J.-M. Thinet

L'AGENT SECRET JOUE AUX CARTES

JEAN-PAUL DELAHAYE

Même les plus puissants des ordinateurs ne peuvent rien contre votre jeu de 54 cartes.

Une bombe atomique explose ! Elle est calculée pour ne pas faire de gros dégâts au sol, mais pour produire un éclair électromagnétique, c'est-à-dire un champ magnétique très puissant et très bref. Ce champ magnétique induit des courants électriques très forts dans tous les circuits, grille tous les transistors et met hors service tous les systèmes électroniques ! Que faire contre ce péril ? Comment pourrions-nous vivre dans un monde dont tous les ordinateurs sont brusquement devenus inopérants ? Comment pouvons-nous protéger nos données ?

Dans le cadre de la préparation à un tel événement et aussi pour le défi intellectuel qu'il constitue, le spécialiste de cryptographie Bruce Schneier a conçu un système de codage n'utilisant comme moyen de calcul qu'un simple jeu de 54 cartes. Le niveau de sécurité du système cryptographique de Schneier, qu'il dénomme *Solitaire,* est équivalent à celui des meilleurs algorithmes utilisés aujourd'hui (qui, eux bien sûr, exigent l'utilisation d'ordinateurs). Bien utilisé, il permet de crypter des messages que même les plus puissantes agences spécialisées d'espionnage et d'information ne pourront pas déchiffrer.

La méthode cryptographique de Schneier vous sera utile aussi, si dans votre métier d'agent secret vous souhaitez ne prendre aucun risque de vous faire repérer et que, pour cela, vous désirez ne porter sur vous aucun objet suspect. Elle pourra être utilisée par les hackers qui après s'être faits prendre (comme le fameux Kevin Mitnick) ont été condamnés à ne plus toucher un ordinateur.

La cryptographie moderne par sa compréhension approfondie des méthodes mathématiques pour cacher de l'information a fait progresser même les méthodes manuelles des bons vieux agents secrets des siècles passés. Ils ne pouvaient utiliser les ordinateurs absents et leurs procédés de chiffrement furent craqués par les services ennemis. Avec le *Solitaire* de Schneier ce ne sera plus possible !

Notons que *Solitaire* a été conçu par Schneier parce que dans le roman de Neal Stephenson intitulé *Cryptonomicon* (dont la traduction française par Jean Bonnefoy est en cours) certains personnages utilisent l'idée de la cryptographie avec un jeu de 54 cartes.

LE MASQUE JETABLE

La base de *Solitaire* est la méthode générale de codage par addition d'un message avec une clef (le message et la clef sont deux listes de lettres). Cette méthode est le fondement de nombreux systèmes cryptographiques. Pour coder le message «L'attaque est pour demain», qui comporte 21 lettres, on utilise une clef de 21 lettres, par exemple FUSREBJFYDZMPHYDALDIU, et on procède de la façon indiquée sur la figure 1.

Cette méthode de codage, lorsqu'on l'utilise avec une clef aléatoire qu'on ne réutilisera plus est une méthode absolument sûre qu'on dénomme méthode du masque jetable. C'est la seule méthode de cryptographie mathématique prouvée sûre d'une manière absolue. Le moindre écart dans son utilisation (clef non choisie aléatoirement car tirée d'un texte réel ; clef utilisée plusieurs fois) met la sécurité en péril car les cryptanalistes peuvent exploiter les particularités des clefs lorsqu'elles en possèdent et les usages multiples d'une même clef *(voir la figure 2).*

Le masque jetable, parfait en théorie, possède un grave défaut pratique : il faut que la clef soit aussi longue que le message à crypter. Aussi, n'est-elle que rarement utilisée. Cependant le principe du masque jetable est tellement simple et sa pratique si commode, qu'on l'utilise en remplaçant la clef aléatoire par une clef pseudo-aléatoire. Finalement, concevoir un bon système cryptographique peut se ramener à concevoir un bon procédé de création de suites pseudo-aléatoires. Certaines méthodes utilisées aujourd'hui comme l'algorithme RC4 fonctionne selon cette idée : un générateur pseudo-aléatoire fournit une clef aussi longue qu'on veut, qu'on utilise pour crypter des messages aussi longs qu'on le désire par le procédé de l'addition du message avec une clef pseudo-aléatoire.

La clef pseudo-aléatoire sera appelée *flux de clefs* car elle est produite en continu et peut être aussi longue qu'on le veut. Il ne faut pas la confondre avec les *clefs de base* qui permettront d'engendrer des flux de clefs différents. Les clefs de base servent à configurer le générateur de flux de clefs.

Une façon de procéder, déconseillée car trop simple, est de convenir que la clef de base est un mot (par exemple DTPDGCVA) et de décider que le flux de clefs sera obtenu en répétant indéfiniment la même clef de base : DTPDGCVA DTPDGCVA DTPDGCVA ... Cette méthode de codage où une clef courte est utilisée répétitivement a été inventée au XVI^{e} siècle par Vigenère, et un procédé pour craquer ce code de Vigenère a été mis au point par Charles Babbage au XIX^{e} siècle (il ne publia jamais sa découverte). Ce craquage montre qu'il faut utiliser des suites pseudo-aléatoires plus subtiles que la simple répétition d'un mot.

Les systèmes à flux de clefs appartiennent à la classe des méthodes cryptographiques symétriques : avec une clef de base secrète (qui sert à créer le flux de clefs) l'émetteur code le message original en message crypté et c'est la même clef de base secrète qui en engendrant le même flux de clefs, permet au récepteur du message de décoder le texte secret pour reconstituer le texte original. Dans les méthodes asymétriques (comme le RSA, voir *Pour la Science*, janvier 2000, *La cryptographie RSA vingt ans après*, pages 104-108) une clef, dite publique, sert au codage et une autre, dite privée, sert au décodage.

Avec les méthodes symétriques si l'agent Alice veut communiquer avec

l'agent Bernard il faut que les agents Alice et Bernard conviennent d'une clef de base secrète que personne d'autre qu'eux ne connaîtra. Nous reviendrons plus loin sur ce problème du partage de la clef et suggérerons des méthodes pour y parvenir dans le cas de *Solitaire*.

ALGORITHME CONNU, CLEF SECRÈTE

En cryptographie moderne la sécurité d'une méthode ne doit pas reposer sur le secret de l'algorithme utilisé, mais uniquement sur le secret de la clef (la clef unique dans le cas de la cryptographie symétrique, la clef privée dans le cas de la cryptographie à double clef). Si vous utilisez une méthode secrète de cryptage votre système risque d'être percé par un ennemi qui analyse, par exemple, les programmes ou les puces destinées à opérer le cryptage. Certains groupements industriels ont oublié le principe selon lequel cacher un algorithme est dangereux et c'est ainsi que le cryptage des DVD a été craqué : l'algorithme secret a été reconstitué (on dit «désassemblé») par des spécialistes et aujourd'hui de nombreux sites internet expliquent comment s'y prendre pour décrypter les DVD *(voir la figure 6)*. Un décodage du même type s'est répété pour les téléphones portables.

Tous les spécialistes s'accordent aujourd'hui sur l'idée que la bonne façon de procéder en cryptographie est de rendre public les algorithmes de cryptographie qu'on utilise, mais de les concevoir de telle façon que, sans la connaissance de la clef, le décryptage est impossible. Un avantage supplémentaire de la diffusion des algorithmes cryptographiques est que cela permet aux spécialistes de s'y confronter : si votre algorithme n'est pas bon vous le saurez rapidement car il sera craqué ; en revanche, s'il résiste cela prouvera qu'il est excellent – ou au moins qu'il n'est pas trop mauvais. Des dizaines d'algorithmes sont ainsi éliminés chaque année.

LA CRÉATION DU FLUX DE CLEFS

Revenons à notre jeu de cartes. Pour définir complètement un codage il suffit de définir une façon de produire des lettres pseudo-aléatoires avec un jeu de cartes. Ce flux de lettres sera utilisé comme flux de clefs qu'on additionnera aux messages qu'on souhaitera coder.

Voici ce que propose B. Schneier. Vous prenez votre jeu de cartes dans un ordre fixé qui constituera la clef de base. Votre correspondant devra, pour décoder, connaître l'ordre de départ que vous avez utilisé. Vous allez successivement faire les quatre opérations décrites figure 3.

1. CODAGE D'UN MESSAGE PAR SOMME AVEC UNE CLEF

1) Le codage du message. Le message "L'attaque est pour demain" est transformé, lettre par lettre, en nombres de 1 à 26 en fonction de l'ordre alphabétique (A=1, B=2, etc, jusqu'à Z=26) ce qui donne ici :

L	A	T	T	A	Q	U	E	E	S	T	P	O	U	R	D	E	M	A	I	N
12	1	20	20	1	17	21	5	5	19	20	16	15	21	18	4	5	13	1	9	14

- La suite des lettres de la clef FUSREBJFYDZMPHYDALDIU est transformée de la même façon :

F	U	S	R	E	B	J	F	Y	D	Z	M	P	H	Y	D	A	L	D	I	U
6	21	19	18	5	2	10	6	25	4	26	13	16	8	25	4	1	12	4	9	21

- On additionne terme à terme les deux listes de nombres :

18	22	39	38	6	19	31	11	30	23	46	29	31	29	43	8	6	25	5	18	35

- On soustrait 26 à chacun des nombres plus grands que 26 :

18	22	13	12	6	19	5	11	4	23	20	3	5	3	17	8	6	25	5	18	9

- On transforme cette suite de nombres entre 1 et 26 en suite de lettres, toujours en utilisant l'ordre alphabétique, ce qui produit le message crypté :

R	V	M	L	F	S	E	K	D	W	T	C	E	C	Q	H	F	Y	E	R	I

Cette addition du message et de la clef est notée symboliquement de la façon suivante :
LATTAQUEESTPOURDEMAIN + FUSREBJFYDZMPHYDALDIU = RVMLFSEKDWTCECQHFYERI

2) Le décodage se fait par un procédé analogue.

- On traduit le message crypté en une suite de nombres.

R	V	M	L	F	S	E	K	D	W	T	C	E	C	Q	H	F	Y	E	R	I
18	22	13	12	6	19	5	11	4	23	20	3	5	3	17	8	6	25	5	18	9

- On soustrait à la liste de nombres du message crypté la liste des nombres de la clef.

	18	22	13	12	6	19	5	11	4	23	20	3	5	3	17	8	6	25	5	18	9
–	6	21	19	18	5	2	10	6	25	4	26	13	16	8	25	4	1	12	4	9	21
=	12	1	-6	-6	1	17	-5	5	-21	19	-6	-10	-11	-5	-8	4	5	13	1	9	-12

- Quand la soustraction donne un nombre inférieur à 1, on ajoute 26 pour se ramener entre 1 et 26.

12	1	20	20	1	17	21	5	5	19	20	16	15	21	18	4	5	13	1	9	14

-On retransforme ce message en une suite de lettres.

L	A	T	T	A	Q	U	E	E	S	T	P	O	U	R	D	E	M	A	I	N

2. POURQUOI NE FAUT-IL PAS UTILISER DEUX FOIS LA MÊME CLEF?

La première règle, lorsqu'on utilise le codage par somme d'un texte avec une clef est de ne surtout pas réutiliser la même clef pour crypter deux messages différents. Si vous le faites, vous réduisez à rien la sécurité du système. Voici pourquoi. Si le Message A et le Message B ont été cryptés par la même clef Clef, les messages cryptés sont :

MessageCrypté A = Message A + Clef.
MessageCrypté B = Message B + Clef.

En faisant la différence des messages cryptés, on obtient :

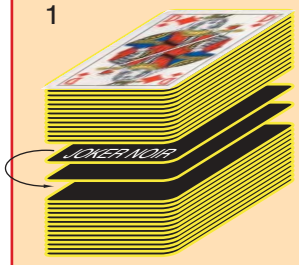
MessageCrypté A – MessageCrypté B =
(Message A + Clef) – (Message B + Clef) = Message A – Message B.

On a donc le même résultat que ce que donne la soustraction de deux textes en clair qui sont des messages en français (ou dans une autre langue, mais cela revient au même). La redondance des langues naturelles écrites (fréquences inégales d'utilisation des lettres, caractéristiques du type "un q est presque toujours suivi d'un u", etc) est un levier que les experts en cryptanalyse savent exploiter, ce qui leur permet de reconstituer Message A et Message B à partir de Message A – Message B (pourvu que les messages soient assez longs). Utiliser deux fois la même clef revient à ne pas crypter ses messages !

3. LES CINQ OPÉRATIONS POUR OBTENIR LE FLUX DE CLEFS À PARTIR D'UN JEU DE 54 CARTES DANS UN DÉSORDRE CONNU

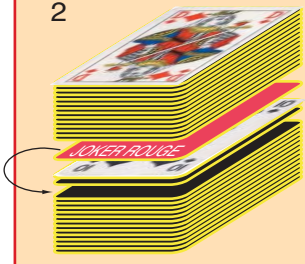
Vous tenez le paquet de cartes dans la main droite, faces vers vous. L'ordre initial du paquet est convenu avec votre correspondant. C'est cet ordre qui constitue la clef de base (voir en figure 4 une méthode pour convenir de cet ordre initial à partir d'une phrase secrète)

1



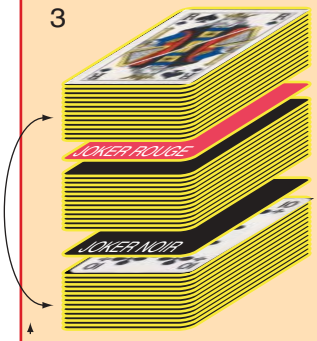
(1) Recul du joker noir d'une position.
Vous faites reculer le joker noir d'une place, (vous le permutez avec la carte qui est juste derrière lui. Si le joker noir est en dernière position il passe derrière la carte du dessus, c'est-à-dire en deuxième position.

2



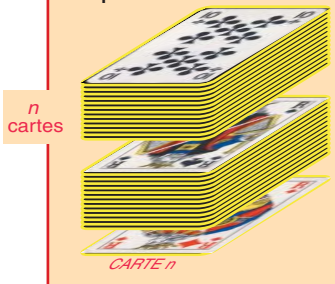
(2) Recul du joker rouge de deux positions.
Vous faites reculer le joker rouge de deux cartes. S'il était en dernière position, il passe en troisième position. S'il était en avant dernière position, il passe en deuxième.

3



(3) Double coupe par rapport aux jokers.
Vous repérez les deux jokers et vous intervertissez le paquet des cartes situées au-dessus du joker qui est en premier avec le paquet de cartes qui est au-dessous du joker qui est en second. Dans cette opération la couleur des jokers est sans importance. Comme pour toutes les opérations on peut faire cette manipulation sans avoir à poser les cartes sur une table.

4



(4) Coupe simple déterminée par la dernière carte.
Vous regardez la dernière carte et vous évaluez son numéro selon l'ordre du Bridge : trèfle-carreau-cœur-pique et dans chaque couleur as, 2, 3, 4, 5, 6, 7,8, 9,10, valet, dame et roi (l'as de trèfle a ainsi le numéro 1, le roi de pique le numéro 52). Les jokers ont, par convention, tous deux le numéro 53. Si le numéro de la dernière carte est *n* vous prenez les *n* premières cartes du dessus et les placez derrière les autres cartes à l'exception de la dernière carte qui reste dernière. Le maintien à sa place de cette carte résulte de considérations de cryptanalyse.

(5) Lecture d'une lettre pseudo-aléatoire
Vous regardez le numérode la première carte, soit n ce numéro, vous comptez n cartes à partir du début vous regardez la carte à laquelle vous êtes arrivé (la *n*+1-ième), soit *m* son numéro. Si c'est un joker vous refaites une opération complète de mélange et de lecture (1-2-3-4-5). Si *m* dépasse 26 vous soustrayez 26. Au nombre entre 1 et 26 ainsi obtenu est associée une lettre qui est la première du flux de clefs servant à coder votre message selon la méthode : message + flux de clefs = message codé. Vous la notez sur un papier (que vous n'oublierez pas de brûler ensuite). L'opération de lecture ne modifie pas l'ordre du paquet de cartes. Vous procédez de la même façon pour avoir la deuxième lettre du flux de clefs. Lorsque vous en avez un nombre suffisant vous pouvez coder votre message.

Quand la première lettre est obtenue, vous mélangez à nouveau en appliquant des opérations 1-2-3-4, et l'opération 5 de lecture vous donne une seconde lettre etc... De cette façon vous disposez d'un flux de clefs aussi long que vous le souhaitez ce qui vous permet de coder votre message selon la méthode de l'addition d'une clef au message :
Message+ Flux de Clefs=Message Crypté

Le décodage se fera en partant du même paquet de cartes initial (la clef de base partagée) qui permet à votre correspondant de reconstituer le flux de clefs que vous avez utilisé, et donc de décoder le message en utilisant l'équation :
Message Crypté – Flux de Clefs=Message

Pour un opérateur un peu entraîné la méthode de Schneier demande moins d'une minute de codage par lettre du message et autant pour le décodage. Une erreur de manipulation dans le déroulement des opérations compromet définitivement toute la partie du message qui est située au-delà de l'erreur. Il est donc conseillé d'opérer deux fois le codage de façon à s'assurer qu'aucune erreur n'est commise. L'algorithme peut bien sûr être programmé et exécuté par un ordinateur, cependant il a été conçu pour ne demander qu'un jeu de cartes sans même avoir à poser les cartes sur une table, uniquement en faisant attentivement des manipulations élémentaires que l'on mémorise sans peine.

La garantie fournie par la méthode de Schneier n'est pas absolue (comme presque toujours en cryptographie mathématique), mais elle est du niveau des meilleures méthodes utilisées aujourd'hui dans le monde bancaire ou du commerce électronique, ce qui veut dire que même un ennemi disposant d'ordinateurs très puissants ne pourra pas, à moins de la découverte jugée improbable d'une technique nouvelle de cryptanalyse, retrouver vos codes sans disposer de la clef de base (l'ordre initial du paquet de carte).

Le nombre de clefs de base possibles est 54! = 0,230 10^{72} soit précisément :
230 843 697 339 241 380 472 092 742 683 027 581 083 278 564 571 807 941 132 288 000 000 000 000

Aucun système informatique envisageable dans un avenir raisonnable ne pourra tester toutes les clefs une par une (méthode d'exploration exhaustive). En effet les calculs les plus longs envisageables aujourd'hui comporte de l'ordre de 10^{22} instructions (c'est déjà plus que les calculs effectués par le projet SETI mettant en jeu des milliers d'ordinateurs recherchant depuis des mois dans les signaux provenant du ciel des traces de vie extraterrestre). L'essai d'une clef de *Solitaire* demande certainement plus 10^3 instructions, donc même avec des moyens consi-

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