

collection informatique dirigée par Jean-Charles Pomerol

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 que sont 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. Ce livre analyse également l'interaction entre ces notions ainsi que leurs mises en œuvre dans des protocoles généraux et dans des applications concrètes. Enfin, cet ouvrage s'intéresse aux attaques contre les systèmes cryptographiques et au 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.

hermes
Science
— publication —

www.hermes-science.com

ISBN 2-7462-1150-5



Pierre Barthélemy
Robert Rolland
Pascal Véron

Cryptographie



collection informatique dirigée par Jean-Charles Pomerol

Cryptographie

Pierre Barthélemy
Robert Rolland
Pascal Véron

hermes

Lavoisier