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

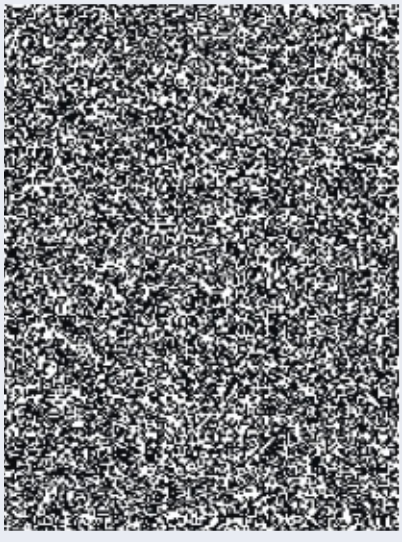
Lorsque Alain souhaite communiquer à Béatrice une image secrète S, il choisit l'un des masques M_i dont il dispose ; il utilise son ordinateur pour calculer l'image $C = M_i$ XOR S qu'il poste ou fait remettre sous la forme d'un transparent à Béatrice en lui indiquant le numéro *i* du masque utilisé. 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