M1 Crypto
Mini-projet

Le spécialiste en 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 de ce système cryptographique, dénommé Solitaire, est équivalent à celui des meilleurs algorithmes utilisés aujourd'hui. Bien utilisé, il permet de crypter des messages que même les agences d'espionnage et de renseignement les plus puissantes ne pourront pas déchiffrer. La méthode cryptographique de Schneier vous sera également utile si, dans le cadre de votre métier d'agent secret, vous souhaitez éviter tout risque de vous faire repérer et, pour ce faire, ne souhaitez transporter aucun objet suspect. Elle pourra aussi être utilisée par des hackers qui, après avoir été arrêtés (comme le fameux Kevin Mitnick), ont été condamnés à ne plus toucher un ordinateur. Même les ordinateurs les plus puissants ne peuvent rien contre votre jeu de 54 cartes.

La base de Solitaire repose sur la méthode générale de codage consistant à additionner un message avec une clé (le message et la clé étant deux listes de lettres). Cette méthode est le fondement de nombreux systèmes cryptographiques. Pour coder un message, on procède comme indiqué dans la section 1. Lorsque cette méthode est utilisée avec une clé aléatoire, qui ne sera jamais réutilisée, elle constitue une méthode absolument sûre, appelée « masque jetable ». C'est la seule méthode de cryptographie mathématique prouvée comme étant absolument sûre. Tout écart dans son utilisation (par exemple, une clé non choisie aléatoirement, mais tirée d'un texte réel, ou une clé utilisée plusieurs fois) compromet la sécurité, car les cryptanalystes peuvent exploiter les particularités des clés lorsqu'elles sont connues et les usages multiples d'une même clé (voir la section 2). Le masque jetable, bien que parfait en théorie, possède un grave défaut pratique : la clé doit être aussi longue que le message à crypter. C'est pourquoi elle est rarement utilisée. Cependant, le principe du masque jetable est tellement simple et sa mise en œuvre si pratique qu'on le remplace souvent par une clé pseudo-aléatoire. En fin de compte, concevoir un bon système cryptographique revient à concevoir une méthode efficace pour générer des suites pseudo-aléatoires. La clé pseudo-aléatoire est appelée flux de clés, car elle est produite de manière continue et peut être aussi longue qu'on le souhaite.

Voici ce que propose Bruce Schneier : vous prenez votre jeu de cartes dans un ordre fixe qui constituera la clé de base. Votre correspondant devra, pour déchiffrer le message, connaître l'ordre de départ que vous avez utilisé. Ensuite, vous allez successivement réaliser les cinq opérations décrites dans la section 3.

1 Le codage/décodage du message par somme avec une clef

1. Le message « L'attaque est pour demain » est transformé, lettre par lettre, en nombres de 1 à 26 en fonction de l'odre 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

2. La suite des lettres de la clef FUSREBJFYDZMPHYDALDIU est transformé 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

3. On addition terme à terme les deux listes de nombres et on soustrait 26 à chacun des nombres plus grand que 26 ; on transforme cette suite de nombres en une suite de lettres :

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

Le décodage est réalisé par l'opération inverse.

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 sécurite du système. Voici pourquoi. Si le message A et le message B ont été cryptés par la même clef C, les messages cryptés sont :

— $MessageCrypte\_A = A + C$

— $MessageCrypte\_B = B + C$

En faisant la différence des messages cryptés, on obtient :

$$MessageCrypte\_A - MessageCrypte\_B = A - B$$

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 $A - B$ (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 la paquet de cartes dans la main droite, face vers vous. L'ordre initial du paquet est convenu avec votre correspondent. C'est cet ordre qui constitue la clef de base.

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 (donc, en deuxième position).

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 Double coupe par rapport aux jokers. Vouz 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.

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 a le numéro 52). Les jokers on par convention le numéro 53. Si le numéro de la dernière carte est n vous prenez les n premières cartes du dessus du paquet et les placez derrière les autres cartes à l'exception de la dernière carte qui reste la dernière.

5 Lecture d'une lettre pseudo-aléatoire : Vous regardez la numéro de la première carte, soit n ce numéro. Vous comptez n cartes à partir du début et vous regardez la carte à laquelle vous êtes arrivé (la $n+1$-ième), soit m son numero. Si c'est un jokers vous refaites une opération complète de mélange et de lecture (les points 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 lettre suivante dans du flux de clefs.

L'opération de lecture ne modifie pas l'ordre du paquet de cartes.

Vous procédez de la même façon pour avoir les autres lettres du flux de clefs. Lorsque vous en avez un nombre suffisant vous pouvez coder votre message.

Réaliser un programme informatique (dans un langage à votre choix) qui implémente le systeme de cryptage présenté ci-dessus.