J.-M. Thiriet

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