

dérables (réseaux d'ordinateurs puissants) on ne peut pas aujourd'hui explorer plus de 10^{19} clefs. Dans 50 ans si la puissance des ordinateurs double tous les ans (hypothèse optimiste, voir l'article de cette rubrique du mois précédent) en utilisant des moyens de calcul puissants on pourra explorer au plus 10^{34} clefs. Dans un siècle toujours sous les mêmes hypothèses optimistes on pourra explorer 10^{49} , ce qui nous laissera encore loin du compte !

PARTAGE DE CLEFS

Nous avons vu que pour partager la clef de base l'agent Alice et l'agent Bernard ordonnent deux jeux de cartes de la même façon, chacun emportant un exemplaire du jeu avec lui.

Si des messages doivent être échangés plusieurs fois, il faut disposer d'un jeu de cartes par message, ce qui pourrait attirer l'attention ou en tout cas sembler louche aux douaniers fouillant les valises d'Alice ou de Bernard.

Une méthode pour éviter cette difficulté consiste à convenir d'un journal publiant une rubrique de problèmes de Bridge. En fonction du problème proposé dans la rubrique les agents conviennent d'un ordre du paquet initial. Alice et Bernard, décident par exemple que le message envoyé le 3 juin utilisera comme clef de base le paquet de cartes ordonné en prenant la dernière rubrique publiée à cette date dans le *Figaro*, et en considérant la description des cartes distribuées dans l'ordre Nord, Ouest, Sud, Est, les jokers étant placés dans le jeu juste derrière les deux cartes dont le nom est mentionné en premier dans le commentaire du problème.

Une troisième méthode de partage de clef est particulièrement intéressante car elle pourra être utilisée encore plus facilement. Alice et Bernard conviennent d'une phrase clef (par exemple la première phrase du premier article de la page 3, de *Libération*). Ensuite, à partir de cette phrase, ils vont chacun de leur côté créer un paquet de cartes désordonné en procédant de la manière suivante :

- prendre le paquet de 54 cartes ordonné selon l'ordre du Bridge, suivi des deux jokers ;
- effectuer les opérations de mélange 1, 2, 3 et 4 ;
- prendre la première lettre de la phrase clef, par exemple *D* (dont le numéro est $n = 4$), et effectuer une coupe en faisant passer les n premières cartes du paquet derrière les autres à l'exception de la dernière qui le reste ;
- effectuer les opérations de mélange 1, 2, 3, et 4 ;
- prendre la deuxième lettre de la phrase clef, etc.

4. UN SYSTÈME INFALLIBLE?

Reprenant une proposition de Ueli Maurer et fondée sur l'idée que les supports mémoires des ordinateurs ne peuvent pas stocker des quantités de données très importantes, un système cryptographique, parfait en théorie, a été décrit par Michael Rabin et Yan Zong Ding il y a quelques semaines.

Ces deux chercheurs de l'Université de Harvard ont imaginé un système utilisant un satellite qui émettrait en continu des données aléatoires (sous forme de chiffres binaires ou de lettres) en telle quantité que leur enregistrement ne serait pas envisageable. Lorsque Alice voudrait envoyer un message crypté à Bernard, elle lui communiquerait par message crypté (selon un procédé traditionnel, dont le décryptage, s'il est possible, prend nécessairement du temps) un numéro de milliseconde qui fixerait l'endroit, dans le flux continu émis par le satellite, où il faut commencer à lire la clef aléatoire. Bernard, prenant connaissance immédiatement de ce point de repère, lirait lui aussi la clef aléatoire émise par le satellite et déchiffrerait donc le message codé en soustrayant la clef que le satellite émettrait, du message qu'Alice lui communiquerait (le cryptage et de décryptage pourraient se faire de manière quasi simultanée).

Pour un adversaire, le décodage serait définitivement impossible, car même s'il réussissait à décrypter le message de synchronisation (codé par une méthode traditionnelle), cela prendrait un certain temps pendant lequel, ne pouvant enregistrer le flux de données aléatoires émis en quantité trop volumineuse, il laisserait passer définitivement la possibilité de connaître la clef utilisée.

Plus intéressant encore, une fois la communication effectuée entre Alice et Bernard, ceux-ci n'auraient aucune raison de garder la clef dans la mémoire de leur ordinateur et donc ils l'effaceraient, rendant impossible tout décryptage ultérieur (même par eux, même sous la menace d'un tiers ou les injonctions d'un juge ou de la police).

Avec un tel système sur la sécurité serait mathématiquement garantie (car en définitive basée sur le principe du masque jetable), la cryptographie aurait atteint une sécurité absolue... ce qui ne plairait pas à tout le monde.



5. EXTRAIT DU ROMAN DE NEAL STEPHENSON

Dans le roman de Neal Stephenson, le Solitaire est appelé Pontifex. La traduction du livre de Neal Stephenson chez Payot-SF en est cours. Merci à Jean Bonnefoy de nous avoir autorisé à utiliser cet extrait de sa traduction avant même sa sortie en librairie.

La carte du dessus est un huit de pique. En l'écartant, ainsi que plusieurs autres, il tombe sur un joker avec des étoiles noires uni aux quatre coins; d'après les indices déjà livrés par Enoch, il s'agit du joker A. En un rien de temps, il le glisse sous celle du dessous, qui se trouve être le valet de trèfle. Aux deux-tiers environ de la pile, il trouve un joker décoré d'étoiles noires à fond blanc. B comme blanc, donc il sait qu'il s'agit du joker B ; il le déplace de deux cartes, pour l'insérer entre le six de trèfle et le neuf de carreau. Il regroupe le jeu et le déploie à nouveau, y introduit les doigts pour récupérer les valets et se retrouve avec une bonne moitié de la pile -- toutes les cartes situées entre les jokers, plus ces derniers -- coincée entre index et majeur. Il écarte alors les deux autres piles, celle du dessus et celle du dessous, pour les intervertir. Enoch observe ce manège et semble approuver. Randy extrait à présent la carte du dessous de la pile, qui s'avère être le valet de trèfle. Se ravisant, il la sort et la pose provisoirement sur son genou, pour ne pas s'emmêler dans la phase suivante. D'après les symboles mnémotechniques qu'il a marqués sur ses ongles, la valeur numérique de ce valet est tout simplement de 11. Donc, en partant du dessus, il compte les cartes jusqu'à la onzième de la pile, coupe en dessous, puis intervertit les deux moitiés, et finalement reprend le valet de trèfle posé sur son genou pour le remettre sous la pile.

La carte du dessus est à présent un joker. « Quelle est la valeur numérique d'un joker? » demande-t-il et Enoch Root de répondre : « Cinquante-trois, pour chacun des deux. » Donc, ce coup-ci est nul : Randy sait que s'il compte les cartes depuis le début, quand il arrivera à 53, il contempera la dernière de la pile. Et il se trouve que cette carte est le valet de trèfle, valeur 11. Onze est donc le premier nombre de la clé....