dérables (réseaux d'ordinateurs puissants) on ne peut pas aujourd'hui explorer plus de 10^{19} clefs. Dans 50 ans si la puissance des ordinateurs double tous les ans (hypothèse optimiste, voir l'article de cette rubrique du mois précédent) en utilisant des moyens de calcul puissants on pourra explorer au plus 10^{34} clefs. Dans un siècle toujours sous les mêmes hypothèses optimistes on pourra explorer 10^{49}, ce qui nous laissera encore loin du compte !

Partage de clefs

Nous avons vu que pour partager la clef de base l'agent Alice et l'agent Bernard ordonnent deux jeux de cartes de la même façon, chacun emportant un exemplaire du jeu avec lui.

Si des messages doivent être échangés plusieurs fois, il faut disposer d'un jeu de cartes par message, ce qui pourrait attirer l'attention ou en tout cas sembler louche aux douaniers fouillant les valises d'Alice ou de Bernard.

Une méthode pour éviter cette difficulté consiste à convenir d'un journal publiant une rubrique de problèmes de Bridge. En fonction du problème proposé dans la rubrique les agents conviennent d'un ordre du paquet initial. Alice et Bernard, décident par exemple que le message envoyé le 3 juin utilisera comme clef de base le paquet de cartes ordonné en prenant la dernière rubrique publiée à cette date dans le *Figaro*, et en considérant la description des cartes distribuées dans l'ordre Nord, Ouest, Sud, Est, les jokers étant placés dans le jeu juste derrière les deux cartes dont le nom est mentionné en premier dans le commentaire du problème.

Une troisième méthode de partage de clef est particulièrement intéressante car elle pourra être utilisée encore plus facilement. Alice et Bernard conviennent d'une phrase clef (par exemple la première phrase du premier article de la page 3, de *Libération*). Ensuite, à partir de cette phrase, ils vont chacun de leur côté créer un paquet de cartes désordonné en procédant de la manière suivante :

– prendre le paquet de 54 cartes ordonné selon l'ordre du Bridge, suivi des deux jokers ;

– effectuer les opérations de mélange 1, 2, 3 et 4 ;

– prendre la première lettre de la phrase clef, par exemple *D* (dont le numéro est $n = 4$), et effectuer une coupe en faisant passer les n premières cartes du paquet derrière les autres à l'exception de la dernière qui le reste ;

- effectuer les opérations de mélange 1, 2, 3, et 4 ;

- prendre la deuxième lettre de la phrase clef, etc.

4. UN SYSTÈME INFAILLIBLE?

Reprenant une proposition de Ueli Maurer et fondée sur l'idée que les supports mémoires des ordinateurs ne peuvent pas stocker des quantités de données très importantes, un système cryptographique, parfait en théorie, a été décrit par Michael Rabin et Yan Zong Ding il y a quelques semaines.

Ces deux chercheurs de l'Université de Harvard ont imaginé un système utilisant un satellite qui émettrait en continu des données aléatoires (sous forme de chiffres binaires ou de lettres) en telle quantité que leur enregistrement ne serait pas envisageable. Lorsque Alice voudrait envoyer un message crypté à Bernard, elle lui communiquerait par message crypté (selon un procédé traditionnel, dont le décryptage, s'il est possible, prend nécessairement du temps) un numéro de milliseconde qui fixerait l'endroit, dans le flux continu émis par le satellite, où il faut commencer à lire la clef aléatoire. Bernard, prenant connaissance immédiatement de ce point de repère, lirait lui aussi la clef aléatoire émise par le satellite et déchiffrerait donc le message codé en soustrayant la clef que le satellite émettrait, du message qu'Alice lui communiquerait (le cryptage et de décryptage pourraient se faire de manière quasi simultanée).

Pour un adversaire, le décodage serait définitivement impossible, car même s'il réussissait à décrypter le message de synchronisation (codé par une méthode traditionnelle), cela prendrait un certain temps pendant lequel, ne pouvant enregistrer le flux de données aléatoires émis en quantité trop volumineuse, il laisserait passer définitivement la possibilité de connaître la clef utilisée.

Plus intéressant encore, une fois la communication effectuée entre Alice et Bernard, ceux-ci n'auraient aucune raison de garder la clef dans la mémoire de leur ordinateur et donc ils l'effaceraient, rendant impossible tout décryptage ultérieur (même par eux, même sous la menace d'un tiers ou les injonctions d'un juge ou de la police).

Avec un tel système dont la sécurité serait mathématiquement garantie (car en définitive basée sur le principe du masque jetable), la cryptographie aurait atteint une sécurité absolue... ce qui ne plairait pas à tout le monde.

5. EXTRAIT DU ROMAN DE NEAL STEPHENSON

Dans le roman de Neal Stephenson, le Solitaire est appelé Pontifex. La traduction du livre de Neal Stephenson chez Payot-SF en est cours. Merci à Jean Bonnefoy de nous avoir autorisé à utiliser cet extrait de sa traduction avant même sa sortie en librairie.

La carte du dessus est un huit de pique. En l'écartant, ainsi que plusieurs autres, il tombe sur un joker avec des étoiles noires uni aux quatre coins; d'après les indices déjà livrés par Enoch, il s'agit du joker A. En un rien de temps, il le glisse sous celle du dessous, qui se trouve être le valet de trèfle. Aux deux-tiers environ de la pile, il trouve un joker décoré d'étoiles noires à fond blanc. B comme blanc, donc il sait qu'il s'agit du joker B ; il le déplace de deux cartes, pour l'insérer entre le six de trèfle et le neuf de carreau. Il regroupe le jeu et le déploie à nouveau, y introduit les doigts pour récupérer les valets et se retrouve avec une bonne moitié de la pile -- toutes les cartes situées entre les jokers, plus ces derniers -- coincée entre index et majeur. Il écarte alors les deux autres piles, celle du dessus et celle du dessous, pour les intervertir. Enoch observe ce manège et semble approuver.

Randy extrait à présent la carte du dessous de la pile, qui s'avère être le valet de trèfle. Se ravisant, il la sort et la pose provisoirement sur son genou, pour ne pas s'emmêler dans la phase suivante. D'après les symboles mnémotechniques qu'il a marqués sur ses ongles, la valeur numérique de ce valet est tout simplement de 11. Donc, en partant du dessus, il compte les cartes jusqu'à la onzième de la pile, coupe en dessous, puis intervertit les deux moitiés, et finalement reprend le valet de trèfle posé sur son genou pour le remettre sous la pile.

La carte du dessus est à présent un joker. « Quelle est la valeur numérique d'un joker?» demande-t-il et Enoch Root de répondre : « Cinquante-trois, pour chacun des deux.» Donc, ce coup-ci est nul : Randy sait que s'il compte les cartes depuis le début, quand il arrivera à 53, il contemplera la dernière de la pile. Et il se trouve que cette carte est le valet de trèfle, valeur 11. Onze est donc le premier nombre de la clé....

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