Collection Histoire des Sciences
Série Études

Cryptologie et mathématiques

Une mutation des enjeux

Marquée du sceau du secret, l'activité cryptographique s'est longtemps exercée dans les secteurs militaires, diplomatiques ou commerciaux, à l'écart des lieux publics de production du savoir. D'abord ancrée dans les jeux d'écriture, ses techniques sont nées de pratiques matérielles dont les machines à chiffrer ont constitué un ultime raffinement. La cryptologie n'est devenue que récemment une discipline académique, enseignée dans les universités, et installée au cœur des mathématiques. Au carrefour entre science, industrie et société, elle envahit aujourd'hui en silence de nombreux vecteurs de communication sociale : carte bancaire, téléphone mobile, commerce en ligne, etc.

La mise en place des réseaux de communication, du télégraphe à Internet, s'est accompagnée d'une mutation de la problématique de la sécurité des messages vers celle de la sécurité de systèmes de communication. Le développement des ordinateurs marque un tournant technologique majeur qui met au premier plan l'algorithme. Les fonctions cryptographiques sont dès lors réalisées dans des dispositifs spécialement conçus et fabriqués pour effectuer les opérations requises, contribuant à les rendre opaques.

Dans cet ouvrage, historiens, acteurs opérationnels et chercheurs de cette discipline confrontent leurs analyses et leurs témoignages pour interroger les conditions et les conséquences de ces mutations, tant sur l'évolution des contenus de la discipline que sur le terrain des échanges en démocratie, lorsque le silence le dispute à la transparence.

Marie-José Durand-Richard *est historienne des mathématiques. Elle a initié un enseignement d'histoire de la cryptologie à l'université de Paris-8 Vincennes-Saint-Denis. Elle est aujourd'hui chercheuse associée du laboratoire SPHERE (Paris), et étudie l'histoire des machines mathématiques.*

Philippe Guillot *est actuellement maître de conférences à l'université Paris-8 Vincennes-Saint-Denis en charge des cours de cryptologie, d'histoire de la cryptologie et d'algorithmique algébrique dans le master « Mathématiques fondamentales et protection de l'information ».*

Illustration de couverture de Clément Doranlo.

32 €
ISBN : 978-2-343-02522-3

Sous la direction de
Marie-José Durand-Richard et Philippe Guillot

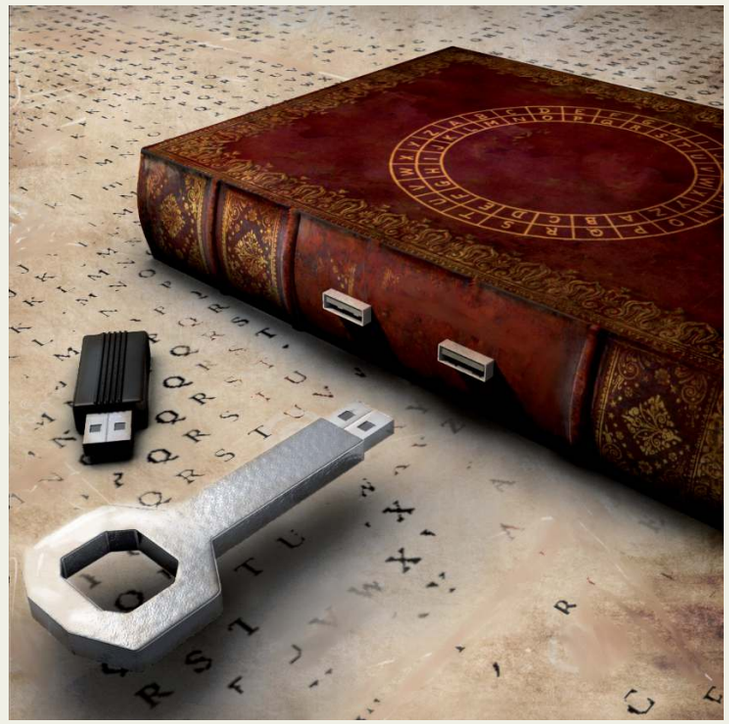
Cryptologie et mathématiques
Une mutation des enjeux

Collection Histoire des Sciences
Série Études

Sous la direction de
Marie-José Durand-Richard et Philippe Guillot

Cryptologie et mathématiques

Une mutation des enjeux



L'Harmattan