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 !