CRYPTOGRAPHIE

Théorie et pratique

2e édition

Douglas Stinson
Traduction de Serge Vaudenay, Gildas Avoine et Pascal Junod

vuibert

Douglas Stinson

Cryptographie

Théorie et pratique

Traduction de Serge Vaudenay,
Gildas Avoine et Pascal Junod

Vuibert Informatique

Table des matières

2e ÉDITION

CRYPTOGRAPHIE

Cryptographie – Théorie et pratique est un ouvrage de référence, universellement traduit et apprécié. Il offre une présentation lisible, et sous forme mathématique précise, des thèmes majeurs de la cryptographie. Il aborde tous les sujets de recherche contemporains, donnant au lecteur introduction et étude des résultats fondamentaux.

La plupart des algorithmes sont présentés sous forme de pseudo-programmes avec des exemples et une présentation informelle des idées sous-jacentes. Cet ouvrage donne une étude méthodique et compréhensible de tous les sujets essentiels en cryptologie : cryptographie à clef secrète, standard de chiffrement, systèmes à clef publique.

Cette deuxième édition prend en compte les avancées techniques de ces cinq dernières années. De nombreux nouveaux sujets ont ainsi été introduits et une mise à jour approfondie de ceux traités dans la première édition a été menée. La nouvelle édition aborde les sujets suivants :

- les plus récents standards FIPS (*Federal Information Processing Standards*) : AES (*Advanced Encryption Standard*), SHA-1 (*Secure Hash Algorithm*), ECDSA (*Elliptic Curve Digital Signature Algorithm*) ;
- l'utilisation de réseaux de substitution-permutation pour le chiffrement par blocs et les concepts d'analyse ;
- les cryptanalyses linéaire et différentielle ; le modèle de l'oracle aléatoire pour les fonctions de hachage ;
- la sécurité sémantique de RSA et OAEP (*Optional Asymmetric Encryption Padding*) ;
- l'attaque de Wiener sur les exposants RSA.

Toutes ses qualités demeurent : explications claires et précises, rigueur mathématique, description en pseudo-code des algorithmes, nombreux exemples.

L'auteur

Douglas Stinson, *docteur en inform[illegible]tique, est professeur à la fac[illegible]de mathématiques de l'université de Waterloo (Ontario). Il a été directeur de la publication [illegible] Journal of [illegible]signs [illegible] est également membre du comité éditorial de quatre autres journaux. Il a p[illegible]blié de nombreux articles dans [illegible]s de la cryptographie, de la combinatoire et de l'informatique théorique. Il a obtenu en 1994 la médaille Hall de l'Institute of Combinatorics and Its Applications.*

Les traducteurs

Serge Vaudenay*, ancien élève de l'École normale supérieure de la rue d'Ulm, est titulaire d'un doctorat en informatique obtenu à l'université de Paris VII. Chercheur au CNRS puis professeur à l'EPFL de Lausanne où il dirige le Laboratoire en sécurité et cryptographie (LASEC), ses recherches concernent principalement la sécurité des algorithmes cryptographiques.*
Gildas Avoine *est titulaire d'un DEA en informatique (intelligence artificielle et algorithmes) et diplômé de l'EPFL (systèmes de communication).* ***Pascal Junod*** *est diplômé du Swiss Institute of Technology de Zurich. Ils sont tous deux assistants au LASEC.*

vuibert

ISBN 2-7117-4800-6