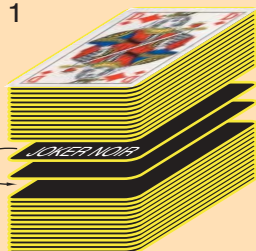


3. LES CINQ OPÉRATIONS POUR OBTENIR LE FLUX DE CLEFS À PARTIR D'UN JEU DE 54 CARTES DANS UN DÉSORDRE CONNU

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 permutiez 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.

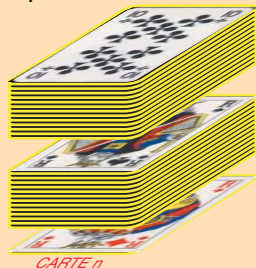
3



(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 numéro de 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 $54! = 0,230 \cdot 10^{72}$ 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-