La cryptographie

Un élément crucial pour le développement du commerce électronique

Si le réseau Internet fascine à ce point, c'est certainement grâce à la possibilité qu'il donne aux usagers d'accéder instantanément à une quantité infinie d'informations et d'interlocuteurs. Mettre à profit cette infrastructure géniale dans le cadre d'un vaste marché global est certainement un des défis économiques à relever à l'aube du troisième millénaire. Dans ce nouvel espace révolutionnaire de communication, les risques bien réels de fraudes, de falsifications et de surveillances intempestives doivent être maîtrisés afin de donner confiance aux utilisateurs et de favoriser ainsi le succès de cette nouvelle forme de commerce. C'est ici que la cryptographie moderne intervient en fournissant une panoplie de solutions adéquates et d'un usage facile en matière de sécurité des données numériques. Nous sommes convaincus du rôle croissant et positif que la cryptographie va continuer de jouer dans les années à venir. La Suisse encourage de manière générale l'emploi et le développement de cette technologie de pointe.

La cryptographie, bien plus qu'un souvenir d'enfance!

Rares sont ceux qui dans leur enfance n'ont eu recours un jour ou l'autre à des codes secrets pour protéger un message confidentiel. Certains se souviendront d'avoir voulu imiter Léonard de Vinci, qui utilisait une écriture illisible pour décrire ses inventions (écriture qui ne pouvait révéler son sens qu'à l'aide d'un miroir). D'autres repenseront aux lettres ultra-secrètes qu'ils ont écrites à leur premier amour en utilisant du jus de citron, ou alors aux petits billets codés qui circulaient sous les pupitres. Nous avons probablement aussi tous été captivés, un jour ou l'autre, par les exploits de James Bond ou d'autres agents-doubles célèbres qui excellaient dans l'emploi de messages chiffrés et de codes secrets. Nous allons découvrir maintenant que la cryptographie n'est de loin pas qu'un jeu d'enfants ou une science réservée aux militaires, mais surtout un élément crucial du commerce électronique.

Une technologie de pointe pour un secteur en ébullition

Le déploiement extraordinaire du réseau Internet est avant tout une révolution en matière d'expression humaine à l'échelle planétaire. Nous disposons à présent d'un gigantesque espace de communication permettant à notre économie de créer de nouveaux types d'entreprises, d'améliorer les canaux de distribution et d'information et de développer des méthodes originales pour prospecter le marché mondial.

Cet espace à la fois international, décentralisé et hétérogène où chacun peut agir, s'exprimer et travailler comme bon lui semble, n'est maîtrisé actuellement par aucun opérateur ni aucun Etat. C'est sur cette infrastructure prometteuse que le commerce électronique a vraiment fait son apparition. Il est aujourd'hui largement reconnu que cette nouvelle forme de commerce jouit d'un grand potentiel économique et qu'elle va jouer un rôle toujours plus grand dans le développement de notre société moderne.

Malheureusement, l'essor du commerce électronique se trouve freiné par une série de risques inhérents aux réseaux numériques ouverts du type Internet. Ceux-ci contribuent à miner la confiance des utilisateurs de cette nouvelle plate-forme de communication. L'importante croissance mondiale des réseaux numériques et le développement du commerce électronique ont ainsi entraîné inévitablement avec eux la question des mesures de sécurité prises dans ce domaine. En effet, ces réseaux, alors qu'ils sont de plus en plus importants pour notre économie avec l'augmentation de la valeur des données transmises et stockées par ces systèmes, deviennent également de plus en plus vulnérables à divers types de menaces.

L'infrastructure numérique qui se met actuellement en place constitue un environnement propice à toutes les formes de délits liés à l'informatique. Les messages confidentiels transmis sur un réseau ouvert comme le web peuvent facilement être interceptés, lus, copiés voire manipulés, et la validité des documents ou des contrats transitant par courrier électronique peut être contestée. Des informations sensibles peuvent ainsi tomber dans les mains d'un concurrent, d'un criminel ou d'un service de renseignements étranger.

Dans le monde entier par exemple, les télécommunications – téléphone, fax, courrier électronique – sont massivement surveillées par un dispositif titanesque appelé Echelon. Les services secrets américains, à la tête de ce réseau d'écoute, sont appuyés dans cette tâche par plusieurs pays alliés. On lit également fréquemment dans la presse que tel ou tel pirate s'est introduit dans le réseau informatique d'un ministère de la défense ou d'une entreprise célèbre, par pure malice, ou alors, ce qui est plus grave, pour avoir accès à des données confidentielles ou encore pour manipuler ou détruire les réseaux attaqués.

Pour pouvoir profiter pleinement des nombreuses possibilités commerciales offertes par les réseaux numériques de communication ouverts, il est indispensable de parvenir à sécuriser cette infrastructure. C'est précisément

1

La cryptographie: une définition moderne

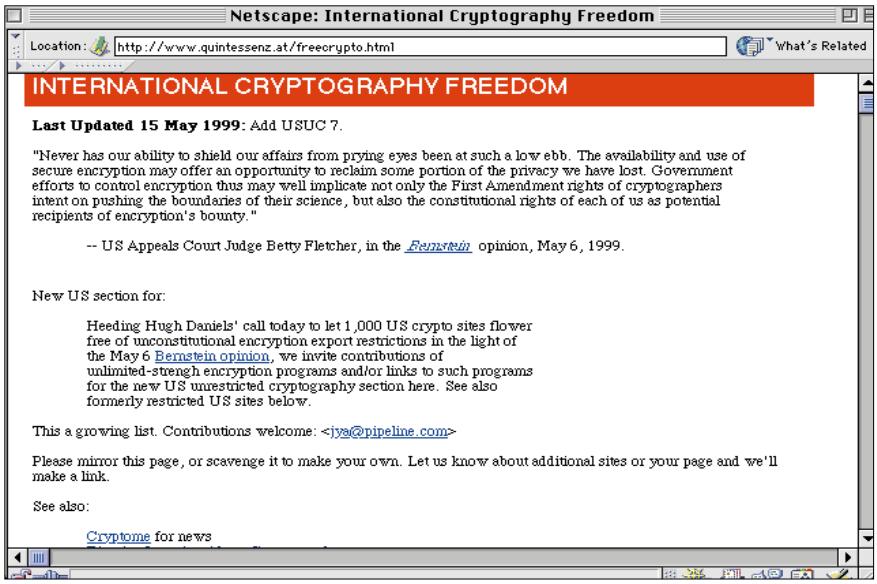
La cryptographie désigne l'ensemble des principes, moyens et méthodes de transformation des données destinés à chiffrer leur contenu, établir leur authenticité, empêcher que leur modification passe inaperçue, prévenir leur répudiation ou leur utilisation non autorisée.

Un peu d'histoire!

L'empereur Jules César fut un adepte célèbre de la cryptographie. Il faisait chiffrer ses messages secrets à Cicéron de manière à les rendre incompréhensibles à ses adversaires (avec soit dit en passant un des algorithmes les moins sûrs de l'histoire de l'humanité consistant en une rotation simple de l'alphabet: le a devenait un d, le b respectivement un e, etc.).

Quels sont les standards actuels?

En matière d'algorithmes symétriques, la longueur des clefs de chiffrement recommandée s'élève à 128 bits. Pour les algorithmes asymétriques, le standard conseillé est de 1024 bits.



ici que la cryptographie intervient. Elle nous offre des outils performants, capables de contribuer de manière significative à la sécurité sur le réseau Internet. A l'aide de logiciels cryptographiques modernes et puissants, il devient possible de garantir la confidentialité des informations échangées sur les réseaux numériques, d'identifier de façon certaine la source des informations reçues et d'offrir l'assurance que le message attribué à quelqu'un n'a pas été modifié en transit par une personne non autorisée.

La cryptographie en trois leçons

Depuis l'ancienne Egypte, en passant par presque toutes les civilisations, la cryptographie n'a cessé d'évoluer pour devenir progressivement une technologie indispensable à notre société moderne d'information. Nous allons à présent vous présenter les trois types de cryptographie les plus employés sur les réseaux numériques.

La cryptographie à clef secrète

Un des principaux buts de la cryptographie classique consiste à rendre incompréhensibles des messages secrets. En d'autres termes, il s'agit d'assurer la *confidentialité* de l'information susceptible de tomber dans de mauvaises mains.

Les systèmes de chiffrement traditionnels dits à *clef secrète*, ou *symétriques*, reposent sur le partage, entre deux interlocuteurs, d'une même clef secrète utilisée à la fois pour le chiffrement d'un message et pour son déchiffrement. Le but d'un tel système est de parvenir à garder une seule information secrète (la clef de chiffrement) à la place des messages proprement dits qui peuvent ainsi, une fois chiffrés, transiter sur des réseaux dits ouverts. La difficulté principale de cette technique est la suivante: la clef doit être remise aux interlocuteurs préalablement à la communication par un canal sûr, donc différent du canal prévu, de façon à ce qu'elle ne soit pas interceptée par des tiers non autorisés. Cette distribution préliminaire de clefs devient cependant vraiment périlleuse et même impraticable lorsqu'il s'agit de communiquer des messages chiffrés à un grand nombre de participants que l'on ne connaît pas forcément, comme c'est le cas sur Internet. Par exemple, pour un réseau comportant 100 utilisateurs, il faudrait échanger préalablement près de 5000 clefs. En doublant le nombre d'usagers, l'échange de 20 000 clefs deviendrait nécessaire(graphique 2)!

D'autres méthodes, comme la stéganographie, sont également fréquemment employées pour protéger des données confidentielles; ces procédés ont pour but de cacher le fait même de l'existence d'une information secrète (encres invisibles, etc.). Des techniques similaires sont encore utilisées de nos jours, par exemple la dissimulation d'un texte confidentiel dans les pixels numériques d'une photo digitale.

La cryptographie à clef publique

Avec l'avènement du chiffrement dit à *clef publique* ou *asymétrique*, qui caractérise la cryptographie moderne, les difficultés décrites plus haut ont été résolues. Cette technique a été développée en 1976 par Martin Hellman et Whitfield Diffie de l'université de Stanford et rapidement perfectionnée par trois mathématiciens américains du MIT: Ronald Rivest, Adi Shamir et Leonard Adleman (créateurs du fameux algorithme RSA). Grâce à ce concept, qui a d'ailleurs complètement révolutionné le domaine du chiffrement, il est devenu possible, non seulement de chiffrer les informations, mais aussi d'authentifier les messages échangés. C'est cette dernière caractéristique qui a fourni la base des signatures digitales.

La cryptographie à clef publique repose sur une idée simple: au lieu de l'échange d'une seule clef secrète, chaque usager possède une paire de clefs mathématiquement liées (c'est-à-dire différentes mais complémentaires). Il s'agit alors d'une clef publique, largement diffusée par exemple dans un annuaire électronique, à laquelle correspond une seule autre clef, la clef privée, gardée secrète par son propriétaire. Il est actuellement impossible pour un pirate de déterminer la clef privée à l'aide de la clef publique. Ce système ne permet pas de chiffrer et de déchiffrer un message avec une seule et même clef, il faut obligatoirement employer les deux clefs à disposition (privée et publique).

L'exemple suivant illustre ce procédé: un message chiffré par Alice avec la clef *publique* de Bob, ne peut être déchiffré que par la clef *privée* correspondante de Bob. De même, lorsqu'un message est signé numériquement par Alice à l'aide de sa clef *privée*, il peut être vérifié par Bob avec la clef *publique* correspondante d'Alice.

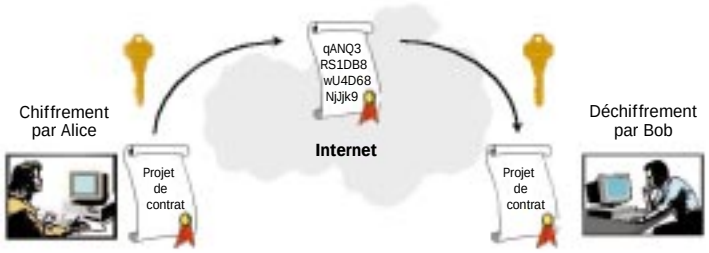
Une fonction mathématique à sens unique (*one-way function*) se cache derrière ce procédé cryptographique. L'annuaire téléphonique peut illustrer ce concept: il est facile de trouver un numéro en connaissant le nom de l'interlocuteur recherché; il est cependant beaucoup plus difficile, à l'aide de l'annuaire, de trouver son nom en étant uniquement en possession de son numéro de téléphone!

Le système à clef publique permet donc d'échanger des informations confidentielles entre des interlocuteurs qui ne se sont jamais rencontrés auparavant. Il suffit de sélectionner la clef publique du destinataire se trouvant par exemple annexée dans un courrier électronique (*e-mail*) et de chiffrer le message avec celle-ci. Le destinataire se servira de sa clef privée pour déchiffrer la communication, que nul autre n'aura pu déchiffrer, même dans le cas où le message aurait été intercepté.

Si un expéditeur veut signer un message de manière électronique, il n'a qu'à effectuer l'opération mathématique inverse à l'aide de sa propre clef privée. Concrètement, il va uniquement «cliquer» avec sa souris sur le bouton «signer» qui apparaît sur son écran! Le résultat de cette opération pourra ensuite être analysé par le destinataire du message à l'aide de la clef publique de l'expéditeur. Si le résultat n'est pas probant, le destinataire saura que le message n'a pas été signé par l'expéditeur, ou qu'il a été modifié pendant le transit.

Avec ce type de cryptographie, il devient toutefois indispensable de s'assurer que la clef publique sélectionnée correspond bien à l'interlocuteur concerné. Ceci est capital pour prévenir les risques d'usurpation d'identité dans un environnement électronique. Il faut donc que les expéditeurs et les destinataires s'assurent que les clefs publiques qu'ils utilisent sont véritablement celles des parties avec lesquelles ils souhaitent interagir. Si les parties se connaissent, il n'y a pas de grandes difficultés; par contre, si les interlocuteurs ne se connaissent pas, ce qui va à l'avenir devenir le cas le plus fréquent, il faut alors passer par l'intermédiaire d'un mécanisme officiel destiné à certifier les clefs publiques. En Suisse, Swisskey est un bon exemple d'une société spécialisée dans la certification des clefs publiques. En émettant un certificat, une entité indépendante, du type de Swisskey, confirme qu'une clef publique appartient bien à une personne ou

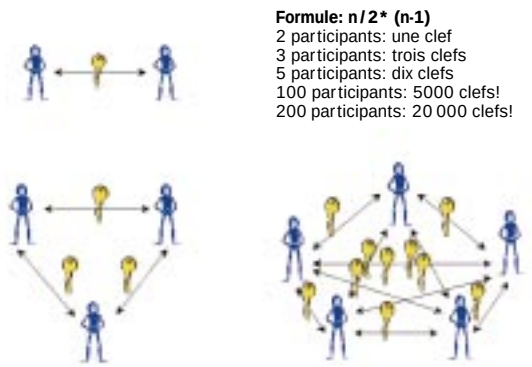
La cryptographie à clef secrète (algorithme symétrique, deux clefs identiques) Graph. 1



La clef employée pour chiffrer et déchiffrer le message est la même.

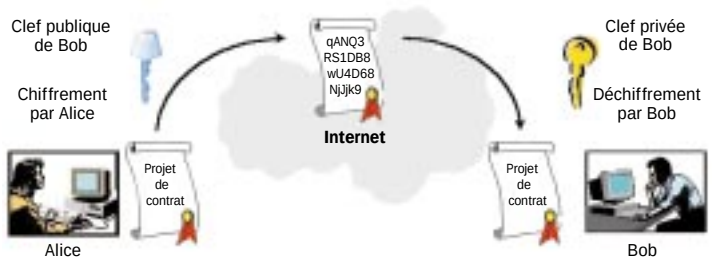
Source: OFAEE — Die Volkswirtschaft/La Vie économique

La cryptographie à clef secrète n'est pas adaptée aux grands réseaux Graph. 2



Source: OFAEE — Die Volkswirtschaft/La Vie économique

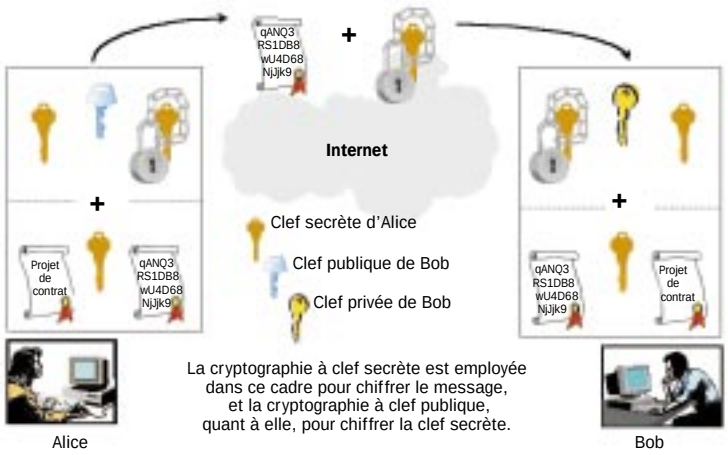
La cryptographie à clef publique (algorithme asymétrique, deux clefs différentes) Graph. 3



Les clefs employées pour chiffrer et déchiffrer le message sont différentes mais mathématiquement liées.

Source: OFAEE — Die Volkswirtschaft/La Vie économique

La cryptographie hybride Graph. 4



La cryptographie à clef secrète est employée dans ce cadre pour chiffrer le message, et la cryptographie à clef publique, quant à elle, pour chiffrer la clef secrète.

Source: OFAEE — Die Volkswirtschaft/La Vie économique

à une entreprise déterminée. On peut donc comparer ces certificats à des cartes d'identité numériques.

La cryptographie hybride

Les algorithmes de chiffrement asymétriques ont cependant également un désavantage, ils sont généralement beaucoup plus lents que les algorithmes symétriques. Ils ne conviennent donc guère au chiffrement de longs messages. Le moyen d'éviter ce désagrément est de combiner les mécanismes symétrique et asymétrique de chiffrement. Cette combinaison est appelée cryptographie hybride ou «enveloppe digitale». De nombreux biens cryptographiques fonctionnent sur ce principe, à l'exemple du logiciel culte Pretty Good Privacy (PGP).

L'exemple suivant illustre de manière simplifiée ce procédé: le texte destiné à Bob est dans un premier temps chiffré par Alice avec un algorithme symétrique rapide (p.ex. IDEA) qui emploie une clef secrète. Dans un second temps, le logiciel d'Alice va coder cette clef secrète avec la clef publique de Bob. L'algorithme de chiffrement asymétrique chiffre uniquement la clef secrète utilisée pour coder le message et non pas le message en tant que tel. Il est donc possible de chiffrer très rapidement les messages tout en bénéficiant des avantages indéniables de la cryptographie à clef publique. Ces étapes sont à présent exécutées de manière tout à fait transparente pour les usagers.

La position suisse en matière de chiffrement

Nous sommes convaincus du rôle positif que joue la cryptographie dans le cadre de ces nouvelles infrastructures numériques de communication et d'information. Le commerce électronique représente certainement une réelle chance pour un pays comme la Suisse, dont le marché national est restreint et qui dépend fortement de ses exportations. La protection des données et des infrastructures numériques est un élément clef du succès de ce nouveau marché. C'est pourquoi la Suisse poursuit une politique en tout point libérale en matière de chiffrement.

La Suisse a un intérêt évident à promouvoir les communications chiffrées au sein de ses entreprises et administrations. Les milieux économiques et l'opinion publique en général sont à cet effet continuellement sensibilisés aux risques courus (espionnage industriel, *hackers*, etc.). Les usagers potentiels de biens de chiffrement doivent toutefois pouvoir jouir de la liberté de choisir quels types de logiciels ou de produits correspondent au mieux à leurs besoins.

Un autre point important de la politique suisse en matière de cryptographie, qui est au demeurant un élément essentiel de notre politique économique extérieure en général, est de garantir à notre industrie du chiffrement un accès non discriminatoire aux marchés mondiaux de la cryptographie. Nous nous efforçons également, par la création de conditions favorables, d'encourager les entreprises suisses, dans la mesure du possible, à développer et lancer de nouveaux logiciels de chiffrement.

Une question fréquemment soulevée au sujet de la cryptographie est l'opposition apparente entre le besoin de confidentialité et les problèmes de sécurité publique et nationale. En

effet, si la cryptographie rend de très nombreux services aux honnêtes gens, elle peut aussi permettre aux criminels de tout bord et aux Etats parias de dissimuler leurs méfaits. Ce problème est souvent évoqué lorsqu'il s'agit de restreindre, d'une manière ou d'une autre, l'usage de la cryptographie. De nombreux Etats, dont la Suisse, s'appuient sur ce constat pour contrôler les exportations de biens de chiffrement.

Il ne faut cependant pas perdre de vue que l'immense majorité des utilisations de biens cryptographiques sont destinées à des fins honnêtes, justifiées et légales. Il serait donc à nos yeux inopportun de prétendre que la cryptographie dite forte représente un danger conséquent pour la sécurité nationale. La cryptographie permet surtout de protéger les réseaux informatiques contrôlant les infrastructures capitales d'un pays, comme les hôpitaux, les aéroports ou les systèmes de défense et les données confidentielles de nos entreprises. Le rôle d'une telle science consiste donc en premier lieu, à nos yeux, à prévenir les crimes et non pas à les dissimuler ou à les encourager. C'est d'ailleurs pour cette raison que la Suisse ne connaît aucune restriction d'emploi ou d'importation pour les biens de chiffrement.

L'environnement international

En matière de chiffrement, comme dans de nombreux autres secteurs, les disparités entre les politiques des Etats peuvent créer des obstacles à l'évolution des réseaux nationaux et mondiaux d'information et de communication, et freiner ainsi le développement du commerce électronique international.

Les gouvernements ont pris conscience, dans une large mesure, de la nécessité d'une approche coordonnée au niveau international pour faciliter le bon développement d'une infrastructure de l'information sûre et efficace. Malheureusement, des conflits majeurs d'intérêts ne cessent d'éclater, souvent au sein même des Etats, au sujet de la politique à suivre en matière de cryptographie. Le litige se situe le plus souvent entre les départements responsables du développement économique et ceux en charge de la sécurité nationale.

Les lignes directrices de l'OCDE

L'Organisation de coopération et de développement économiques (OCDE), dont la Suisse fait partie, a adopté le 27 mars 1997, après une année de négociations, des lignes directrices à propos de la politique de cryptographie. Cet accord non contraignant, qui se veut libéral, tente de recenser les principaux aspects que les pays devraient prendre en considération pour définir leurs politiques en matière de cryptographie aux niveaux national et international. Ces lignes directrices visent à promouvoir l'utilisation de la cryptographie, à développer le commerce électronique à travers une diversité d'applications commerciales, à susciter la confiance de l'utilisateur dans les réseaux numériques et à garantir la sécurité des données et la protection de la vie privée.

Ce texte encourage les secteurs public et privé à recourir à la cryptographie pour ses avantages indéniables en matière de protection des données et d'applications commerciales. Il invite également les acteurs concernés à élaborer des politiques de chiffrement qui tiennent compte des divers intérêts en jeu.

Ce document souligne que les efforts entrepris dans le domaine de la cryptographie doivent s'appuyer sur des consultations et une coopération entre pays. Ces échanges sont indispensables, en raison même du caractère international des réseaux d'information et de communication, mais aussi en raison des difficultés que posent, sur le plan international, la définition et la mise en œuvre des compétences dans le nouvel environnement mondial, par exemple dans le domaine des autorités nationales de certification des identités numériques.

L'Arrangement de Wassenaar

L'Arrangement de Wassenaar, juridiquement non contraignant, a été établi fin 1996 afin de contribuer à la sécurité et à la stabilité régionales et internationales, en favorisant la transparence et une responsabilité accrue en matière de transferts d'armes conventionnelles et de biens et technologies à double usage (civil et militaire), prévenant ainsi les accumulations déstabilisantes. Ce régime de contrôle à l'exportation comprend actuellement 33 Etats membres, dont la Suisse.

Les biens de chiffrement peuvent être qualifiés de biens à double usage et figurent donc dans les listes de contrôle de ce régime. Pour tenir compte de l'évolution technologique, des négociations ont lieu régulièrement dans le cadre de cet arrangement, dans le but d'adapter les paramètres de contrôle des biens contrôlés.

En 1998, l'accent a été mis sur la refonte complète de la catégorie consacrée aux biens de chiffrement. Le résultat obtenu, au terme d'une année d'intenses négociations, est un succès pour la Suisse. Nous sommes en effet parvenus, d'une part, à améliorer de manière significative la structure et le texte de contrôle de la catégorie en question, et d'autre part, à empêcher la concrétisation d'une série de propositions visant à étendre les contrôles à l'exportation des biens de chiffrement au-delà de toutes proportions.

Les contrôles à l'exportation des biens de chiffrement relevant de l'Arrangement de Wassenaar sont pratiqués en Suisse en vertu de la loi sur le contrôle des biens. L'adaptation de la liste de contrôle aux résultats de la toute récente série de négociations interviendra au second semestre 1999, par une modification de l'ordonnance

sur le contrôle des biens (*www.admin.ch/bawi*). L'exportation de technologies de chiffrement faible disposant de clefs symétriques jusqu'à 56 bits (ou/et de clefs asymétriques jusqu'à 512 bits) sera maintenant totalement libre. Au demeurant, l'exportation de technologies de cryptage vers les principaux partenaires commerciaux de la Suisse (les principaux Etats membres de l'OCDE, dont l'UE, les Etats-Unis et le Japon) continuera de passer par des procédures simplifiées (licences générales d'exportation). Certains logiciels de chiffrement seront dorénavant soumis à des contrôles, mais leur exportation bénéficiera elle aussi de procédures simplifiées. Quant à l'exportation de logiciels de chiffrement accessibles à chacun sans frais et dont l'utilisation ne nécessite pas le soutien substantiel du fabricant, elle reste totalement libre.

La cryptographie moderne: un défi à relever pour la Suisse

Le rôle déterminant que joue la cryptographie dans le domaine du commerce électronique et de la communication sur Internet n'a été pleinement reconnu que récemment, ce qui a eu pour conséquence de créer un décalage frappant entre la rapidité du développement de l'informatique et l'emploi de la cryptographie sur les nouvelles infrastructures numériques. La Suisse a été touchée de plein fouet par cette évolution, qui s'étend à l'ensemble de son économie et à ses réseaux de télécommunications.

L'industrie suisse est en mesure de relever ce défi, car elle possède les atouts indispensables pour développer des systèmes performants, concurrentiels et de haute qualité. Notre pays a longtemps été l'un des principaux producteurs mondiaux de biens de chiffrement destinés aux clients dits traditionnels (gouvernements et militaires). Il s'agit maintenant d'adapter notre savoir-faire dans ce domaine à la génération Internet.

Une série de facteurs positifs devraient être à même de propulser notre pays à nouveau sur le devant de la scène du chiffrement. La Suisse est un pays neutre, connu pour le haut niveau de ses centres de recherche et de ses universités, pour sa précision, sa compétence et sa fiabilité. La politique suisse en matière de cryptographie est libérale, l'emploi et l'importation de biens de chiffrement sont libres et les contrôles nécessaires à l'exportation sont effectués de la manière la plus efficace possible.

Le marché du chiffrement, actuellement en pleine expansion, est doté d'un potentiel important. Il y a là une chance à saisir pour un pays comme le nôtre. ■

Internet 2

- Un excellent site pour tous ceux que la cryptographie intéresse: *www.jya.com/crypto.htm*
- Le site de l'Office fédéral des affaires économiques extérieures: *www.admin.ch/bawi*
- Le site de Swisskey: *www.swisskey.com*
- Le site de l'Arrangement de Wassenaar: *www.wassenaar.org*
- Le site de l'OCDE: *www.oecd.org*
- Le site pour fortifier votre browser Netscape: *www.fortify.net*

Lectures recommandées 3

- Martin Raepple; *Sicherheitskonzepte für das Internet*; édition dpunkt; 1998.
- Klaus Schmeh; *Safer Net, Kryptographie im Internet und Intranet;* édition dpunkt; 1998.
- Albrecht Beutelspacher; *Kryptologie*; Vieweg; 5e édition; 1996.
- Albrecht Beutelspacher, Jörg Schwenk, Klaus-Dieter Wolfenstetter; *Moderne Verfahren der Kryptographie*; Vieweg; 2e édition; 1998.
- Bruce Schneier; *Applied Cryptography;* John Wiley & Sons, Inc.; 2e édition; 1996.
- David Kahn; *The Codebreakers, The Story of Secret Writing*; Scribner; 1967, 1996.

Thomas Hafen

Chef de la Section politique des contrôles à l'exportation et des sanctions, Office fédéral des affaires économiques extérieures, Berne
thomas.hafen@bawi.admin.ch

Steffen Erik Milner

Collaborateur scientifique, Section politique des contrôles à l'exportation et des sanctions, Office fédéral des affaires économiques extérieures, Berne
steffen.milner@bawi.admin.ch