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 !