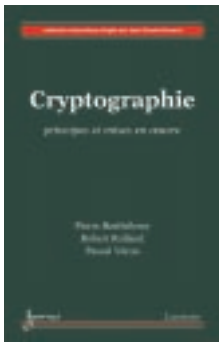
Hermes Lavoisier
14, rue de Provigny 94236 Cachan cedex, France • tél. : +33 (0)1 47 40 67 00 • fax : +33 (0)1 47 40 67 02 • e-mail : info@Lavoisier.fr

VIENT DE PARAITRE

Collection informatique dirigée par Jean-Charles Pomerol



Cryptographie

Principes et mises en œuvre

Pierre Barthélemy, Robert Rolland, Pascal Véron

Quels sont les problèmes de la cryptographie moderne ? Quels sont ses objets, son langage ? Quelles sont les solutions actuelles aux problèmes de confidentialité et d'authentification ? Quel degré de confiance peut-on accorder à ces solutions ?
L'ouvrage, sous forme d'un cours de cryptographie générale, expose l'état actuel des réponses à ces questions. Il comprend une présentation et une analyse des méthodes ainsi qu'une description précise des techniques mathématiques indispensables et des principales primitives cryptographiques.
Les fonctionnalités de base – le chiffrement, la signature et l'authentification – sont étudiées dans le cadre de la cryptographie à clé publique et de la cryptographie à clé secrète. *Cryptographie* analyse également l'interaction entre ces notions ainsi que leurs mises en oeuvre dans des protocoles généraux et dans des applications concrètes. Il s'intéresse aux attaques contre les systèmes cryptographiques et aborde le domaine en plein essor des preuves de sécurité.

Les auteurs

• **Pierre Barthélemy** est ingénieur de recherche au CNRS (Institut de mathématiques de Luminy). Il s'intéresse plus particulièrement aux services de l'Internet et à leur sécurisation.
• **Robert Rolland** est enseignant à l'université de la Méditerranée et chercheur à l'Institut de mathématiques de Luminy.
• **Pascal Véron** est enseignant à l'université du Sud Toulon-Var et chercheur au sein du groupe de recherche en informatique et mathématiques.

Sommaire

Avant-propos
Préface
1. Introduction - Un tour d'horizon
2. Cryptographie à clé publique
3. Cryptogaphie à clé secrète
4. Mise en oeuvre des outils cryptographiques
5. Cryptographie et codes correcteurs d'erreurs
6. La sécurité des systèmes cryptographiques
Annexes
A. Complexité des algorithmes
B. Arithmétique
C. Développement en fraction continue
D. Paradoxe des anniversaires
Bibliographie
Index

85 € • 416 pages • 16 x 24 • 2005 • ISBN : 2-7462-1150-5

Bon de commande

• BARTHÉLEMY / ROLLAND / VÉRON :
Cryptographie.....ex. x 85 € ISBN : 2-7462-1150-5

À faxer au : +33 (0)1 47 40 67 02
ou à retourner à l'adresse ci-dessous.

➤ Adresse de facturation :
TVA/VAT : .....
société/organisme/service : .....
.....
nom/prénom : .....
qualité : .....
adresse : .....
code postal : ..... ville : .....
Pays : .....
tél. : ..... fax : .....
e-mail : .....
adresse complète de livraison (si différente) : .....
.....
.....

Lavoisier LIBRAIRIE
Lavoisier
14, rue de Provigny
F-94236 CACHAN CEDEX

www.Lavoisier.fr

Renseignements complémentaires sur les ouvrages au : +33 (0)1 42 65 39 95, suivi de votre commande au : +33 (0)1 47 40 67 00

➤ **Règlement joint par :** Franco de port (UE, Suisse) / Frais de port : 10 € (Autres pays)

❑ bon de commande administratif ❑ chèque (à l'ordre de Lavoisier) ❑ habituel entre nous
❑ carte bleue / Visa date d'expiration : ⌊_⌊_⌊ ⌊_⌊_⌊
n° de carte : ⌊_⌊_⌊_⌊_⌊ ⌊_⌊_⌊_⌊_⌊ ⌊_⌊_⌊_⌊_⌊ ⌊_⌊_⌊_⌊_⌊
notez les 3 derniers chiffres du n° au verso de votre carte bancaire : ⌊_⌊_⌊

date, signature, cachet