2. Un système absolument sûr : le masque jetable

En 1915, l'ingénieur Gilbert Vernam, alors en charge de la sécurité des téléscripteurs au sein du département *recherche et développement* de l'entreprise AT&T, dépose un brevet pour un dispositif dont l'objet, selon ses propres termes, est « d'assurer la sécurité des transmissions de messages, et par suite, de fournir un système où les messages peuvent être transmis et reçus en clair, ou codés de manière connue, mais où les impulsions du signal sont si altérées avant leur transmission sur la ligne qu'elles sont inintelligibles à quiconque les intercepte ».

Les téléscripteurs transmettent les textes à l'aide d'un codage inscrit sur un ruban perforé. Chaque caractère est codé par cinq unités qui vont se traduire par le passage ou non du courant électrique. L'idée de Vernam est de combiner le ruban qui contient le texte en clair avec un second ruban. La règle de combinaison est la suivante

$$0 + 0 = 0$$
$$0 + 1 = 1$$
$$1 + 0 = 1$$
$$1 + 1 = 0$$

Ce codage, connu aujourd'hui sous le nom de *ou exclusif*, présente l'avantage de rendre l'opération de déchiffrement identique à l'opération de chiffrement. Il n'y a donc qu'une seule sorte de réalisation électromécanique à prévoir. En utilisant un ruban identique on retrouvera le message clair.

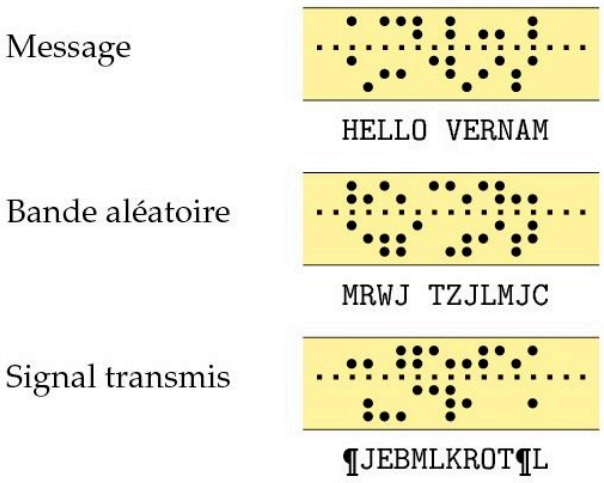

Fig. 2.2 Le système de Vernam. La première bande perforée contient le message en clair. Les signaux sont combinés avec ceux d'une deuxième bande perforée contenant des caractères aléatoires. Le résultat de la combinaison est un signal chiffré, illustré ici par une troisième bande. Ce signal est transmis par le système télégraphique. A la réception, une bande perforée identique à la bande aléatoire utilisée à l'émission permet de reconstituer le message en clair à partir du signal reçu.

L'intérêt de cette invention est clair : le chiffrement est intégré à la chaîne de transmission. Les opérateurs n'ont pas à s'en préoccuper. La seule contrainte est de placer dans la machine la bonne bande-clé, identique pour le chiffrement et le déchiffrement.

Il sera très tôt établi que la seule clé sûre est une clé aléatoire, comparable en longueur au message et utilisée une seule fois (*one-time pad*). Pour cette raison, ce procédé est appelé *masque jetable*, le ruban servant de masque devant être jeté après usage. Cette assertion de sécurité sera prouvée par Claude Shannon dans un article publié en 1949, montrant que si le ruban-clé contient une séquence de caractères aléatoires et indépendants, alors le système de Vernam atteint la sécurité inconditionnelle : quels que soient les moyens de calcul dont il dispose, l'adversaire n'a pas de meilleure stratégie que d'essayer de deviner le message en clair en le tirant au hasard et de compter sur sa chance.

Ce système sera rapidement adopté pour les communications de très haut niveau de sensibilité. Ce qu'on appelle le *téléphone rouge*, mis en place le 30 août 1963 entre les présidences américaine et soviétique à la suite de la crise des missiles de Cuba de 1962 était d'abord un téléscripteur, chiffré selon ce procédé avec des bandes aléatoires transportées par la valise diplomatique.