5. LES JEUX DE CARTES COMME ARMES DE GUERRE ET LES NOMBRES PREMIERS ILLÉGAUX

Le matériel de cryptographie est assimilé dans certains pays à une arme de guerre et, à ce titre, sévèrement contrôlé. Les systèmes trop puissants, car utilisant des clefs longues, empêchant les approches exhaustives, sont par exemple interdits à l'exportation par les lois fédérales des États-Unis. Pour prendre en compte l'existence du système cryptographique de Schneier qui n'utilise comme matériel qu'un jeu de 54 cartes et dont les clefs dépassent les longueurs autorisées, les douaniers américains confisqueront-ils tous les jeux de 54 cartes que les voyageurs emportent dans leurs bagages?

Ce n'est pas le seul cas où la cryptographie met les lois en difficulté, conduisant à des situations plus ou moins ridicules. Récemment, l'algorithme de cryptage des DVD (le DVD *Movie encryption scheme* : DeCSS) a été reconstitué par des spécialistes qui ont analysé des puces et des logiciels chargés du décryptage (cet exemple montre que vouloir cacher un algorithme est une mauvaise idée).

En janvier 2000, le juge Lewis Kaplan, de New York, a décidé d'interdire la diffusion du programme de décryptage des DVD qui avait été publié sur internet. Cette interdiction est apparue en contradiction avec le principe exprimé par le premier amendement de la constitution américaine qui garantit la liberté d'expression. Le juge a donc été amené à préciser dans un jugement complémentaire que les codes sources (les programmes d'ordinateurs que l'ordinateur comprend et fait fonctionner) ne rentraient pas dans le champ du premier amendement et pouvaient être interdits.

La difficulté est qu'entre le langage parlé courant (qui ne peut être soumis à restriction) et le langage symbolique codé d'un programme toutes sortes d'intermédiaires sont possibles. On peut, par exemple, prendre le texte interdit du programme de décryptage des DVD et en faire une description lettre par lettre du type : "la première lettre du texte est un A, puis vient un =, etc." Ce texte, qui n'est pas un programme source, ne peut pas être interdit, alors que pourtant, il permet de reconstituer le programme source interdit.

Pour montrer l'absurdité des arrêts pris par le juge Kaplan une série de textes et d'images décrivant de manière indirecte le programme interdit ont été réalisés et placés sur internet. Plusieurs dizaines de ces documents sont disponibles librement à l'adresse internet suivante : www.cs.cmu.edu/~dst/DeCSS/Gallery/

En particulier, on y propose un nombre premier qui, quand on le traduit en base de numération 16, correspond à une version comprimée du programme interdit par le juge Kaplan. Connaître ce nombre premier c'est donc à peu de chose près connaître le programme interdit.

Si le juge Kaplan réussit à faire prévaloir son point de vue le nombre premier est donc illégal et interdit de publication. La rédaction de *Pour la Science,* choquée qu'un nombre premier puisse être interdit de publication, a décidé de passer outre en offrant à ses lecteurs ce magnifique nombre premier que l'on pourra consulter sur le site de *Pour la Science* : www.pourlascience.com

Pour plus de détails voir :
www.utm.edu/research/primes//curios/48565...29443.html

Une fois passées toutes les lettres de la phrase convenue, le paquet de 54 cartes sera dans un ordre qui sera celui qu'on utilisera pour produire (par l'utilisation répétée des opérations 1, 2, 3, 4, et 5) un flux de clefs.

Avec un tel procédé, après s'être rencontré une seule fois pour convenir de la façon de choisir la phrase clef du jour Alice et Bernard peuvent échanger indéfiniment des messages qui seront inviolables, même pour les plus puissants systèmes informatiques d'aujourd'hui et des décennies à venir.

ATTAQUES?

L'idée de Schneier suscite un certain intérêt et depuis que l'algorithme a été publié (il y a quelques mois) des attaques contre ce système ont été lancées. Bien que bâti par un des meilleurs cryptologue mondial, à partir de principes dont les spécialistes sont convaincus de l'efficacité, seule la résistance à des attaques nombreuses et répétées attestera de l'inviolabilité de *Solitaire* de Schneier.

Un premier travail a consisté à écrire un programme qui peut essayer 10^6 clefs par seconde et conduit à établir des statistiques. C'est ainsi que Paul Crowley a découvert que dans les suites pseudo-aléatoires engendrées par *Solitaire* un léger biais statistique était décelable : la probabilité que deux lettres consécutives dans un flux de clefs soient identiques au lieu d'être égale à 1/26 est de 1/22,5. Ce léger biais ne remet pas en cause la robustesse de *Solitaire*, mais si d'autres propriétés plus fines du flux de clefs sont découvertes il se pourrait que Schneier doive modifier son système.

D'autres chercheurs ont dès à présent proposé d'autres méthodes analogues ne demandant qu'un jeu de cartes pour le calcul et c'est peut-être bien tout un domaine nouveau de recherche qui vient de naître : la crypto-carto-ludico-graphie.

Paul CROWLEY, *Problems with Bruce Schneier's «Solitaire»* (Une attaque du Solitaire de Schneier) : www.cluefactory.org.uk/paul/solitaire/

David KAHN, *The Codebreakers*, 2e éditions, Scribner, New York, 1996. Traduction de la première édition : *La Guerre des codes secrets,* Interéditions, 1980.

Simon SINGH, *Histoire des codes secrets,* J.-C. Lattès, Paris, 1999.

Bruce SCHNEIER, *The Solitaire Encryption Algorithm*,1999. www.counterpane.com/solitaire.html

Bruce SCHNEIER, *Secret and Lies*, John Wiley and Sons, Inc., New York, 2000.

J. SAVARD, *Fun With Playing Cards* (un autre système de cryptographie à base de jeu de cartes) http://home.ecn.ab.ca/~jsavard/crypto/pp0105.htm

Neal STEPHENSON, *Cryptonomicon I. Le code enigma*, Payot-SF, 2000. Site internet consacré au roman de N. Stephenson. www.cryptonomicon.com