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 :

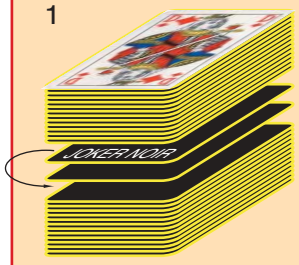
MessageCrypté A – MessageCrypté B =
(Message A + Clef) – (Message B + Clef) = Message A – Message B.

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

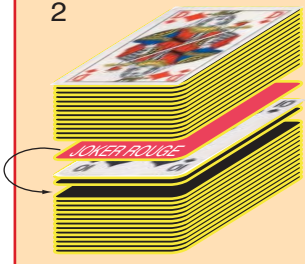
Vous tenez le paquet de cartes dans la main droite, faces vers vous. L'ordre initial du paquet est convenu avec votre correspondant. C'est cet ordre qui constitue la clef de base (voir en figure 4 une méthode pour convenir de cet ordre initial à partir d'une phrase secrète)

1



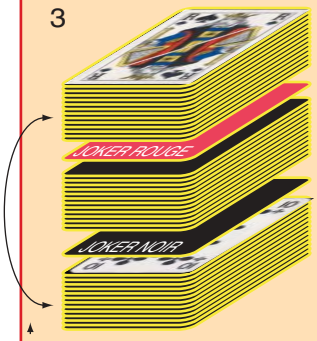
(1) Recul du joker noir d'une position.
Vous faites reculer le joker noir d'une place, (vous le permutez avec la carte qui est juste derrière lui. Si le joker noir est en dernière position il passe derrière la carte du dessus, c'est-à-dire en deuxième position.

2



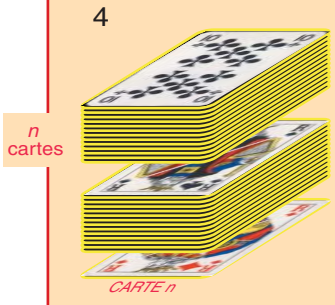
(2) Recul du joker rouge de deux positions.
Vous faites reculer le joker rouge de deux cartes. S'il était en dernière position, il passe en troisième position. S'il était en avant dernière position, il passe en deuxième.

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-