

L'Harmattan



RETROUVEZ NOUS MAINTENANT !

<https://www.facebook.com/Editions.Harmattan>  
<https://twitter.com/HarmattanParis>  
<http://www.youtube.com/user/harmattan>

Édition - Diffusion

5-7, rue de l'École Polytechnique 75005 Paris

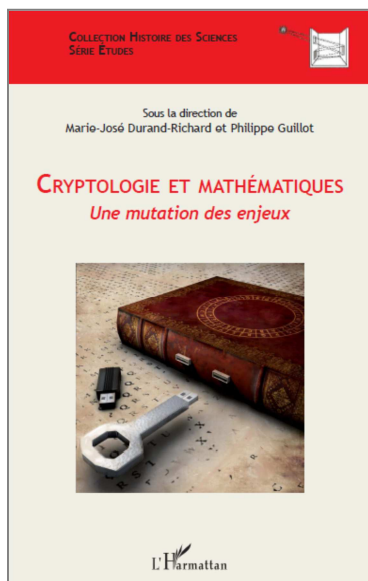
Tél. 01 40 46 79 20 (comptoir et renseignement libraires)

Tél. 01 40 46 79 14 (manuscrits et fabrication)

Tél. 01 40 46 79 22 (service de presse)

Fax 01 43 25 82 03 (commercial)

Fax 01 43 29 86 20 (manuscrits et fabrication)



## Cryptologie et mathématiques

Une mutation des enjeux

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

ISBN : 9782343025223 • 32 € • 312 pages

Collection : *Histoire des sciences*

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.

### LES AUTEURS

**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'algèbre algébrique dans le master « Mathématiques fondamentales et protection de l'information ».

### Contact

Service de promotion et de diffusion

Marianne Ravaud

7, rue de l'École polytechnique 75005 Paris

Marianne.ravaud@harmattan.fr

## SOMMAIRE

### Introduction - Marie-José DURAND-RICHARD et Philippe GUILLOT

1. L'ancrage de la cryptologie dans les jeux d'écriture, Marie-José DURAND-RICHARD et Philippe GUILLOT
2. Sur l'extraction de l'obscur, *Al-KINDI* - Traduction Abderrahman DAIF et Kaltoum TANTAOUI
3. Les travaux de la Section du Chiffre pendant la Première Guerre Mondiale, Sophie DE LASTOURS
4. Du message chiffré au système cryptographique, Marie-José DURAND-RICHARD
5. La cryptologie gouvernementale française et ses relations avec les mathématiques, André CATTIEUW
6. Les nouvelles orientations de la cryptographie, Whittfield DIFFIE et Martin E. HELLMAN – Traduction Marie-José DURAND-RICHARD et Philippe GUILLOT
7. Pourquoi et comment la cryptologie vient de surgir dans le domaine public ? le rôle de la carte à puce, Louis GUILLOU
8. Cryptographie et théorie des nombres : quelques remarques sur la mémoire d'une rencontre, Catherine GOLDSTEIN
9. L'influence de la cryptologie moderne sur les mathématiques et l'université, Jean-Louis NICOLAS
10. La relation agitée entre mathématiques et cryptographie Neal KOBLITZ - Traduction Marie-José DURAND-RICHARD et Philippe GUILLOT

### ABONNEMENT GRATUIT A NOTRE NEWSLETTER MENSUELLE (présentation des nouveautés) :

Je souhaite recevoir votre newsletter par voie postale :

-NOM, prénom :

-Adresse :

-CP, ville :

**Vous pouvez aussi vous inscrire à notre Newsletter électronique hebdomadaire sur notre site [www.harmattan.fr](http://www.harmattan.fr) rubrique Les Editions**

### BON DE COMMANDE valable pour la vente par correspondance uniquement

à retourner à L'HARMATTAN 7 rue de l'École Polytechnique - 75005 Paris

Veuillez me faire parvenir ..... exemplaire(s) du livre : **Cryptologie et mathématiques** • Prix 32 €

Frais de port à ajouter : 3,50 euros (1 livre) + 1 euro par livre supplémentaire

NOM : .....

ADRESSE.....

Ci-joint un chèque de ..... €. (À l'ordre de L'Harmattan)

Pour l'étranger, vos règlements sont à effectuer :

- en euros sur chèques domiciliés sur banque française

- par virement en euros sur notre CCP Paris (IBAN : FR 04 2004 1000 0123 6254 4N02 011 / BIC : PSSTFRPPPAR)

- par carte bancaire (Visa uniquement) N°..... date d'expiration...../...../...../

le numéro CVx2 (les 3 derniers chiffres se trouvant au dos de votre carte, à gauche de votre signature)

Nous possédons plusieurs librairies dans le 5<sup>e</sup> arrondissement de Paris, chacune ayant un fonds spécifique.

Vous pourrez trouver ou commander cet ouvrage à :

#### **Harmattan - Sciences Humaines**

21, rue des Ecoles

75005 – Paris

tel : 01 46 34 13 71

Vous pouvez aussi commander l'ouvrage de Marie-José Durand-Richard et Philippe Guillot

à votre libraire habituel

*ou sur notre site internet :*  
[www.editions-harmattan.fr](http://www.editions-harmattan.fr)

## Contact

### Service de promotion et de diffusion

Marianne Ravaud

7, rue de l'École polytechnique 75005 Paris

Marianne.ravaud@harmattan.fr