID` ;
   (b) vérifier son empreinte et la comparer avec celles notée : `gpg2 --fingerprint KEYID`
   (c) vérifier ses identités et les comparer avec celle notée ;
   (d) signer les identités : `gpg2 --edit-key KEYID` ;
   (e) envoyer la clef ainsi signée à son propriétaire : `gpg2 --armor --output FICHIER --export ID`.

Faire signer sa clef : idem à l'envers !

1. Sur place :
   (a) rencontrer quelqu'un ;
   (b) lui présenter sa carte d'identité et un papier avec son empreinte de clef (idéalement, une carte de visite).
2. De retour chez soi :
   (a) attendre de recevoir de sa part sa clef avec un nouvelle signature ;

Chapitre 1

Une brève histoire de la cryptographie

1.1 Antiquité : naissance de la cryptographie

1.1.1 Aparté : la stéganographie

La stéganographie est l'art de la dissimulation.
Exemples célèbres :
- écrire sur une tablette de bois, puis la recouvrir de cire gravée d'un autre texte ;
- écrire sur la tête d'un esclave rasé, puis laisser repousser ses cheveux ;
- écrire sur les bits de poids faible des points d'une image numé-

rique.

1.1.2 La cryptographie

Chiffre de transposition : *scytale*, rouleau stéganographique.

Le chiffre de César consiste à remplacer chaque lettre par la suivante dans l'alphabet : c'est de la substitution mono-alphabétique. Variantes : ROT-13, avocat, K6, K7…

Des chiffres de substitution mono-alphabétiques variés : carré de Polybe, chiffre des templiers, etc.

Ces chiffres mono-alphabétiques sont très faciles à casser par analyse statistique, en se basant sur les fréquence d'occurrence des lettres de l'alphabet dans la langue utilisée.

1.2 La course au chiffre

1.2.1 Le chiffrement humain

Des chiffres sont inventés, toujours plus puissants, mais limités par la puissance de calcul de l'homme. Cassés au fur et à mesure.

Le chiffre de Vigenère (1586) consiste en l'addition des lettres du message et de celle d'une clef :

```
IL FAIT BEAU
CL EFCL EFCL
LX KGLF GKDG
```


4.2.4 Serveur de clefs

Une clef publique OpenPGP peut être exportée sous forme de fichier pour la communiquer à ses correspondants. Pour faciliter cela, on peut également la publier sur des serveurs de clefs.

Un serveur de clefs accepte :

- les soumissions de nouvelles clefs : `gpg2 --send-key ID` ;
- les mises à jour de clefs existantes – nouvelle identité, nouvelles signatures – : `gpg2 --send-key ID` ;
- les révocations de clefs : c'est une forme particulière de mise à jour ;
- les recherches de clefs : `gpg2 --search-keys NOM` ;
- la récupération d'une clef donnée : `gpg2 --recv-key ID`.

Notes qu'on ne supprime pas une clef d'un serveur : on la révoque (répudie) pour que tout le monde soit au courant.

Les serveurs de clefs les plus connus (`pgp.mit.edu`, `subkeys.pgp.net`, `wwwkeys.pgp.net`, `keys.gnupg.net`) sont synchronisés en « anneau » : une clef publiée sur l'un d'entre eux est répliquée sur les autres.

4.3 Utilisation

4.3.1 Génération de clefs

1. Générer une paire de clefs, algorithme RSA, 4096 bits : `gpg2 --gen-key`.
2. Ajouter des identités, une photo : `gpg2 --edit-key`.
3. Générer des certificat de révocation : pour perte, pour vol, arbitraire : `gpg2 --gen-revoke`.
4. Noter l'empreinte de sa clef sur ses cartes de visite : `gpg2 --fingerprint`.

derniers chiffres hexadécimaux de son empreinte, sans garantie d'unicité.

4.2.2 Identité

Les clefs sont publiées avec des informations annexes, notamment *les* identités du propriétaire : Prénom Nom <adresse>.

Clef publique algorithme, données

Identité 1 Prénom Nom <adresse1>

Identité 2 Prénom Nom <adresse2>

Identité 3 photo !

4.2.3 Signature de clef

Les clefs publiques sont accompagnées des signatures numériques apposées par les gens qui ont vérifié l'identité de son propriétaire annoncé.

Clef publique

Identité 1 Prénom Nom <adresse 1>

Auto-signature du propriétaire

Signature de untel

Signature de unetelle…

L'auto-signature, signature d'une identité par son propre propriétaire, a une fonction particulière : elle indique sa date d'expiration et éventuellement sa révocation.

Attaque de Babbage (1854) : l'analyse de la répartition des couples de lettres permet de déterminer la longueur de la clef ; on peut ensuite considérer chaque colonne – les lettres situées sur une même lettre de la clef – du message comme un cryptogramme mono-alphabétique.

1.2.2 La mécanisation

Avec la mécanisation, puis l'informatique, la complexité des chiffres explose. Les moyens de les casser également.

Enigma (1919, améliorée pour la Seconde guerre mondiale) est une machine électromécanique qui combine plusieurs mécanismes de chiffrement : un tableau de substitution des lettres, trois à six rotors tournants de substitution et un réflecteur qui renvoie dans les mécanismes précédants. Le chiffre est ainsi évolutif et réflexif.

Le déchiffrement d'Enigma fait intervenir des techniques aussi bien scientifiques que sociales :

- capture d'une machine Enigma ;
- déchiffrement de bulletins météo qui utilisent un chiffre partiel ;
- déchiffrement de messages commençant tous par les mêmes mots ;
- les « bombes » de Turing, ancêtres des ordinateurs.

1.3 La révolution informatique

1.3.1 Chiffres symétriques

Dans la lignée des chiffres classiques, les chiffres symétriques – à clef secrète commune – actuels sont des moulinettes infernales à bits :

DES, 3DES, AES…

Les chiffres symétriques sont peu coûteux en temps de calcul, mais nécessitent un secret partagé. Deux approches permettent d'éviter cet inconvénient, mais laissent le problème de la confiance en les échanges initiaux entre lee correspondants.

1.3.2 Échange de clefs

Le protocole Diffie-Hellman (1976) permet à deux correspondants de construire un secret partagé sans qu'un observateur puisse le déterminer.

Dans un groupe fini :

1. Alice et Bob choisissent une génératrice g.
2. Alice choisit un nombre a et envoie à Bob g^a.
3. Bob choisir un nombre b et envoie à Alice g^b.
4. Alice connaît a et g^b, et calcule g^{ab}.
5. Bob connaît b et g^b, et calcule g^{ab}.

Ce protocole peut être attaqué par *l'homme du milieu*, c'est à dire par interception et réécriture à la volée des échanges, l'attaquant faisant un échange Diffie-Hellman avec chacun des correspondants.

1.3.3 Chiffres asymétriques

Le chffre RSA (1978) permet de dissocier la clef (publique) de chiffrement de la clef (privée) de déchiffrement : la clef publique permet de chiffrer un message mais seule la clef privée permet de le déchiffrer.

Pour contourner les restrictions américaines sur exportation de matériel cryptographique [3], il publia ce logiciel sous la forme d'un livre imprimé, dont la diffusion est garantie par la Constitution américaine au titre de la liberté d'expression.

4.1.4 OpenPGP et GnuPG

Le format utilisé par le logiciel PGP fut normalisé par l'IETF [4] sous le nom d'OpenPGP. Ce format fut alors mis en œuvre par le logiciel libre GnuPG – *GNU privacy guard*, abrégé GPG – dans le cadre du projet GNU [5].

4.2 Notions

4.2.1 Clef

Les clefs vont évidemment par paire, clef privée et clef publique. Plusieurs algorithmes de chiffrement peuvent être utilisés, d'où autant de types de paires de clefs : RSA, DSA + ElGamal, IDEA…

Une clef est caractérisée par son *empreinte* (fingerprint) qui est une somme de contrôle de son contenu. Elle est souvent désignée par son *identifiant* (key ID) qui est composé des 4 derniers octets, donc des 8

3. Zimmermann a été poursuivi par les douannes américaines pour exportation de munition sans licence !

4. L'Internet engineering task force est l'organisation qui élabore les normes des protocoles et des formats de l'Internet, de façon remarquablement ouverte et transparente.

5. GNU, acronyme récursif de GNU's not UNIX, est un projet de développement d'un système d'exploitation libre, aujourd'hui répandu dans sa variante GNU/Linux.

ment permettrait également d'éviter que les anti-conformistes attirent les soupçons en étant seuls à chiffrer leurs communications, et en ce sens, une bonne chose pour la démocratie et la liberté de pensée.

Or, l'évolution des lois américaines donnait l'impression d'une volonté de réguler et même d'interdire l'usage de la cryptographie. Par conséquent, en libéralisant son usage autant que possible tant que c'était encore autorisé, il devait être possible d'empêcher son interdiction future.

Vingt ans après, on peut constater la réussite de cette démarche. Le chiffrement est aujourd'hui massivement utilisé dans des communications qui n'ont rien de répréhensibles et ne sont pas liées à la sécurité et à la défense nationale [1]. Une grande quantité de données chiffrées circule sur Internet, de sorte que chiffrer ses communications ne peut plus éveiller de soupçon. Les États-Unis en 2000, et la France en 2004, ont libéralisé l'usage de la cryptographie ; l'importance de son utilisation dans les échanges commerciaux rend son interdiction future très peu probable.

4.1.3 Le système PGP

Pour atteindre cet objectif, Zimmermann développa et publia le logiciel semi-libre [2] PGP – *pretty good privacy* –, une mise en œuvre du modèle de cryptographie asymétrique basé sur un réseau de confiance.

1. On chiffre des transactions commerciales, mais également tous les échanges liés à l'identité, comme la récupération de courrier électronique – sauf chez des incompétents comme Orange, qui *imposent* un échange en clair pour transmettre les mots de passe.
2. Semi-libre, c'est à dire librement utilisable et diffusable sauf à des fins commerciales.

Ce système peut être attaqué par *l'homme du milieu*, c'est à dire par interception de la transmission de la clef publique et remplacement par la clef publique de l'attaquant.

Chapitre 2

Principes de la cryptographie asymétrique

2.1 Fondements mathématiques

2.1.1 Principes généraux

La cryptographie asymétrique est basée sur des fonctions à sens unique avec trappe : on utilise une fonction de chiffrement paramétrée f_P, qui n'a pas de formule inverse déterminable.

En revanche, connaissant une information supplémentaire S, on peut calculer son inverse : $f_S = f_P^{-1}$.

Chapitre 4

Le système OpenPGP

4.1 Origine

4.1.1 Les restrictions d'usage de la cryptographie

Pendant un temps, les systèmes cryptographiques furent considérés comme des armes de guerre, et leur diffusion restreinte par les gouvernements.

4.1.2 L'idée de Zimmermann

Pour Philip Zimmermann, le droit à la vie privée était important, mais était menacé par les facilités d'espionnage des communications électroniques. Dans ce cadre, la cryptographie était un excellent moyen de protéger ses communications privées. La généralisation du chiffre-

- tant qu'elle n'est pas détectée, cela affecte exclusivement ceux qui accordent une confiance totale aux signatures effectuées avec cette clef,
- dès qu'elle est détectée, on peut révoquer cette clef, ainsi toutes les signatures qui y sont apposées, ce qui ramène au cas d'une cessation d'activié ;

– signatures abusives d'un membre : ce cas est semblable à une corruption de clef, à ceci près que son propriétaire ne la révoquera pas, en revanche ses signataires révoqueront leurs signatures.

3.3.3 Limites

Un réseau de confiance :

– est plus lent à construire qu'un ensemble de confiance basé sur des autorités ;
– n'est soutenu par aucun intérêt commercial ;
– dépend de l'honnêteté des membres du réseau.

Notez toutefois que le modèle du réseau de confiance est une extension de celui des autorités de certifications : par conséquent, le système des autorités de certification en est un sous-ensemble, et peut être mis en œuvre dans un système de réseau de confiance.

P est la clef publique, S est la clef privée (ou secrète).

2.1.2 L'algorithme RSA

Du nom de ses inventeurs, Rivest, Shamir et Adleman (1977). Breveté [1] par le MIT en 1983, brevet expiré en 2000.

Pour créer une paire de clefs :

1. on choisit deux nombres premiers p et q ;
2. on calcule le *module de chiffrement* $n = pq$;
3. on calcule *l'indicatrice d'Euler* $\varphi(n) = (p-1)(q-1)$;
4. on choisit *l'exposant de chiffrement* e premier avec $\varphi(n)$;
5. on calcule *l'exposant de déchiffrement* $d = e^{-1} \pmod{\varphi(n)}$ (théorème de Bezout) ;
6. la clef publique est (n, e) et la clef privée est (n, d).

Pour chiffrer un message M :

$$M' = M^e \pmod{n}$$

Théorème 1 (Euler) *Soit n un entier naturel et a un entier premier avec n, alors :*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

1. Le brevet sur l'algorithme RSA n'était valable qu'aux États-Unis. En Europe, on ne peut pas breveter d'algorithme mathématique. Enfin, en réalité on peut, et l'OEB l'acceptera puisqu'ils sont payés au dépôt de brevet, mais il sera invalide.

Pour déchiffrer un message M' :

$$\begin{aligned} M'' &\equiv M'^{d} \pmod{n} \\ &\equiv M^{ed} \pmod{n} \\ &\equiv M^{1+k\varphi(n)} \pmod{n} \\ &\equiv M \pmod{n} \end{aligned}$$

Pour déchiffrer un message, il faut donc connaître d. À partir de la clef publique (n, e), cela nécessite :

1. de décomposer $n = pq$;
2. de calculer $\varphi(n) = (p-1)(q-1)$;
3. d'inverser e modulo $\varphi(n)$.

C'est l'étape de décomposition de n qui est exponentiellement coûteuse en temps.

2.2 Transmission des clefs

1. Alice transmet à Bob sa clef publique A.
2. Bob transmet à Alice sa clef publique B.

En pratique, les deux peuvent même la publier au monde entier.

2.3 Chiffrement

Pour chiffrer un message, Alice calcule $M' = f_B(M)$ et le transmet.

Pour le déchiffrer, seul Bob peut calculer $M = f_{B'}(M')$.

3.3 Le réseau de confiance

C'est une extension du principe de certification à des certifications multiples.

3.3.1 Fonctionnement

Le fonctionnement du système d'autorités de certification est étendu comme suit :

Un certificat est une clef publique accompagnée :
- de l'identité civile de son prétendu propriétaire ;
- *des* signatures de personnes qui se portent garantes de la correspondance entre cette identité affichée et l'identité civile vérifiée de celui qui a présenté la clef publique.

On fait confiance aux signatures de personnes de confiance, aux signatures d'un certain nombre de personnes de confiance marginale, ou aux signatures à plusieurs niveaux d'indirection selon une formule dépendant du nombre de niveaux et des degrés de confiance.

3.3.2 Forces

Le réseau de confiance est très résistant à des problèmes qui mettraient en déroute un système basé sur l'autorité de certification :
- cessation d'activité d'un membre : chacun ayant un rôle partiel limité dans le fonctionnement du réseau de confiance, cela n'a pratiquement aucun impact ;
- corruption d'une clef d'un membre :

1. les gens émettent des requêtes de certificat ;
2. les autorités de certifications vérifient leur identité et signent ces requêtes, en faisant des certificats ;
3. les gens font confiance aux autorités de certifications et acceptent les certificats qu'elles ont signées.

Cette organisation a été retenue pour le protocole SSL, qui sécurise les applications d'Internet.

3.2.2 Limites

Les autorités de certification :

- forment une guilde mondiale, avec une très forte barrière à l'entrée.
- disposent du pouvoir d'émettre et faire accepter des papiers d'identité numériques sans contrôle des États ;
- sont incontournables, pour établir une boutique en ligne par exemple ;
- émettent parfois des certificats sans vérifications sérieuses : un simple coup de fil ;
- sont contrôlées pour leurs procédures de sécurité, pas pour leur intégrité.

Les problèmes liés à la confiance entière en des autorités de certification privilégiées sont réels : en 2005, pour répondre aux *vérifications trop légères* que certaines AC effectuaient sur leurs clients, le forum des autorités de certification a décidé d'introduire la notation *Extended Validation* censée garantir le sérieux des vérification d'un certificat.

2.4 Signature

Pour signer un message, seule Alice peut calculer $M^* = f_{A'}(M)$ et le transmettre à côté du message M.

Pour le vérifier, Bob calcule $M^? = f_A(M^*)$ et le compare à M.

En pratique : $M^* = f_{A'}(H(M))$, où H est un hachage cryptographique.

2.5 Problème

Pour chiffrer : être certain que la clef publique est bien fournie par son destinataire.

Pour vérifier une signature : être certain que la clef publique est bien celle de l'expéditeur.

Chapitre 3

La certification

3.1 Organisation de base : la confiance directe

3.1.1 Fonctionnement

Dans l'organisation de base, spontanée, les interlocuteurs se transmettent directement leurs clefs publiques, de la main à la main.

Alice sait que la clef B vient de Bob parce qu'il lui a donné en personne.

3.1.2 Limites

Trop peu efficace : il faut rencontrer en personne tous ses interlocuteurs au moins une fois, par exemple la banque américaine à qui je vais envoyer l'ordre de transfert du paiement de mon billet d'avion pour New York.

3.2 Modèle simple : les autorités de certification

Pour pouvoir faire une confiance non aveugle à des interlocuteurs qu'on ne connaît pas directement, il n'y a qu'une solution : déléguer son pouvoir de confiance à… des personnes « de confiance ».

3.2.1 Fonctionnement

Une requête de certificat est une clef publique accompagnée d'informations sur l'identité civile de son prétendu propriétaire.

Un certificat est une clef publique accompagnée :

- de l'identité civile de son prétendu propriétaire ;
- de la signature d'une personne qui se porte garante de la correspondance entre cette identité affichée et l'identité civile vérifiée de celui qui a présenté la clef publique.

Une autorité de certification est une personne dont la caution, matérialisée par les signatures qu'il appose sur des certificats, est reconnue par « les gens ».

Ainsi :