Hermes Lavoisier
14, rue de Provigny 94236 Cachan cedex, France • tél.:+33 (0)1 47 40 67 00 • fax:+33 (0)1 47 40 67 02 • e-mail : info@Lavoisier.fr

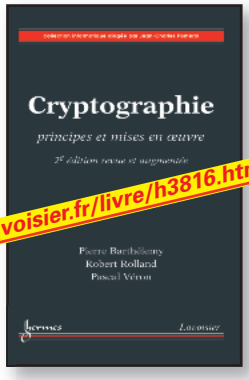
VIENT DE PARAITRE

Collection informatique dirigée par Jean-Charles Pomerol

Cryptographie

Principes et mises en œuvre

2e édition revue et augmentée



www.lavoisier.fr/livre/h3816.html

Pierre BARTHÉLEMY, Robert ROLLAND, Pascal VÉRON

Quels sont les enjeux de la cryptographie moderne ? Quels sont ses objets, son langage ? Quelles sont les solutions actuelles aux problèmes de confidentialité, d'authentification et d'anonymat ? Quel degré de confiance peut-on accorder à ces solutions ?

Cette seconde édition, enrichie et mise à jour, propose un panorama des outils et procédés de la cryptographie. Après avoir présenté et analysé les méthodes, cet ouvrage offre une description précise des techniques mathématiques indispensables et des principales primitives cryptographiques. Les fonctionnalités de base comme le chiffrement, la signature ou l'authentification, sont étudiées dans le cadre de la cryptographie à clé publique ou secrète.

Cryptographie analyse également l'interaction entre ces notions ainsi que leurs mises en œuvre dans des protocoles généraux et dans des applications concrètes. Il s'intéresse aux attaques contre les systèmes cryptographiques y compris celles par canaux cachés et par injection de fautes. Il aborde le domaine désormais indispensable des preuves de sécurité.

L'auteur

• **Pierre Barthélemy** est ingénieur de recherches au CNRS (Institut de Mathématiques de Luminy). Il s'intéresse plus particulièrement aux services de l'internet et à leur sécurisation.

• **Robert Rolland** est chercheur associé à l'Institut de Mathématiques de Luminy et au laboratoire ERISCS (Aix-Marseille Université). Son domaine de recherche est centré sur les mathématiques et leurs applications à la cryptographie et au codage.

• **Pascal Véron** est enseignant à l'Université du Sud Toulon-Var et chercheur au sein de l'Institut de Mathématiques de Toulon et du Var. Ses domaines de recherche sont la cryptographie, la théorie algébrique du codage et les liens entre ces deux disciplines.

Sommaire

95 € • 472 pages • 16 x 24 • 2e éd. 2012 • ISBN : 978-2-7462-3816-9

BON DE COMMANDE

à retourner complété avec votre règlement sous enveloppe dûment affranchie à : *Lavoisier* - 14, rue de Provigny 94236 Cachan cedex **ou à faxer au** : 01 47 40 67 02

Titre de l'ouvrage	ISBN	Prix TTC	Qté	Total
Cryptographie - 2e éd.	978-2-7430-3816-9	95 €		

Plus simple et plus rapide, je commande sur : www.lavoisier.fr

Frais de port

Total TTC

Frais de port

Si paiement à la commande (France métropolitaine, Suisse, UE*) :
- ▶ Offerts pour toute commande supérieure à 60 €
- ▶ 7 € pour toute commande inférieure à 60 €

Si paiement différé : port en sus.
* Pour tout autres pays, envoi express ou par avion, nous consulter : info@lavoisier.fr

Une facture acquittée sera jointe au colis.

Je joins mon règlement à la commande et je paye par :

☐ Chèque bancaire ou postal payable en France à l'ordre de LAVOISIER S.A.S.

☐ Carte bancaire n° |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_| Date d'expiration : |_|_| |_|_| Cryptogramme : |_|_|_|

COORDONNEES

N° DE CLIENT |_|_|_|_|_|_|_|_|_|_|

NOM/PRÉNOM.....FONCTION.....

INSTITUTION .....TVA INTRACOMMUNAUTAIRE .....

ADRESSE DE FACTURATION.....

.....

ADRESSE DE LIVRAISON (SI DIFFÉRENTE).....

E-MAIL .....TÉL. |_|_|_|_|_|_|_|_|_|_|

Date et signature obligatoire

Suivre ma commande : +33 (0) 1 47 40 67 00