de pixel, si le pixel de M est le même que celui de S, on dessine sur C un pixel blanc, sinon on dessine un pixel noir. Le message chiffré C résulte ainsi d'un XOR entre le masque M et le secret S, c'est-à-dire C = M XOR S.

Après avoir créé les images M et C, si vous imprimez M et C sur des transparents, vous constaterez que la superposition de M et de C fait apparaître S. Si vous disposez d'un ordinateur, vous verrez encore mieux l'image S en opérant un XOR entre M et C *(voir l'encadré 1)*.

Voici maintenant comment utiliser ce procédé pour faire circuler des informations secrètes et les envoyer à quelqu'un ne disposant pas d'ordinateur, cela d'une manière parfaitement sûre.

Alain souhaite envoyer des messages secrets à Béatrice. Ils se rencontrent une première fois et produisent une série d'images aléatoires, les masques M_1, M_2, ..., M_n, dont ils gardent chacun une copie et que bien sûr personne d'autre ne devra connaître. Ils peuvent aussi convenir de ces masques secrets en les faisant circuler sur le réseau : Alain les crée et les envoie à Béatrice, ou l'inverse. Cependant, si on utilise le réseau, il faut être certain au moment de l'échange des images M_1, M_2, ..., M_n que personne d'autre n'en prend connaissance. C'est possible en utilisant un canal de communication protégé, ou en utilisant un procédé cryptographique tel que le RSA qui permet sans risque ce type de partages à distance.

Alain n'est pas prêt à noircir à la main pixel par pixel l'image chiffrée C ! Aussi dispose-t-il des masques sous la forme de fichiers informatiques et il utilise un ordinateur pour produire les images chiffrées C. Béatrice, elle, n'aura besoin de rien d'autre que ses yeux pour le déchiffrage. L'opération de partage des masques réalisée, Alain et Béatrice vont échanger des secrets en parfaite sécurité par la poste ou en utilisant des émissaires, même si ceux-ci peuvent être douteux.

Un masque à usage unique

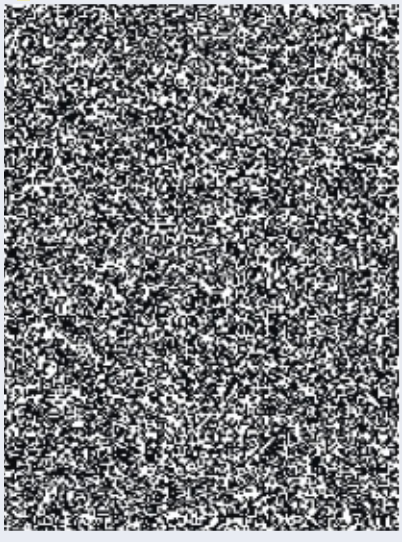
Lorsque Alain souhaite communiquer à Béatrice une image secrète S, il choisit l'un des masques M_i dont il dispose ; il utilise son ordinateur pour calculer l'image $C = M_i$ XOR S qu'il poste ou fait remettre sous la forme d'un transparent à Béatrice en lui indiquant le numéro *i* du masque utilisé. Ce numéro *i* peut être inscrit sans risque sur le transparent, car celui qui ne dispose pas des transparents M_1, M_2, ..., M_n ne peut rien faire de l'information *i*, pas plus qu'il ne peut tirer quoi que ce soit du transparent C. Alain peut aussi transmettre l'image chiffrée C en utilisant le réseau et demander à Béatrice d'imprimer le transparent C quand elle reçoit le fichier numérique.

Pour que Béatrice prenne connaissance de l'image secrète, elle superpose le transparent reçu C et le transparent du masque M_i dont elle dispose. Alain et Béatrice jetteront le masque M_i qu'il ne faudra plus jamais utiliser.

Pour que la méthode résiste aux attaques d'espions, il est essentiel que les images des masques M_1, M_2, ..., M_n soient aussi aléatoires que possible : il faut les produire avec de bons procédés de génération de suites aléatoires et ne surtout pas prendre pour masques des images représentant quelque chose. De plus, il ne faut jamais réutiliser un masque M_i : si vous le faites, plus aucune garantie de confidentialité ne pourra être assurée *(voir l'encadré 2)*.

En respectant cette double consigne de sécurité, le procédé est sûr, car ce système cryptographique est équivalent à la méthode du masque jetable (aussi dénommé *one-time pad* ou code de Vernam), dont

c IMAGE CHIFFRÉE : C = M XOR S



d IMAGE DÉVOILÉE : M OU C

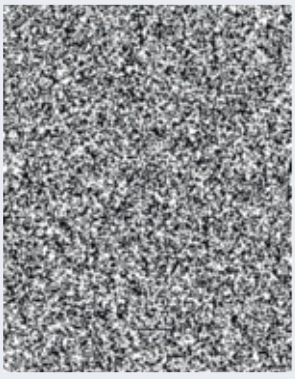
e IMAGE RECONSTITUÉE : M XOR C

© Pour la Science - n° 416 - Juin 2012

2. Jamais deux fois le même masque !

a IMAGE SECRÈTE : S'

b IMAGE CHIFFRÉE : C' = M XOR S'



c IMAGE DÉVOILÉE : C OU C'

d IMAGE RECONSTITUÉE : C XOR C'

Si on utilise la méthode du masque jetable *(voir l'encadré 1)* pour créer des transparents chiffrés, il ne faut surtout pas utiliser deux fois le même masque. En voici la preuve.

Ici, en utilisant le même format d'image que pour l'encadré 1, et le même masque de chiffrage M, on a créé une image où est caché le mot SECRET, en opérant un XOR avec le masque M ; S' = SECRET *(a)*, C' = M XOR S' *(b)*. Un espion qui s'emparerait des deux messages secrets (celui avec la tête de Napoléon, et celui contenant le mot SECRET) et superposerait les transparents C et C' verrait l'image C OU C' *(c)*. Si l'espion opérait (à l'aide d'un ordinateur) un XOR entre les deux images chiffrées *(d)* soit C XOR C', ce qu'il obtiendrait serait encore plus net : car C XOR C' = (M XOR S) XOR (M XOR S') = S XOR 0 XOR S'= S XOR S'.

Utiliser un masque aléatoire une seule fois est une méthode inviolable, mais utiliser le même masque deux fois est une énorme bêtise.

L'AUTEUR

Jean-Paul DELAHAYE
est professeur à l'Université de Lille et chercheur au Laboratoire d'informatique fondamentale de Lille (LIFL).

Claude Shannon a démontré l'absolue inviolabilité en 1949.

La superposition des deux transparents M_i et C fait bien apparaître l'image S, mais sous une forme dégradée (bruitée), car le OU opéré instantanément par l'œil laisse un bruit qui remplace le blanc de l'image secrète initiale. Si, au lieu d'utiliser l'œil, Béatrice dispose d'un ordinateur, un déchiffrage parfait est possible. En effet, nous savons que pour un message quelconque A, on a A XOR A = 0 et 0 XOR A = A (vous pouvez le vérifier avec les valeurs blanches et noires, blanc = 0, noir = 1) ; Béatrice opère un XOR entre M_i et C qui redonne S, car :
M_i XOR C = M_i XOR (M_i XOR S) =
(M_i XOR M_i) XOR S = 0 XOR S = S.

Insistons bien sur le fait qu'une fois le masque M_i et l'image chiffrée C créés, aucun des deux transparents à lui seul n'a la moindre information sur l'image secrète S. C'est évident pour M_i, puisqu'il a été créé sans même qu'on sache quelle serait l'image S qu'on chiffrerait. Voici maintenant le raisonnement qui montre que connaître C sans connaître M_i ne permet pas d'avoir la moindre information sur S.

Un espion qui dispose de l'image C et sait qu'elle a été engendrée par la méthode du masque jetable sans connaître le masque peut essayer tous les masques possibles qui, *a priori*, ont la même probabilité d'avoir été utilisés pour créer C à partir de S.

L'espion se dit qu'en essayant les masques systématiquement, quand il arrivera au bon M_i, il verra apparaître un dessin différent d'un nuage aléatoire, ce qui lui indiquera qu'il est en train d'utiliser le bon masque M_i. Cependant, cette idée est illusoire : pour toute image S' autre que S, il existe un masque M' qui, quand on l'applique à l'image chiffrée C en faisant un XOR, donne S' (il s'agit du masque M' = C XOR S'). En conséquence, en essayant systématiquement tous les masques possibles (ce qui par ailleurs n'est pas envisageable du fait de leur trop grand nombre), l'espion tombera sur une fausse solution S' avec la même probabilité que sur la véritable image secrète S. Cela étant vrai de n'importe quelle fausse solution S', pour celui qui n'a en main que C, il n'existe aucun moyen de distinguer S de n'importe quelle autre image S', et donc aucun moyen de

© Pour la Science - n° 416 - Juin 2012