Qu'est-ce que la cryptologie ?

Dr David-Olivier Jaquet-Chiffelle

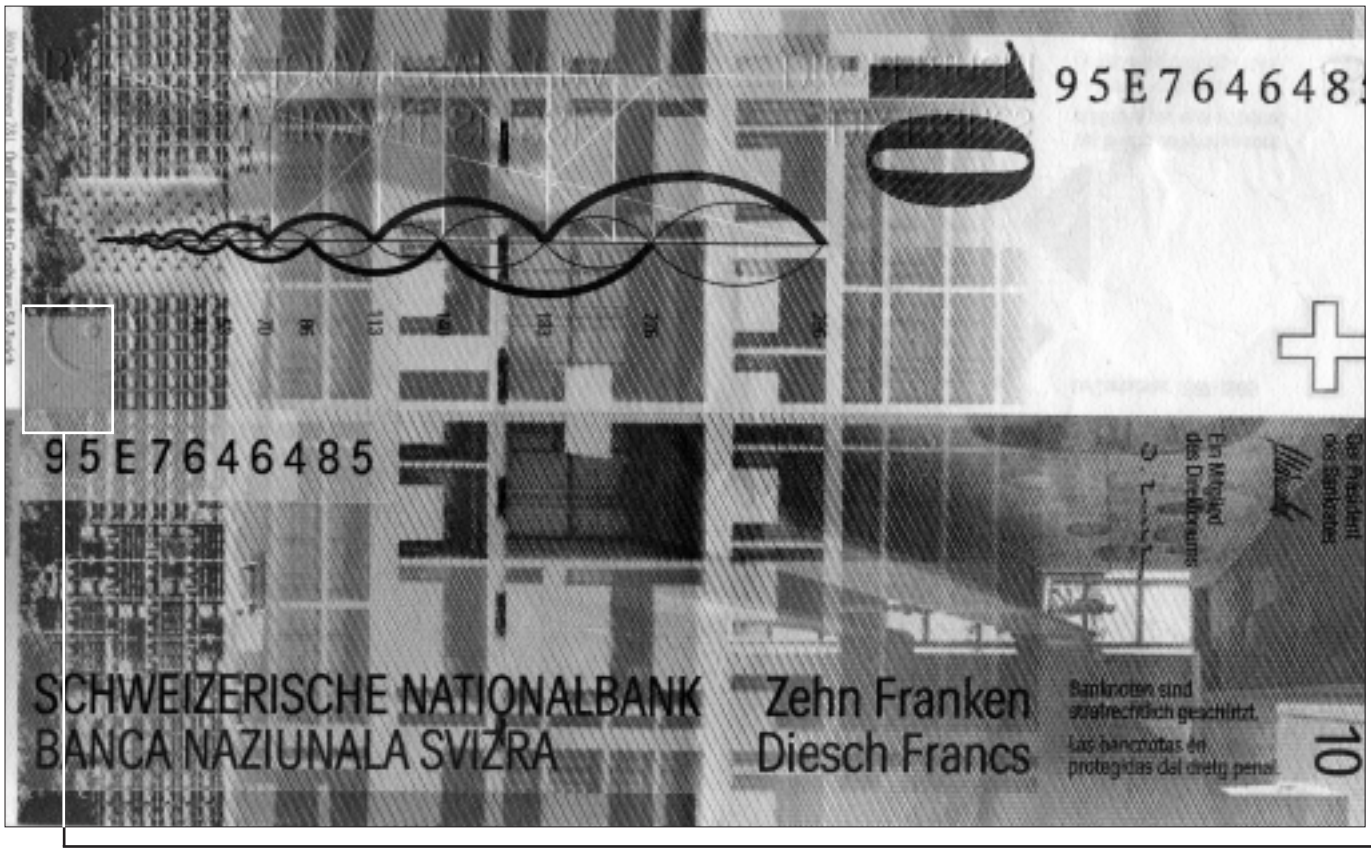
Historiquement, la cryptologie s'apparente à la "science" des codes secrets ; aujourd'hui, on parle plutôt de la science de l'intégrité de l'information. Elle regroupe la cryptographie (code making) et la cryptanalyse (code breaking).

La cryptographie vise deux objectifs dont on peut montrer qu'ils sont indépendants l'un de l'autre :

- la confidentialité des données et/ou l'anonymat des participants,
- l'authenticité des données et/ou des participants.

Jusqu'à récemment, l'usage de la cryptologie se limitait essentiellement aux applications gouvernementales : communications militaires et entre personnes haut placées du gouvernement, services diplomatiques et services secrets. Depuis le début des années septante, les applications civiles n'ont cessé de croître. Par exemple, la cryptologie permet de sécuriser des bases de données et de protéger les communications électroniques entre banques; lorsqu'on prélève de l'argent à un bancomat, la liaison avec la banque est cryptée en arrière-plan ; lorsqu'on téléphone avec un Natel D (GSM), la communication est également cryptée jusqu'à la station de base. Avec l'essor d'Internet, la cryptologie se profile comme une science d'avenir (e-mail sécurisé, e-commerce, argent électronique) et les applications qui l'utilisent se multiplient.

La plupart des applications modernes n'auraient jamais vu le jour sans la découverte, à la fin des années septante, de la cryptographie à clé publique : la clé utilisée pour crypter un message n'a plus besoin d'être secrète (pour décrypter le message, le destinataire utilise une autre clé, privée et bien entendu secrète). Même la personne qui a crypté le message n'ar-



rive plus à le décrypter !
Les algorithmes cryptographiques modernes et les méthodes les plus performantes de cryptanalyse font massivement appel aux mathématiques, tout particulièrement à la théorie des nombres et aux mathématiques discrètes. Par exemple, les nombres premiers —qui intéressaient déjà Euclide il y a plus de deux mille ans— sont plus que jamais d'actualité : ils jouent un rôle central dans la cryptographie à clé publique. Des sommes importantes sont investies dans la recherche d'algorithmes mathématiques permettant la factorisation des grands entiers (plus de 150 chiffres). Et ce n'est pas un hasard si la NSA (National Security Agency), aux Etats-Unis, est considérée comme le plus grand employeur de mathématiciens au monde…
Pour terminer, j'aimerais donner un exemple de cryptographie rudimentaire : la stéganographie. Il ne s'agit pas à proprement parler d'une méthode de cryptage ; la stéganographie consiste plutôt à "cacher" l'information. Toutefois, en plus de son rôle historique, elle garde aujourd'hui encore tout son intérêt lorsqu'on la combine avec un algorithme mathématique de cryptage. On trouve un bel exemple de stéganographie sur le billet de 10 SFR. Qui se doute que sur nos billets de banque se cache un texte qui parle d'un célèbre architecte suisse, Charles Edouard Jeanneret-Gris, né à la Chaux-de-Fonds en 1887? Presque chaque jour, pourtant, on utilise un billet de 10 francs. C'est bien là la force de la stéganographie !

"Le Corbusier hat als Architekt Urbanist Maler und Theoretiker bahnbrechende und visionäre Anwendungen für den Wohn und Städtebau verwirklicht"