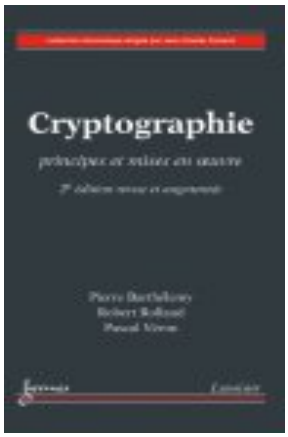
Cryptographie : principes et mises en oeuvre.
Auteurs : Pierre Barthélemy, Robert Rolland, Pascal Véron



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 œuvre 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.

Site de mises à jour et compléments