De la cryptographie

Tanguy Ortolo

13 juin 2012

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 **4**
- 1.1 Antiquité : naissance de la cryptographie . . . 4
  - 1.1.1 Aparté : la stéganographie . . . 4
  - 1.1.2 La cryptographie . . . 4
- 1.2 La course au chiffre . . . 5
  - 1.2.1 Le chiffrement humain . . . 5
  - 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 **7**
- 2.1 Fondements mathématiques . . . 7
  - 2.1.1 Principes généraux . . . 7
  - 2.1.2 L'algorithme RSA . . . 7
- 2.2 Transmission des clefs . . . 8
- 2.3 Chiffrement . . . 8
- 2.4 Signature . . . 8
- 2.5 Problème . . . 8

3 La certification **10**
- 3.1 Organisation de base : la confiance directe . . . 10
  - 3.1.1 Fonctionnement . . . 10
  - 3.1.2 Limites . . . 10
- 3.2 Modèle simple : les autorités de certification . . . 10
  - 3.2.1 Fonctionnement . . . 10
  - 3.2.2 Limites . . . 11
- 3.3 Le réseau de confiance . . . 11
  - 3.3.1 Fonctionnement . . . 11
  - 3.3.2 Forces . . . 12
  - 3.3.3 Limites . . . 12
- 3.4 Note générale . . . 12

4 Le système SSL/TLS **13**
- 4.1 Fonctionnement . . . 13
  - 4.1.1 Des certificats . . . 13
  - 4.1.2 Côté serveur . . . 13

4.1.3 Côté client 13
4.2 Cas pratiques 14
4.2.1 Connexion non chiffrée 14
4.2.2 Connexion chiffrée mais non vérifiée 14
4.2.3 Connexion chiffrée et vérifiée 15

5 Le système OpenPGP 16
5.1 Origine 16
5.1.1 Les restrictions d'usage de la cryptographie 16
5.1.2 L'idée de Zimmermann 16
5.1.3 Le système PGP 17
5.1.4 OpenPGP et GnuPG 17
5.2 Notions 17
5.2.1 Clef 17
5.2.2 Identité 17
5.2.3 Signature de clef 17
5.2.4 Serveur de clefs 18
5.3 Utilisation 18
5.3.1 Génération de clefs 18
5.3.2 Signature de clef 18
5.3.3 Logiciels 19

Vocabulaire

Clair texte lisible.

Coder transformer un message, c'est à dire une suite de lettres, en une suite de chiffres. Exemples de codages : morse, ASCII, UTF-8.

Chiffrer appliquer un chiffre, procédé permettant de rendre un message illisible à qui ne dispose pas des informations de déchiffrement.

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.

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 d'un message.
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 numérique.

1.1.2 La cryptographie

La *scytale* était un rouleau permettant de modifier l'ordre des lettres d'un message, le rendant illisible sans disposer d'un rouleau identique. Il s'agit d'un chiffre de transposition, qui agit sur l'ordre des lettres.

Le chiffre de César consiste à remplacer chaque lettre par la quatrième suivante dans l'alphabet : il s'agit d'un chiffre de substitution mono-alphabétique, qui agit sur chaque lettre en la remplaçant par une autre, chaque lettre étant toujours remplacé par la même lettre. Variantes : ROT13, 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
```

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, qui ne sont plus limités par les capacités humaines, 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 précédents. 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

L'invention de l'électronique, puis de l'informatique, permet de développer des chiffres encore plus complexes.

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 que les interlocuteurs disposent d'une clef de chiffrement commune, qui constitue un secret partagé. Il faut donc qu'ils se transmettent au préalable cette clef, ce qui est souvent problématique, cet échange devant se faire par un moyen intrinsèquement sécurisé sous peine de compromettre tous les échanges futurs. Deux approches permettent d'éviter cet inconvénient.

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^a, et calcule g^{ab}.

Ce protocole peut être attaqué par la technique de *l'homme du milieu*, c'est à dire par interception et réécriture à la volée des échanges, l'attaquant se faisant passer pour l'autre correspondant auprès de chaque correspondant, et réalisant un échange Diffie-Hellman avec chacun d'entre eux.

1.3.3 Chiffres asymétriques

Les chiffre asymétriques tel que RSA (1978), permettent 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.

Ce système est également vulnérable à l'attaque de *l'homme du milieu*, c'est à dire par interception et remplacement de la clef publique, l'attaquant récupérant la clef publique d'un interlocuteur et fournissant au second sa propre clef publique à la place.

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 f_P paramétrée par une clef P, qui n'a pas de formule inverse — de fonction de déchiffrement — déterminable.

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

Le paramètre P est appelé clef publique, S étant la clef privée (ou clef secrète).

2.1.2 L'algorithme RSA

Ainsi nommé d'après le nom de ses inventeurs, Rivest, Shamir et Adleman, RSA est le premier algorithme de chiffrement asymétrique inventé, en 1977. Breveté [1] par le MIT en 1983 jusqu'en 2000.

Depuis, d'autres cryptosystèmes ont été inventés, comme DSA ou ElGamal, mais RSA est l'algorithme le plus souvent utilisé comme exemple.

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 :

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

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.

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

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

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 déterminer d. À partir de la clef publique (n, e), ce qui 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 $M = f_{B'}(M')$.

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, on signe plutôt un hachage cryptographique $H(M)$ qui occupera moins de place que le message entier : $M^* = f_{A'}(H(M))$.

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.

En effet, comme mentionné précédemment, les algorithmes de chiffrement asymétrique sont également vulnérables à l'attaque de l'homme du milieu :

1. l'attaquant Oscar intercepte et bloque la transmission de la clef d'Alice à Bob ;
2. il se fait passer pour Alice auprès de Bob et lui sa propre clef publique à la place ;
3. lorsque Bob voudra transmettre un message chiffré à Alice, il le chiffrera donc avec la clef publique d'Oscar ;
4. Oscar pourra alors déchiffrer ce message avec sa propre clef privée, en prendre connaissance, puis le chiffrer avec la clef publique d'Alice pour lui envoyer sans qu'elle puisse détecter l'attaque.

Chapitre 3

La certification

Pour se prémunir de l'attaque de l'homme du milieu décrite dans les sections 1.3.2 page 6 et 2.5 page 8, il faut se donner un moyen de s'assurer que la clef publique dont on dispose est bien celle de son interlocuteur et non celle de quelqu'un qui voudrait se faire passer pour lui.

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

On utilise des documents informatiques contenant la clef publique, les *certificats*.

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 :

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 qui encourage le maintien d'un oligopole minimal.
- disposent du pouvoir d'émettre et faire accepter des papiers d'identité numériques sans contrôle des États ou des citoyens ;
- sont incontournables, pour établir une boutique en ligne par exemple ;
- ont intérêt à émettre des certificats sans vérifications sérieuses — un simple coup de fil ;
- sont contrôlées pour leurs procédures de sécurité, et non pour leur intégrité.

Les problèmes liés à la confiance entière en des autorités de certification privilégiées sont réels : en 2005, pour résoudre le problème des *vérifications trop légères* que certaines autorités effectuaient sur leurs clients, le forum des autorités de certification a décidé d'introduire une nouvelle notation, *Extended Validation*, censée garantir que l'identité du propriétaire d'un tel certificat a été vérifiée sérieusement.

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 :
  - 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'activé ;
- 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.

3.4 Note générale

Quel que soit le modèle de certification utilisé, la garantie obtenue qu'une clef appartient bien à son propriétaire annoncé n'est jamais absolue mais consiste plutôt en un transfert de responsabilité. En effet, même en ayant reçu en main propre la clef publique d'Alice, un tiers malveillant pourra éventuellement lire les message chiffrés qu'on lui enverra par la suite dans les cas suivants :

- Alice a perdu sa clef secrète ;
- Alice a volontairement donné sa clef secrète à un tiers ;
- Alice a volontairement présenté la clef d'un tiers à la place de la sienne ;
- Alice transmet volontairement les messages qu'elle reçoit à un tiers.

Dans tous ces cas, on remarque que, si les messages peuvent être lus par un tiers, c'est toujours *la faute d'Alice*. Ainsi, lorsqu'on a pu vérifier l'identité du propriétaire d'une clef publique, cela signifie simplement qu'on peut le considérer comme responsable de cette clef, et que si quelqu'un d'autre dispose de la clef secrète correspondante, c'est sa faute et non la nôtre.

Chapitre 4

Le système SSL/TLS

Le système TLS *(transport layer security)*, anciennement appelé SSL *(secure socket layer)*, est le système de chiffrement utilisé pour sécurisé la majorité des échanges de type client–serveur sur Internet. Dans son utilisation actuelle, il est lié à la norme X.509 de l'Union internationale des télécommunications, que j'assimilerai par endroits à TLS lui-même.

4.1 Fonctionnement

Ce système utilise un modèle de cryptographie asymétrique basé sur des autorités de certification, décrit à la section 3.2.1 page 10. Il est essentiellement utilisé pour chiffrer les échanges entre client et serveur et permettre au client de s'assurer de l'identité du propriétaire du serveur : c'est donc ce cas précis que je détaillerai ici.

4.1.1 Des certificats

Le système TLS utilise des certificats selon la norme X.509. Comme indiqué à la section 3.2.1 page 10, ces certificats sont constitués d'une clef publique, des informations d'identité du propriétaire et de la signature d'une autorité de certification.

La norme X.509 permet d'indiquer des informations d'identité assez détaillées, mais pour des raisons de simplicité, seuls les noms de domaines y sont habituellement indiqués, et le véritable nom du propriétaire n'est que très rarement indiqué.

4.1.2 Côté serveur

L'administrateur d'un serveur Internet génère une paire de clef et installe la clef publique dans une demande de certificat (cf. section 3.2.1 page 10). Il transmet cette demande à une autorité de certification. Celle-ci le facture, effectue quelques vérifications — peu poussées pour ne pas perdre un client ! — puis signe cette demande pour en faire un certificat.

L'administrateur installe ensuite ce certificat ainsi que la clef privée sur son serveur.

4.1.3 Côté client

Le client, ou plus précisément, son logiciel, dispose d'une liste de certificats d'autorités de certification. Cette liste, pré-établie par l'éditeur du logiciel est critique pour

la sécurité des échanges futurs ; sur les systèmes qui ne fournissent aucun moyen de vérification des logiciels installés [1], elle peut être corrompue par un attaquant.

La connexion à un serveur utilisant TLS se déroule ainsi :

1. le serveur envoie son certificat, qui a été signé par une autorité de certification ;
2. le client vérifie la signature de cette autorité, et selon le résultat de cette vérification, accepte ce certificat ou ferme la connexion, l'échange se terminant alors à ce point ;
3. la clef publique du serveur est utilisée pour chiffrer un échange initial permettant de construire un secret partagé ;
4. un flux chiffré est finalement établi avec un chiffrement symétrique utilisant ce secret partagé comme clef de chiffrement.

Le passage à un chiffre symétrique permet de simplifier les calculs, celui-ci étant moins coûteux en puissance qu'un chiffre asymétrique. La construction du secret partagé fait en réalité plutôt intervenir un échange de Diffie-Hellman signé, mais le détail n'apporte pas grand chose à la compréhension générale du système.

4.2 Cas pratiques

L'usage le plus courant de TLS est la sécurisation des transmissions avec un site Web. Dans cet exemple, on peut distinguer trois cas.

4.2.1 Connexion non chiffrée

FIGURE 4.1 – Un site Web non chiffré

Dans ce cas, qui est représenté par une absence d'indication particulière dans la zone d'adresse du navigateur (figure 4.1), la transmission s'effectue *en clair*.

Une telle connexion est vulnérable à tout type d'écoute ou d'interception, et ne devrait jamais être utilisée pour transmettre des données sensibles telles que des mots de passe. En particulier, si le moyen physique de connexion n'est pas sûr, par exemple sur un réseau sans fil public, n'importe qui dans le voisinage peut prendre connaissance des données transmises.

4.2.2 Connexion chiffrée mais non vérifiée

FIGURE 4.2 – Un site Web chiffré mais non vérifié

Dans ce cas, représenté par un avertissement du navigateur (figure 4.2), la transmission est effectivement chiffrée ; contrairement à ce que pourrait laisser penser cet avertissement, ce chiffrement est toujours *préférable* à une absence de chiffrement.

1. Les gestionnaires de paquets comme celui de Debian permettent de vérifier cryptographiquement l'intégrité des paquets avant de les installer.

En revanche, l'identité du propriétaire de la clef n'a pas pu être vérifiée, par exemple parce qu'il a utilisé une autorité de certification inconnue, parce qu'il s'est trompé de nom, ou parce qu'un attaquant a effectivement pris sa place.

Ce type de connexion est invulnérable aux simples écoutes et aux interception effectuées *après* l'établissement de la connexion. Elle est en revanche vulnérables aux interceptions et réécritures par un attaquant présent depuis le début de la connexion.

4.2.3 Connexion chiffrée et vérifiée

FIGURE 4.3 – Un site Web chiffré et vérifié

Dans ce cas, représenté par un cadenas ou une zone bleue ou verte (figure 4.3), la transmission est chiffrée et l'identité du propriétaire de la clef a pu être vérifiée : elle est garantie par une autorité de certification et correspond au nom de domaine du serveur.

Ce type de connexion est invulnérable aux attaques ordinaires précédemment mentionnées, mais reste vulnérable aux attaques plus graves telles que le vol de clef privée ou la corruption d'une autorité de certification.

Notez toutefois que, comme indiqué à la section 4.1.1 page 13, l'identité du propriétaire ainsi vérifiée est en réalité seulement constituée par son nom de domaine. Il est donc essentiel de vérifier ce nom de domaine dans la barre d'adresse : il est par exemple possible de tomber sur un site Web `https://particuliers-societegenerale.com/`, sécurisé par un certificat tout à fait valide, mais bien distinct du site de la banque `https://particuliers.societegenerale.com/` et administré par un pirate prêt à enregistrer vos paramètres d'accès à vos comptes en banque.

Chapitre 5

Le système OpenPGP

OpenPGP est un système de cryptographie asymétrique basé sur un réseau de confiance tel que décrit à la section 3.3 page 11. Il est essentiellement utilisé pour sécuriser des échanges entre particuliers, par courrier électronique ou par messagerie instantanée.

5.1 Origine

5.1.1 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.

5.1.2 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 chiffrement 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.

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.

5.1.3 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.

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.

5.1.4 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].

5.2 Notions

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

5.2.2 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 !

5.2.3 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>

2. Semi-libre, c'est à dire librement utilisable et diffusable sauf à des fins commerciales.

3. Zimmermann a été poursuivi par les douanes 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.

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.

5.2.4 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.

5.3 Utilisation

5.3.1 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`.

5.3.2 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 ;
   (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`.

5.3.3 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 était une extension pour Mozilla Firefox qui prenait en charge le système de chiffrement OpenPGP au sein du navigateur. Cela permettait 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 était surtout utile avec des webmails. À ce jour, FirePGP est abandonné et n'a pas de successeur.

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.