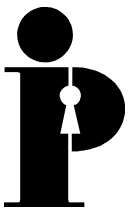
Commissaire à
l'information et à
protection de la
vie privée/Ontario

Le chiffrement du courrier électronique : Rien de plus simple!



Ann Cavoukian, Ph.D.
Commissaire
Août 1999

Cette publication est également disponible sur le site Web du Bureau du commissaire à l'information et à la protection de la vie privée/Ontario.

This publication is also available in English.

Le Bureau du commissaire remercie Mike Gurski de sa contribution au présent document.

Le Bureau du commissaire aimerait remercier de façon toute spéciale Jim Heath, de Viacorp, société de communication établie en Australie, pour avoir si généreusement fourni temps et expertise à la révision de ce document. M. Heath a déjà prodigué ses conseils aux secteurs privé et public sur la sécurité du courriel.

Commissaire à l'information et à la protection de la vie privée/Ontario

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
M4W 1A8

416-326-3333
1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site Web : www.ipc.on.ca

Table des matières

Le chiffrement du courrier électronique : Rien de plus simple![1]

Introduction

Tout le monde peut-il lire vos messages de courrier électronique? Si vous répondez oui, alors le chiffrement du courrier électronique pourrait s'avérer un luxe coûteux. Cependant, si votre courrier électronique est de nature confidentielle ou personnelle ou s'il contient des renseignements commerciaux, il est fort probable que le chiffrement constitue une nécessité.

À moins que vous ayez vécu en ermite au cours des dernières années, les médias vous ont déjà abruti avec un paquet d'histoires sur les dangers du courrier électronique non chiffré.[2] Il n'en reste pas moins que 99 % de tout le courrier électronique voyage sur Internet sans protection aucune.[3]

Un message électronique non chiffré peut rebondir de Toronto à Bruxelles à New York Il peut se rendre n'importe où, à vrai dire. Tout dépend du niveau de « trafic » Internet ce jour-là. Un message électronique peut traverser plusieurs systèmes informatiques en transit vers sa destination finale. Par ailleurs, il peut se trouver, dans certains ordinateurs servant de relais à ce message, des espions (*sniffers*) ou autres outils logiciels qui ne vous veulent aucun bien. Ils ne demandent rien de mieux que de copier, modifier ou trafiquer ce message d'une façon ou d'une autre. Certains recherchent des noms ou des mots clés. D'autres veulent savoir votre numéro de carte de crédit ou votre mot de passe d'entrée en communication (*log-in*).

Les personnes qui utilisent un système quelconque de chiffrement peuvent croiser les bras au-dessus de leur clavier. Ils n'en ont pas moins des sueurs froides chaque fois que l'on rapporte un nouveau défaut de leur cuirasse de sécurité. Certains de ces défauts se retrouvent dans les outils de chiffrement. Le plus souvent, cependant, ce sont les applications qui font appel à ces outils de chiffrement qui ont de bogues. Les logiciels de navigation Internet (*browsers*) y sont très exposés à cause de leur taille et de leur complexité. Même si le chiffrement du message demeure sûr, les bogues de l'application peuvent laisser la porte arrière du système entrouverte et faire du chiffrement du courrier une précaution inutile.

Les utilisateurs de Netscape Communicator et de MS Internet Explorer ont éprouvé bien des frissons depuis que ces logiciels de navigation se sont ouverts au chiffrement du courrier électronique. Communicator 4.0 avait un bogue permettant aux sites Web d'avoir accès aux renseignements contenus sur le disque dur de leurs visiteurs. Plus récemment, Explorer 5 avait des défauts permettant aux pirates Internet d'avoir accès aux dossiers du système de l'utilisateur.[4]

---

[1] Einstein est réputé avoir dit : « Simplifiez tant que vous pouvez mais pas plus que vous pouvez. »

[2] http://www.wired.com/news/news/technology/story/20481.html

[3] E-mail Privacy, Dave Kosiur, Help Channel ZDnet.

[4] http://www2.pcworld.com/news/daily/data/0697/970618170431.html et http://www2.pcworld.com/heres_how/article/0,1400,10579,00.html

Le Bureau du commissaire à l'information et à la protection de la vie privée/Ontario ne recommande pas les produits ou services associés aux sites mentionnés dans ce document, non plus qu'il ne garantit les renseignements fournis par ces sites.

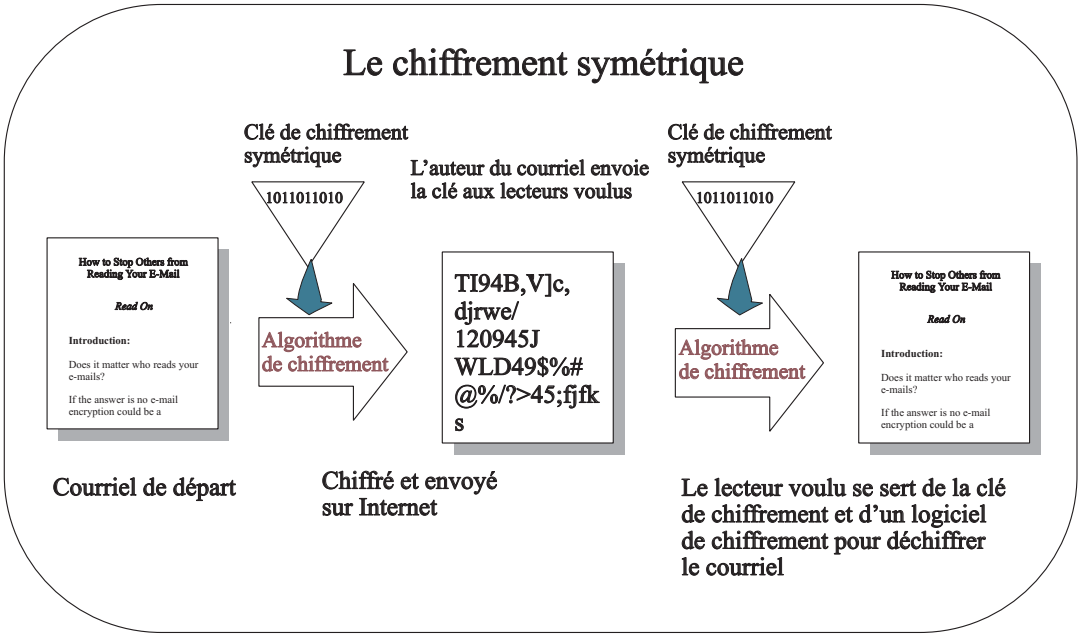
Qu'est-ce que le chiffrement du courrier électronique et comment fonctionne-t-il?

Il semble qu'il ne se passe pas une journée sans qu'un nouveau produit de chiffrement du courriel n'arrive sur le marché. Chacun de ces produits prétend avoir le meilleur algorithme de chiffrement possible et garantit une sécurité à l'épreuve de toute attaque. Avant qu'un particulier ou qu'une société décide d'acquérir ou d'utiliser un produit, il convient de procéder à une recherche et à une analyse. Le présent document ne peut tenir lieu de recherche mais il n'en tentera pas moins d'indiquer certaines étapes nécessaires.

Il y a plus de 800 programmes de chiffrement sur le marché présentement. La « qualité » de ces produits varie. Certains sont sûrs (ceux que des tierces parties ont testés sans réussir à les décrypter). D'autres sont faibles (ceux qui peuvent être déchiffrés en quelques secondes par « un expert dans le domaine »). Certains, enfin, sont tout simplement dangereux (les produits non testés).

Le chiffrement par clé symétrique

Au coeur de tout programme de chiffrement symétrique se trouvent les clés cryptographiques. Une clé n'est rien de plus qu'un nombre binaire composé de 1 et de 0 (ex. : 11001010110101000111001010 1). L'auteur crée une « phrase passe ». Le programme de chiffrement crée à son tour une clé à partir de cette phrase passe. Cette clé servira à la fois à chiffrer et à déchiffrer le courriel dans le cadre d'un « programme cryptographique à clé symétrique ». Ceci signifie que le destinataire voulu (et personne d'autre) doit recevoir copie de la phrase passe par un autre moyen sécuritaire. Le programme de chiffrement se sert de la clé pour brouiller ou chiffrer le contenu du message. Les programmes de chiffrement symétrique sont innombrables. Nommons tout de même Pkzip, Blowfish, Des et Idea.



Bien entendu, si l'auteur se sert de la même clé pour tous ses messages, il pourrait avoir des problèmes. L'auteur peut empirer ces problèmes si sa phrase passe ne se compose que d'un mot ou de quelques mots. Il suffit de quelques secondes à un pirate équipé d'un outil de bidouillage utilisant un dictionnaire pour élucider un tel système. C'est la raison pour laquelle les autorités incitent les auteurs à créer des phrases passes longues et complexes comportant des chiffres, des lettres et des caractères de clavier en haut et bas de casse. Reste encore à savoir de quelle façon l'auteur du courriel communiquera sa phrase passe aux destinataires voulus de façon sécuritaire…

Le chiffrement asymétrique

En 1976, Whitfield Diffie et Martin Hellman, professeur de l'université Stanford, inventaient ce que les experts ont qualifié du plus important progrès cryptographique des temps modernes. Ils ont mis au point un système permettant de communiquer en toute confidentialité. Un an plus tard, un groupe du MIT se servait de la théorie Diffie-Helman pour lancer RSA (d'après Ron **R**ivest, Adi **S**hamir et Leonard **A**dleman). RSA livrait la cryptographie asymétrique au grand public. (Les services secrets britanniques l'avaient inventée bien des années auparavant mais ne l'avaient jamais partagée avec le public.)[5]

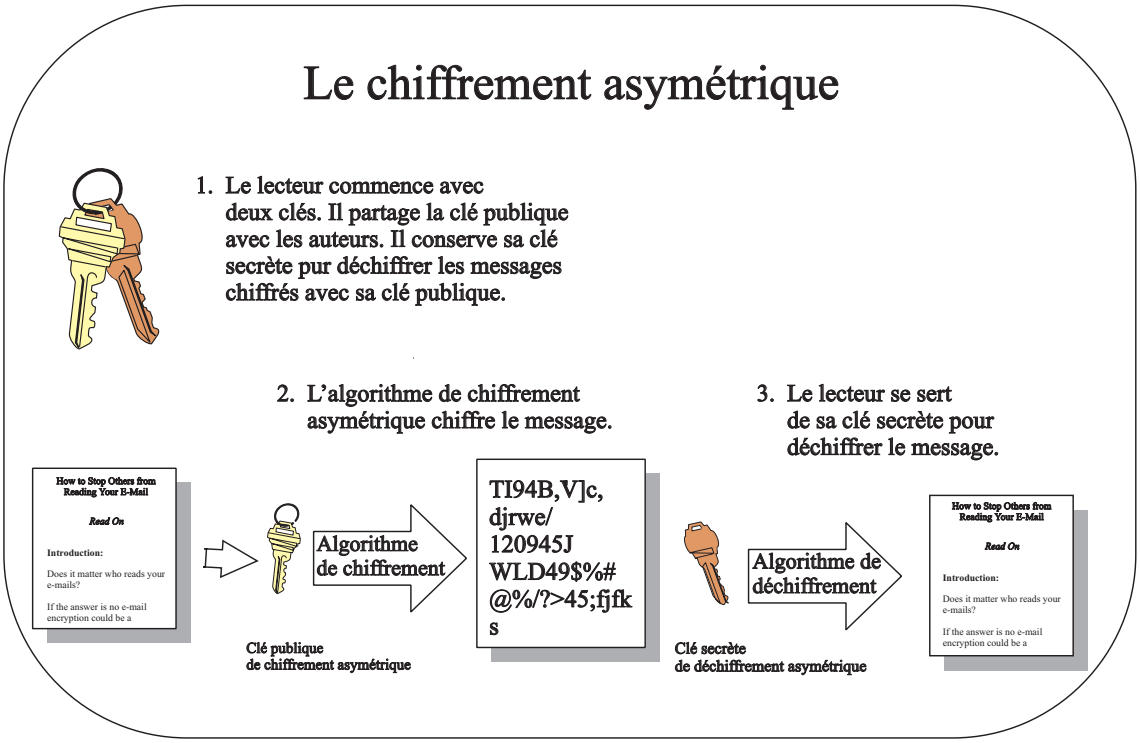
Un logiciel RSA est capable de générer une paire de clés pouvant servir à la fois au chiffrement et au déchiffrement d'un message. Chaque clé est constituée d'un grand nombre entier. Ces deux nombres sont reliés par un certain rapport mathématique. Chacune de ces deux clés peut servir au chiffrement d'un message par un logiciel de chiffrement. L'autre clé sert ensuite à déchiffrer le message.

Le lecteur peut partager une clé, appelée la clé publique, avec les auteurs voulus. La clé secrète du lecteur, par contre, demeure privée. Lorsqu'un auteur reçoit la clé publique du lecteur, il s'en sert pour chiffrer l'information. L'auteur peut alors envoyer un message chiffré. Le lecteur peut ensuite déchiffrer le courriel de l'auteur à l'aide sa propre clé secrète. Autrement dit, l'auteur chiffre le message à l'aide de la clé publique du lecteur voulu. Le lecteur déchiffre ensuite le message à l'aide sa clé secrète. Ce concept fait toujours un peu sourciller au début. (Voyez l'illustration plus bas.)

Le chiffrement asymétrique résout le problème du partage de la même clé, élément essentiel du chiffrement symétrique.[6] Le chiffrement asymétrique constitue un important progrès. Il exige cependant beaucoup de travail pour l'ordinateur. S'en servir pour chiffrer et déchiffrer tout son courrier électronique essoufflerait rapidement l'ordinateur personnel moyen.

[5].http://www.wired.com/wired/archive/7.04/crypto.html

[6] http://www.viacorp.com/crypto.html et http://www.rsa.com/rsalabs/faq/index.html



Il est aujourd'hui courant dans la plupart des application de chiffrement d'utiliser le chiffrement asymétrique pour le chiffrement de la seule clé symétrique. On choisit cette clé au hasard et le programme en génère une nouvelle pour chaque message. Rappelez-vous que la clé symétrique sert à chiffrer le message. Le lecteur voulu du courriel chiffré de l'auteur peut alors déchiffrer la clé symétrique en utilisant sa propre clé secrète. Après quoi, la clé symétrique déchiffre le message. Heureusement, le programme de chiffrement fait tout ceci en coulisses de telle sorte qu'on n'a pas besoin de mémoriser des nombres premiers de 300 chiffres ou de manipuler de longues séquences binaires.

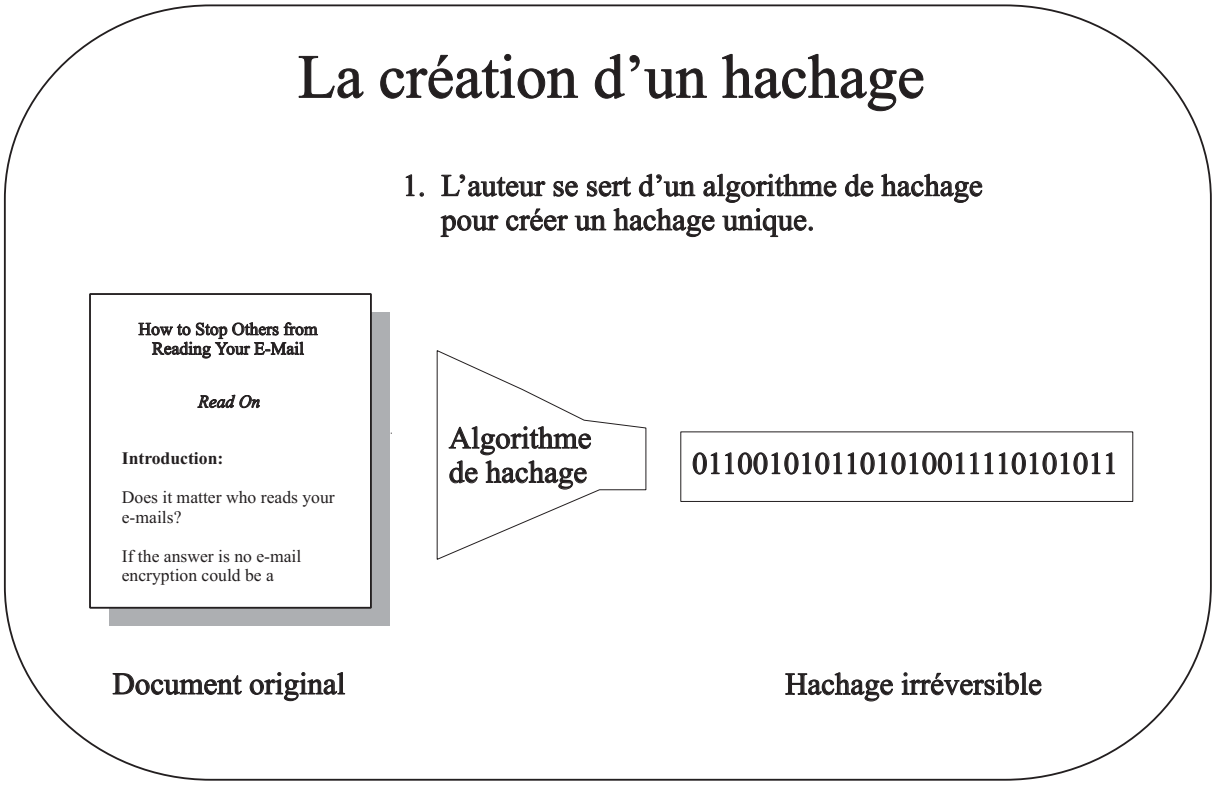
Les signatures numériques

La plupart des outils de chiffrement du courrier électronique comportent un autre élément. Ils offrent, en plus d'algorithmes de chiffrement, la signature numérique. Celle-ci assure le lecteur du courriel que personne n'a trafiqué le message et que celui-ci a bien été envoyé par son auteur présumé.

Pour ce faire, la signature numérique comporte deux éléments d'information : un hachage (ou adressage calculé) et la clé secrète de l'auteur. Parlons d'abord du hachage. Le logiciel crée le hachage qui est une longue séquence de uns et de zéros particulière au message de l'auteur. Le logiciel arrive à cette séquence en brouillant le message. Imaginez des oeufs brouillés et des boulettes rissolées de pommes de terre en hachis que les Américains appellent *hash browns*, dans la poêle à frire. Le logiciel comprime le tout, numériquement s'entend. Imaginez que l'on puisse réussir à comprimer les oeufs brouillés et le hachis de pommes de terre pour que le tout tienne dans un coquetier. Le hachage, c'est ça : ce qui reste au fond du coquetier.

Le logiciel de chiffrement ne peut créer qu'un seul hachage possible à partir d'un message donné. Il pourrait cependant exister d'autres messages dont la compression produirait le même hachage. Il serait cependant impossible de retrouver ces autres messages. Aussi improbable que ce soit, il est toujours possible de trouver un message différent qui produise le même hachage. Cet autre message serait cependant presque certainement illisible ou absurde.

On ne peut « désosser » un hachage, c'est-à-dire qu'on ne peut remonter à sa source : il s'agit d'un processus irréversible. La hachage numérique ressemble beaucoup au hachis du coquetier. Il est impossible d'en extraire des oeufs dans leur coquille et des pommes de terre non pelées. De la même façon, il est impossible de se servir du hachage numérique pour reconstruire le message original ou pour créer un message différent donnant le même hachage. Un hachage comporte habituellement 128 bits.

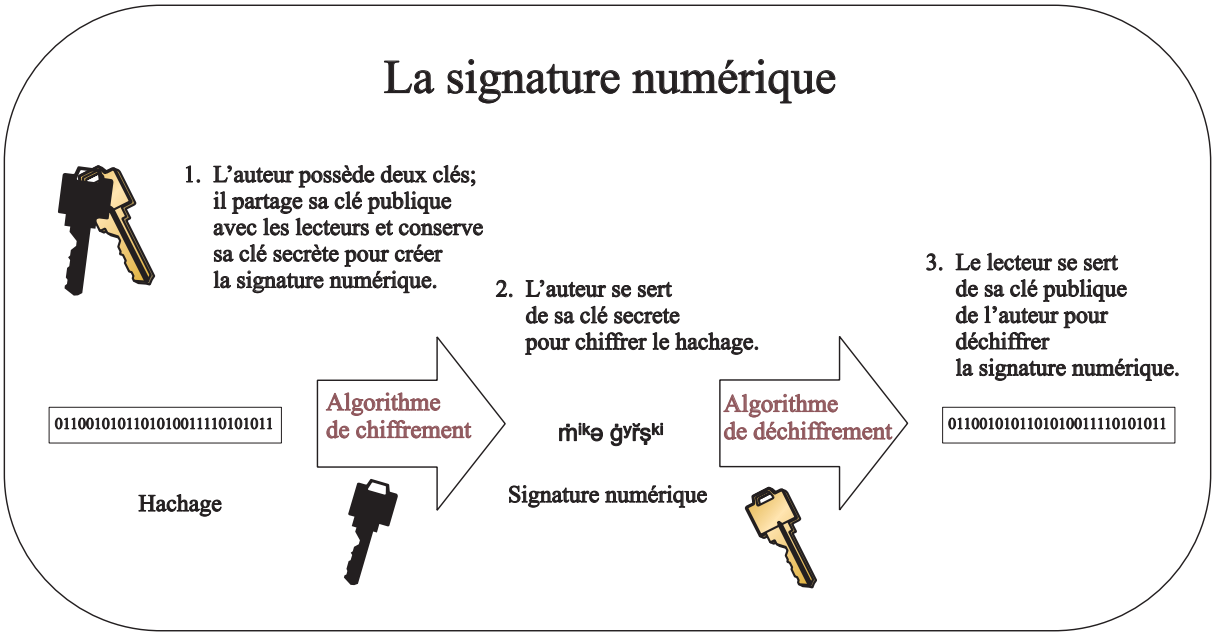


La deuxième étape consiste à chiffrer le hachage. L'auteur chiffre le hachage en se servant de sa clé secrète. Et cela donne une signature numérique. Le lecteur peut déchiffrer le hachage chiffré en se servant de la clé publique de l'auteur. Le logiciel de chiffrement du lecteur voulu vérifie si le message de l'auteur recrée le même hachage. Ceci prouve que personne n'a trafiqué le message.

Les signatures numériques fonctionnent à l'inverse des messages ordinaires. L'auteur chiffre le message sortant avec sa clé secrète. Il expédie ensuite sa clé publique pour que ses lecteurs puissent vérifier l'authenticité du hachage. Le lecteur peut ainsi s'assurer que seul cet auteur a pu chiffrer et expédier le message. Seul l'auteur possède la clé secrète qui permet au système de fonctionner. Le point faible est la complexité des clés créées par l'utilisateur. Une façon sûre de procéder est d'utiliser un minimum de 230 chiffres.

Le chiffrement du courrier électronique fait de plus en plus souvent partie des progiciels dont l'utilisateur se sert de façon transparente. Ces produits s'adressent aux organismes des secteurs privé et public plutôt qu'aux utilisateurs individuels. Pour s'en servir, « les utilisateurs n'ont pas besoin de savoir quoi que ce soit sur la sécurité ». Et, ce qui est encore plus important, il n'ont pas à mémoriser des clés de 230 chiffres!

Par contre, les décideurs de ces organismes ont besoin d'en savoir un peu plus long. Pour commencer, ils doivent garder à l'esprit que l'on ne peut effectuer le balayage des virus sur le courrier chiffré au niveau du coupe-feu ou de l'application anti-virus. Ceci s'applique également au courriel chiffré expédié et reçu par l'organisme. Une solution consiste à arrêter les messages chiffrés au coupe-feu et à les déchiffrer à cette étape du parcours. Une autre solution est de déchiffrer les messages au niveau du serveur ou de l'ordinateur personnel et d'effectuer l'opération de balayage des virus à ce moment-là.[7]



Types de produits de chiffrement du courrier électronique

La plupart des produits de chiffrement du courrier électronique comportent l'une des caractéristiques décrites plus haut. Ils se divisent cependant en deux standards ou protocoles principaux. Les standards ad hoc et de facto sont : le protocole S/MIME V. 3 et le protocole Open PGP. S/MIME V. 3 signifie « Secure Multipurpose Internet Mail Extension, Version 3 » (extension de courrier Internet multi-tâches sécuritaire, version 3). Open PGP signifie « Open Pretty Good Privacy » (protocole ouvert d'assez bonne confidentialité). Dans la pure tradition des standards ad hoc rivaux, ils sont incompatibles. Cette incompatibilité est sans doute permanente. S/MIME V. 3 vient d'être

[7] http://www8.zdnet.com:80/pcweek/stories/news/0,4153,1015432,00.html

[8] http://www.imc.org/smime-pgpmime.html

reconnu standard approuvé du groupe Internet Engineering Task Force (IETF). Le groupe IETF travaille aujourd'hui à créer également un standard Open PGP avant la fin du millénaire.[8] L'existence de deux protocoles incompatibles n'est pas un problème pour la compagnie qui décide de n'utiliser qu'un seul protocole dans ses communications internes. Mais cela représente un défi de taille lorsque vient le temps de communiquer de façon sécuritaire avec une foule d'organismes externes ou de particuliers qui ont choisi d'utiliser des produits incompatibles.[9]

En plus de devoir choisir quel protocole utiliser, le consommateur doit arrêter son choix sur un produit. C'est ici que les choses se compliquent. Ce qui suit ne constitue qu'un échantillon restreint des divers produits offerts :[10]

1. Les services de chiffrement du Web fournissent à l'utilisateur un compte de courrier électronique sur un site Web et le logiciel de chiffrement directement sur ce site. Le site Web jour le rôle de contrôleur de trafic pour le courriel de l'utilisateur :

    - http://www.ZipLip.com
    - http://www.Hushmail.com

Il est facile d'utiliser les systèmes des sites Web. On n'a qu'à suivre la liste d'instructions. Il faut cependant savoir que certains systèmes de chiffrement de courrier électronique du Web exigent que l'auteur et le lecteur s'inscrivent tous deux au site Web pour chiffrer et déchiffrer le courrier.

2. Les applications d'ordinateur personnel (OP) s'installent sur l'OP ou sur le réseau de l'utilisateur :

    - http://www.jawstech.com
    - http://www.pgpi.com
    - http://www.cypost.com
    - http://www.ancort.ru/
    - http://abi.hypermart.net
    - http://www.invisimail.com
    - http://www.cybergs.com/~issonline/
    - http://www.symantec.com

Les applications sur OP varient par leur niveau de convivialité et de force. Il est toujours préférable de choisir celles que les magazines spécialisés ont testées et auxquelles ils ont conféré le titre tant convoité de « choix de la rédaction ». La plupart des produits d'aujourd'hui ont fait du chiffrement du courriel l'affaire d'un ou deux cliquetis après l'installation du programme. Ceci constitue une nette amélioration sur la situation d'il y a à peine un an. Ces produits pour OP ne dépendent en rien du fournisseur de service Internet avec qui vous faites affaire et s'installent en quelques cliquetis de la souris.

---

[9] Pour une étude plus approfondie de ces deux protocoles, voyez un article de Dave Kosiur, sur le zdnet Help Channel, 28 avril 1999, intitulé « E-mail Privacy »: http://www.zdnet.com/zdhelp/. Cet article n'est pas directement accessible. Une fois à l'adresse URL, tapez « email » dans la fenêtre de recherche et choisissez « Internet » dans le fenêtre des catégories. Dans les renseignements complémentaires, cliquez sur « E-mail Privacy (How to) ».

[10] Le Bureau du commissaire à l'information et à la protection de la vie privée ne recommande aucun des produits de cette liste ni aucun autre produit. Cette liste est fournie uniquement comme outil de référence.

3. Les infrastructures de clé publique fournissent un service complet de sécurisation des organismes :

    - http://www.entrust.com
    - http://www.verisign.com

    Ces solutions comportent une foule d'autres services en plus du chiffrement courriel de base, depuis la sécurisation des sites Web jusqu'à la gestion de l'authentification. Ceci comprend le traitement de tous les certificats numériques (par lesquels une tierce partie garantit votre identité) requis par l'organisme pour acheminer l'information de façon sécuritaire. Ces produits sont virtuellement transparents pour l'utilisateur.

4. Les application hybrides offrent le chiffrement du courriel et d'autres caractéristiques comme les anonymiseurs/pseudonymiseurs qui effacent tout lien entre l'utilisateur et les traces électroniques qu'il peut laisser derrière lui dans sa navigation sur Internet :

    - http://www.zeroknowledge.com
    - http://www.proxymate.com

    Le logiciel prometteur Freedom de Zero Knowledge en était au stade de développement bêta en août 1999. Selon la compagnie, ce logiciel :

    - gère toutes vos identités numériques, surveille le trafic sortant pour s'assurer qu'il ne contient pas de renseignements personnels, chiffre automatiquement la communication et la dirige vers le réseau Freedom, déchiffre en transparence tout trafic entrant, gère les témoins de navigation (*cookies*) et filtre le multipostage abusif (*spam*).

    Le service Proxymate n'offre pas le chiffrement du courriel mais fournit des pseudonymes. Ce service est facile à installer et à utiliser. Ce service de mandataire assure l'anonymat des utilisateurs qui surfent sur Internet. Après l'inscription (le logiciel offre une option d'installation automatique), les seules autres étapes sont l'entrée d'un nom d'utilisateur et d'un mot de passe lors du lancement du logiciel de navigation (*browser*). Proxymate fournit des pseudonymes aux sites Web qui exigent le nom et l'adresse électronique de l'utilisateur. Ce service constitue en fait une cloison protectrice opaque…mais d'usage transparent pour l'utilisateur.

5. Les outils de chiffrement de Netscape Communicator et d'Internet Explorer nécessitent l'achat d'un certificat numérique (avec période d'essai gratuit de 60 jours) d'une tierce partie comme Verisign. Les fournisseurs ont simplifié le processus et l'ont parfaitement intégré pour installation et utilisation sur logiciel de navigation. Attendez-vous cependant à payer de 10 $ à 20 $ par année pour votre carte d'identité numérique. Les fournisseurs offrent également un tarif d'entreprises.

Prochaines étapes

Une fois que l'utilisateur ou l'organisme a fait sa recherche et a commencé à explorer le marché des produits de chiffrement du courrier électronique, il devient très important de se poser les questions suivantes :

1. Le code de chiffrement a-t-il été testé?

Ceci suppose que le code a été mis à la disposition des testeurs. Les codes non testés sont des outils dangereux, comme Netscape s'en est rendu compte avec Communicator 4. Netscape a publié le code de Communicator 5 aux fins de mise à l'épreuve. Mais ce ne sont pas toute les compagnies qui procèdent ainsi. Les meilleurs tests sont le fait de tierces parties associées à des organismes universitaires spécialisés en cryptographie. Le Centre for Applied Cryptography de l'Université de Waterloo (http://www.cacr.math.uwaterloo.ca) en est un bon exemple en Ontario. Comme le disait Robert Morris Sr, ex-préposé principal à la recherche de la National Security Agency des États-Unis, « Il ne faut jamais sous-estimer le temps, l'argent et les efforts que certains peuvent dépenser pour briser un code. »

2. S'agit-il d'un logiciel de chiffrement stabilisé?

Un logiciel est dit stabilisé lorsqu'il est utilisé depuis au moins trois ans et qu'il est toujours en service après avoir été testé et révisé. En 1997, le magazine *PC* a fait la critique de plusieurs systèmes de chiffrement du courrier électronique. Deux ans plus tard, certains de ces produits et de leurs fabricants sont impossibles à retracer ou, ce qui est encore pire, ont peut-être cessé d'exister.

3. Ce logiciel répond-il aux besoins de votre organisme ou à vos préférences personnelles?

L'utilisateur doit évaluer si ce produit peut convenir au volume des messages électroniques existant. Il doit décider si le produit offre la protection voulue. Par ailleurs, si le contenu des messages électroniques n'offre qu'un intérêt limité pour les autres, on devrait utiliser un produit comme Pkzip. On se sert couramment de ce programme utilitaire pour comprimer les dossiers par chiffrement symétrique. Un mot de passe complexe peut suffire à la tâche. Il suffit de changer de mot de passe souvent et d'éviter les noms de dossiers décrivant trop bien leur contenu, ce qui fournit de précieux indices aux espions éventuels.

4. Quelle est la courbe d'apprentissage et la facilité d'utilisation du produit?

Cela revient souvent à dire : combien de touches de clavier faut-il pour chiffrer et déchiffrer un courriel? Cela signifie également le temps et le nombre d'étapes nécessaires pour acquérir les certificats numériques (qui évitent d'avoir à mémoriser et à gérer un grand nombre de mots de passe).[11]

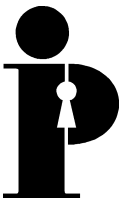
[11] http://www.netscape.com/security/basics/getpercert.html

Conclusion

Le chiffrement du courrier électronique est un outil très puissant dans la protection de la vie privée. Le présent document a tenté d'en expliquer les concepts de base. Le commissaire à l'information et à la vie privée encourage les lecteurs à mettre en pratique ces nouvelles connaissances et à étudier activement l'utilisation d'un logiciel de chiffrement du courriel.

Puisque ce document n'offre qu'un bref aperçu du sujet, nous proposons aux lecteurs de visiter les sites Web mentionnés pour acquérir une compréhension encore plus complète de la question. Il est toujours utile de commencer avec une liste de vos exigences. Une telle liste peut servir à évaluer tout nouveau produit. Quand vous le pouvez, faites vous-même l'essai d'un produit. Les logiciels de chiffrement vous deviendront bien vite très familiers.

Si vous ne protégez pas votre vie privée avec des outils comme le chiffrement du courrier électronique, vous risquez de la perdre. Ce qui se produit par la suite peut aller de la simple contrariété au sentiment abject d'avoir été violenté à la perte d'importantes sommes d'argent. Protégez bien votre vie privée; les outils sont déjà en place pour vous y aider.



Commissaire à l'information et à la protection de la vie privée/Ontario

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
M4W 1A8

416-326-3333
1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site Web : www.ipc.on.ca