Bertrand Lemaire
http://www.bertrandlemaire.com

Initiation au cryptage et à la signature électronique

Table des matières

Principes de base

Qu'est-ce que le cryptage ? A quoi sert-il ? Comment ça marche ?

Le cryptage consiste à transformer un fichier selon un algorithme donné afin de le rendre illisible sans avoir appliqué l'algorithme inverse.
Le cryptage sert à protéger des fichiers contre une appropriation non désirée. Même récupéré, un fichier crypté est normalement inutilisable par son possesseur s'il ne possède pas le moyen de décrypter. Seul le fichier crypté doit être échangé. Le fichier initial "en clair" doit rester sur votre disque dur ou, mieux, être détruit ou sauvegardé uniquement sur un support amovible mis en sécurité.
L'algorithme de cryptage peut reposer soit sur une paire de clés privée/publique (la clé privée pouvant être protégée par un mot de passe, comme avec PGP ou GnuPG), soit sur un mot de passe (système de protection intégré dans la plupart des logiciels de bureautique).
Crypter est bien évidemment très utile pour partager des fichiers avec des amis à partir d'un site web, dont l'accès est forcément public (la protection d'un site avec mot de passe étant facilement contournable par des gens mal intentionnés).

Clé privée/clé publique ou mot de passe ?

PGP, GnuPG et beaucoup d'autres produits de cryptage utilisent le principe de la paire de clés publique/privée ou PKI (Public Key Infrastructure), également appelée Architecture à Clés Asymétriques.
Clés publiques et clés privées sont de petits fichiers informatiques servant à sécuriser d'autres fichiers lors d'un échange ou d'un stockage par du cryptage. Elles contiennent des paramètres utilisées par l'algorithme de cryptage. Dans ce cas, pour crypter un fichier, il faut posséder la clé publique du destinataire. Pour décrypter un fichier, il faut posséder la clé privée de celui-ci. Les deux clés (publique et privée) sont deux fichiers de paramètres différents, d'où le terme de *cryptage à clés asymétriques*.
Normalement, seul le propriétaire légitime d'une clé privée la possède... et ne l'a pas perdue. La clé privée est, de plus, pour fonctionner, le plus souvent associée à un mot de passe qui, lui aussi, doit rester la seule possession de son propriétaire légitime. Par contre, votre clé publique doit être remise à chacun de vos correspondants, pour que ceux-ci puissent vous envoyer des fichiers cryptés.
Dans le cas d'un algorithme reposant sur un simple mot de passe, aucune "clé" n'est à échanger entre celui qui a crypté un fichier et son destinataire. Le cryptage ne repose en effet que sur les caractères composant le mot de passe.

	Avantages	***Inconvénients***
Clé publique/clé privée	Seul moyen d'identification reconnu légalement dans le cadre de la signature électronique, via la notion de certificat (voir ci-dessous). Un seul mot de passe à retenir (le sien) : il suffit de disposer de sa clé privée personnelle et de la clé publique de ses destinataires. La PKI permet de crypter ses fichiers en les destinant à une personne précise ou un groupe de personnes précis. Seule la PKI permet une mise en place d'une vraie politique de sécurité avec des droits d'accès attachés aux personnes et non aux fichiers.	Les produits existants ne sont pas forcément très simples d'emploi pour des néophytes. Il est nécessaire d'échanger des clés avant toute transmission de fichiers cryptés. La mise en place d'une "vraie" PKI est très complexe, comme toute politique de sécurité informatique. Le cryptage devra être réalisé à destination de personnes précises et identifiées. Si on en a oublié une, il faut recommencer.
Mot de passe	Très simple à mettre en oeuvre. L'absence de "produit standard" (au contraire de la PKI) gêne les pirates qui se trouvent confrontés à chaque fois à de nouveaux produits, de nouveaux algorithmes... Il suffit de ne noter nulle part le mot de passe pour le protéger tandis qu'une clé privée peut toujours traîner sur un disque dur.	Le mot de passe est attaché au fichier, pas à la personne émettrice/destinataire. Il faut retenir un certain nombre de mots de passe... (si on utilise toujours le même, chacun ayant accès à un fichier peut accéder à tout). La mise en place d'une vraie politique de sécurité est impossible.

Paire de clés, certificat et signature électronique

Pour crypter à l'attention de quelqu'un en utilisant la clé publique de cette personne (voir ci-dessus), il faut posséder cette clé et être sûr de l'identité de son propriétaire.
Si, dans un petit groupe où chacun se connaît et où l'on s'échange les clés via des disquettes ou des e-mails, cela ne pose pas vraiment de problème. Mais il en est tout autrement dans les rapports d'affaires ou juridiques.
D'où la notion de clé certifiée (ou de certificat). L'idée est simple : on fait confiance à quelqu'un (le tiers de confiance) pour dire si son interlocuteur est bien celui qu'il prétend être. C'est le principe de la carte d'identité : on fait confiance à la Préfecture pour dire que celui qui est en photo dessus est bien celui dont le nom est écrit. Il existe, comme pour la carte d'identité, un système d'opposition (la révocation de certificat).
C'est sur le principe de la clé certifiée que repose le concept légal de signature électronique, au

travers de "tiers de confiance agréés".
La signature électronique est encadrée légalement par le décret 2001-272 du 30 Mars 2001 (Référence NOR : JUSC0120141D), pris en application de la loi de Février 2000 (modifiant l'article 1316-4 du Code Civil). Ces textes transposent en droit français (avec quelques aménagements) la directive européenne du 12 décembre 1999 (Référence 1999/93/CE).

Voir à ce sujet le site de la FNTC (Fédération Nationale des Tiers de Confiance) : http://www.fntc.org
Les textes (lois, décrets...) peuvent être consultés gratuitement en connaissant la référence NOR ou la date de publication sur le site Légifrance.
Enfin, la partie "portail" de ce site vous donnera un grand nombre de liens utiles (éditeurs de logiciels, sites juridiques...), pour cette question comme pour d'autres.

La signature électronique : comment ça marche ?

L'article 1316-4 du Code Civil donne la même force probante à une signature qu'elle ait été réalisée électroniquement ou grâce à un stylo. L'objectif d'une signature est de prouver que l'individu ayant signé est d'accord avec le contenu du document signé, dont l'intégrité doit donc être garantie. L'identité du signataire doit donc également être démontrée.

La signature électronique repose sur les certificats. Un certificat est une clé publique dont le titulaire a son identité certifiée par un tiers de confiance, l'autorité de certification. Le certificat est utilisé, combiné à une empreinte numérique du document, pour signer celui-ci. L'empreinte garantit l'intégrité, le certificat l'identité du signataire. La norme la plus courante de certificats, recommandée par les organismes de normalisation, est la X509. Cette norme garantit que la plupart des logiciels pourront utiliser le certificat : messagerie, cryptographie,…

Le certificat peut être révoqué s'il a été perdu par son titulaire (ou volé) ou automatiquement au bout d'un certain temps (à la fin d'un contrat, d'une mission). La reconnaissance d'un certificat suppose donc d'interroger l'autorité qui l'a délivré pour vérifier sa validité. Les logiciels lisant les certificats font cette interrogation auprès du serveur de l'Autorité automatiquement ou manuellement.

La création et la gestion d'un certificat se réalise grâce à trois intervenants qui peuvent être regroupés en une ou deux entités. L'autorité de certification (AC) décide des règles de délivrance et de gestion des certificats réalisés sous son autorité. L'autorité d'enregistrement (AE) exécute ces règles en délivrant effectivement les certificats aux titulaires. L'opérateur de certification (OC) fournit l'infrastructure matérielle et logicielle requise.

La seule signature peut être insuffisante pour donner une valeur juridique à un document. La date et l'heure de celle-ci peut être essentielle, d'où la notion d'horodatage, également réalisée par des tiers de confiance en signant des agrégats datés.

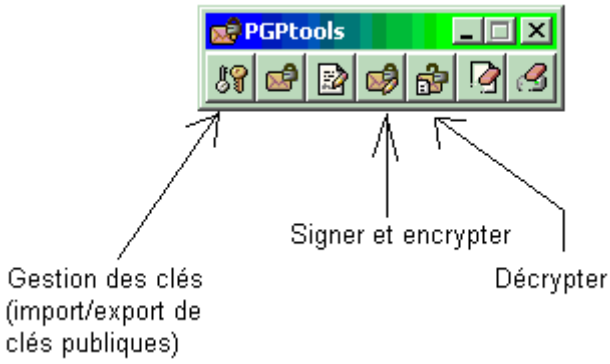
Petit didacticiel de PGP

PGP est un logiciel de cryptage utilisant le principe des clés privées / clés publiques (PKI). Les fichiers cryptés ont l'extension "pgp" sous Windows.
ATTENTION : PGP n'est compatible avec Windows XP qu'à partir de la version 8.
Les clés publiques de PGP sont compatibles avec celles de GnuPG.

Installer le programme de cryptage PGP

Allez sur http://www.pgp.com et choisissez la version de PGP appropriée à votre système d'exploitation. Installez le comme n'importe quel autre programme. Le programme est en Anglais seulement (mais ça n'a pas vraiment d'importance au delà de l'installation). Les différents sites de chargement sont similaires. Choisir la version la plus récente disponible.
Lors de l'installation, si vous êtes un nouvel utilisateur, il vous faudra créer votre clé privée et votre clé publique en indiquant un e-mail (facultatif) et un mot de passe (obligatoire). Vos clés publique et privée (une de chaque) seront dans un sous-répertoire "PGP" (dans "Mes documents" sous Windows). Il est fortement recommandé de sauvegarder celles-ci (voir ci-dessous).

Lancer PGP



PGP 7.4

Utiliser l'icône PGPTools (Sous Windows : Menu Démarrer, sous-menu Programmes puis groupe PGP). Elle ouvre une barre d'outils mobile (voir image ci-dessous).
Pour quitter PGP, il suffit de fermer cette barre d'outils en cliquant sur la croix en haut à droite.

PGP 8 sous Windows XP

Cliquer sur le petit cadenas dans la barre des tâches, à côté de l'heure.

Distribuer votre clé publique (pour que l'on puisse vous envoyer des fichiers cryptés)

- Cliquer sur le bouton "gestion des clés" (voir schéma ci-dessus) ou, pour PGP 8, cliquer sur "PGP Keys";
- Menu "Keys", choix "Export" ;
- Choisir le dossier d'export de votre clé publique et le nom du fichier (Exemple : votre nom de famille, en laissant l'extension ".asc") et cliquer sur "enregistrer" ;
- Envoyer le fichier obtenu à vos correspondants, par exemple en pièce jointe d'e-mail.
- Fermer la fenêtre PGPKeys

Sauvegarder vos clés

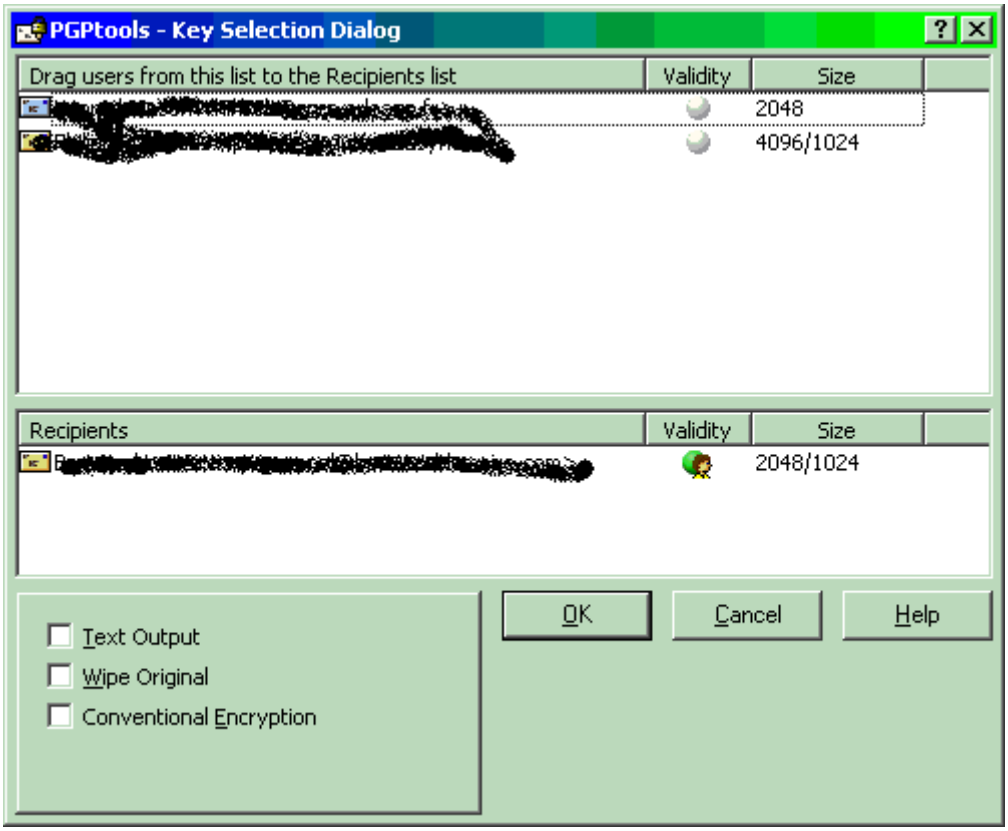
- Cliquer sur le bouton "gestion des clés" (voir schéma ci-dessus) ou, pour PGP 8, cliquer sur "PGP Keys" ;
- Menu "Keys", choix "Export" ;
- Cocher, en bas à gauche, la case "Include private key"
- Choisir le dossier d'export de vos clés publique et privé ainsi que le nom du fichier (Exemple : votre nom de famille, en laissant l'extension ".asc") et cliquer sur "enregistrer" ;
- NE JAMAIS DONNER CE FICHIER. Sauvegardez le dans un endroit sûr puis détruisez le de votre disque dur.
- Fermer la fenêtre PGPKeys.

Note : si vous vous faîtes voler votre clé privée, il faut encore que le voleur possède votre mot de passe pour s'en servir.

Importer la clé publique d'un correspondant (pour que vous puissiez lui envoyer des fichiers cryptés)

- Télécharger la clé d'un correspondant (soit par e-mail, soit sur ce site) et l'enregistrer sur votre disque dur (conseil : dans le répertoire PGP, dans "Mes Documents" sous Windows)
- Cliquer sur le bouton "gestion des clés" (voir schéma ci-dessus) ou, pour PGP 8, cliquer sur "PGP Keys";
- Menu "Keys", choix "Import" ;
- Sélectionner le fichier approprié puis "ouvrir" (Note : l'importation n'a pas à être répétée pour des opérations successives de cryptage).

Crypter et signer un fichier



PGP 7.4

- Cliquer sur le bouton "signer et encrypter"
- Sélectionner le fichier à encrypter
- Faîtes un cliquer-glisser (draguez) pour chaque destinataire de la liste des destinataires possibles (en haut, ceux dont vous avez la clé publique) vers la liste des destinataires de ce fichier (en bas) - Note : Par défaut, vous êtes vous-mêmes destinataire (conseil : le rester ! Il vaut mieux pouvoir décrypter ses propres fichiers...). Pour une sauvegarde cryptée, vous êtes le seul destinataire. Cliquer sur OK.
- Dans la zone blanche, saisir votre mot de passe.
- Dans le répertoire du fichier choisi, il y a maintenant un fichier ayant le même nom mais avec l'extension "pgp" : c'est votre fichier crypté, celui à faire parvenir à vos correspondants.

PGP 8 sous Windows XP

Faire un clic droit sur le fichier. Choisir le sous-menu PGP et cliquer sur l'option adéquate.

Décrypter un fichier

PGP 7.4

- Cliquer sur le bouton "décrypter" ;
- Sélectionner le fichier à décrypter ;

- Taper votre mot de passe dans la zone blanche ;
- Sélectionner le répertoire de destination puis cliquer sur "enregistrer"

PGP 8 sous Windows XP

- Double cliquer sur le fichier ayant l'extension ".pgp" ;
- Taper votre mot de passe dans la zone blanche ;
- Le fichier décrypté apparaît dans le même répertoire que le fichier crypté.

Petit didacticiel de GnuPG

GnuPG est un logiciel de cryptage open-source utilisant le principe des clés privées / clés publiques. Il existe sur de multiples systèmes d'exploitations. Au contraire de PGP, il est nativement en mode "ligne de commande" et son utilisation graphique requiert donc un composant additionnel. Le tutorial qui suit prend en compte la version Windows 9x/2000/XP et l'interface graphique GPGShell, au look "PGPlike".
ATTENTION : Les clés publiques de PGP sont compatibles avec celles de GnuPG, mais pas les clés privées => vous pouvez échanger des fichiers cryptés entre utilisateurs de PGP et de GnuPG mais vous ne pouvez pas vous "convertir" de l'un à l'autre sans recréer une paire de clés.

Installer le programme de cryptage GnuPG (gratuit)

Le site de référence est http://www.gnupg.org. Vous y trouverez les versions les plus récentes du produit et une documentation complète. GPGShell est un produit gratuit de Jumaros.
1) Téléchargez les composants.
2) Créez un répertoire facile à retrouver au nom ayant moins de 8 caractères (exemple : c:\gnupg). Décompressez GnuPG dedans. Le répertoire choisi doit être dans le Path du système. Sous Windows 2000/XP, le fichier autoexec.bat est un fichier système caché. Le plus simple est d'ouvrir une fenêtre "ligne de commande" et de lancer l'éditeur texte du Dos (edit c:\autoexec.bat). Il faut alors ajouter le répertoire dans la ligne de path. Si autoexec.bat est un fichier vide, il suffit de taper, dans notre exemple : path c:\gnupg. Enregistrer et quitter.
3) Décompressez le runtime de Visual Basic 4 dans un répertoire temporaire et copiez tous ses fichiers dans c:\windows\system32. Bien évidemment, ne pas remplacer les fichiers existants. Détruire ensuite ce répertoire temporaire.
4) Décompressez GPGShell dans un répertoire temporaire. Lancez la procédure d'installation automatique puis détruire ce répertoire temporaire.
5) Redémarrez le PC. GPGShell est désormais lancé au démarrage et une icône est désormais présente dans la barre des tâches, juste à côté de l'horloge (un petit cadenas vert). Cette icône permet de lancer rapidement les principales opérations.

Générer une paire de clés avec GnuPG / GPGShell

Pour générer une paire de clés, utilisez GPGKeys, l'un des composants de GPGShell. Dans le menu Keys, cliquez sur New et laissez vous guider. Repérez le KeyID de votre clé publique.
Faîtes un clic droit sur votre paire de clés. Choisissez subkeys. Cliquez sur votre clé privée puis cliquez sur copy to clipboard pour copier le KeyID de votre clé privée puis close. Dans le menu preferences, choisissez GnuPG. Dans la zone [Default Key], collez le KeyID de votre clé privée. Sauvegardez et fermez.

Importer une clé publique avec GnuPG / GPGShell

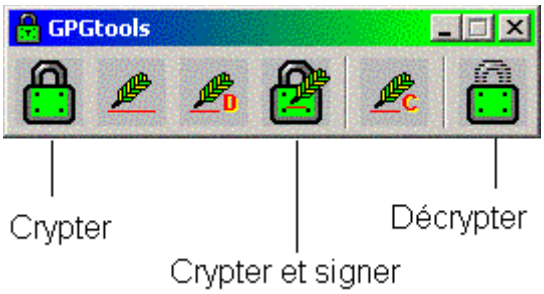
Pour importer une clé publique d'un de vos correspondants, utilisez GPGKeys, l'un des composants de GPGShell. Dans le menu Keys, cliquez sur Import, allez chercher le fichier adéquat (dont l'extension doit être asc).

Exporter une clé publique (dont la sienne) avec GnuPG / GPGShell

Pour exporter une clé publique à l'attention de l'un de vos correspondants, ouvrez une fenêtre "ligne de commande" (Sous Windows 2000/XP, cela s'appelle une "invite de commande" et le raccourcis est dans le groupe "accessoires"). Placez vous dans le répertoire de GnuPG (dans notre exemple : cd\gnupg). et tapez l'instruction suivante : gpg -o publickey.asc --armor --export 0xKKKKKKKK. (0xKKKKKKKK est le KeyID de la clé à exporter, publickey le nom du fichier à obtenir). Quitter la fenêtre "ligne de commande" en tapant "exit" puis récupérez le fichier publickey.asc (ou sous le nom que vous lui avez donné).

Crypter un fichier avec GnuPG / GPGShell

Pour crypter un fichier, utilisez GPGtools, l'un des composants de GPGShell (voir image ci-dessous). Cliquez sur "crypter" ou "crypter et signer". Choisir le fichier à crypter (il ne sera pas détruit) puis cliquez sur ouvrir. Choisir ensuite votre/vos destinataire(s) (éventuellement par une sélection multiple dans la liste, en cliquant sur chacun en maintenant la touche CTRL du clavier enfoncée) + OK. Vous passez alors en mode texte. Suivez les instructions (tapez votre mot de passe. Si le logiciel vous signale qu'une clé (ou plusieurs) n'est pas certifiée, confirmez (à chaque fois) le cryptage en tapant Y puis Entrée). N'oubliez pas de vous mettre dans la liste des destinataires (faute de quoi, vous ne pourrez plus décrypter le fichier !). Le fichier crypté a l'extension "gpg" par défaut.



Décrypter un fichier avec GnuPG / GPGShell

Pour décrypter un fichier, utilisez GPGtools, l'un des composants de GPGShell (voir image ci-dessus). Cliquez sur le bouton pour décrypter, choisissez votre fichier crypté et suivez les instructions.