SCIENCES SUP

Cours et exercices corrigés

Licence 3 • Master 1 • Écoles d'ingénieurs

INTRODUCTION À LA CRYPTOGRAPHIE

Johannes Buchmann

DUNOD

INTRODUCTION À LA CRYPTOGRAPHIE

Cours et exercices corrigés

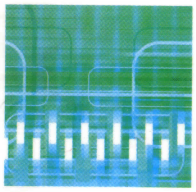
Johannes Buchmann
professeur d'informatique et de mathématiques
à l'université de Darmstadt (Allemagne)

Traduit de l'anglais par
JACQUES VÉLU
professeur au CNAM de Paris

Table des matières

CHAPITRE 2 • CONGRUENCES ET CLASSES RÉSIDUELLES

SCIENCES SUP



Johannes Buchmann
Traduit de l'anglais par Jacques Vélu

INTRODUCTION À LA CRYPTOGRAPHIE

Les techniques de cryptographie présentent de nombreux usages. De la signature des documents électroniques à la protection du copyright, elles permettent d'assurer la confidentialité, l'accès et l'identification des documents.

Ce livre présente, sans formalisme mathématique excessif, les outils mathématiques et algorithmiques utiles à la compréhension de la cryptographie. Le cours est complété par des exercices simples dont la moitié trouvent leurs corrigés en fin d'ouvrage.

Ce manuel s'adresse aux étudiants en Licence 3 ou Master 1 de mathématiques appliquées ou d'informatique ainsi qu'aux élèves ingénieurs.

JOHANNES BUCHMANN
est professeur d'informatique et de mathématiques à l'université de Darmstadt (Allemagne).

JACQUES VÉLU
est professeur au CNAM de Paris.

MATHÉMATIQUES
PHYSIQUE
CHIMIE
SCIENCES DE L'INGÉNIEUR
INFORMATIQUE
SCIENCES DE LA VIE
SCIENCES DE LA TERRE

ISBN 2 10 049622 0

www.dunod.com

DUNOD