A classical introduction to cryptography exercice book

Type de contenu : Texte

Titre(s) : A classical introduction to cryptography exercice book [texte imprimé] / Thomas Baignères, Pascal Junod, Yi Lu [et al.]

Autre(s) auteur(s) : Junod, Pascal
Lu, Yi

Editeur, producteur : New York : Springer science and business media, 2006

Description matérielle : 254 p. ; 24 cm

ISBN : 978-1-4419-3912-8

Note sur les bibliographies et les index : Bibliogr. p. 249-254

Résumé ou extrait : Sommaire : Préhistoire de la cryptographie. Cryptographie conventionnelle. Primitives spécifiques de cryptographie conventionnelle. Analyse conventionnelle de sécurité. Protocoles de sécurité en cryptographie conventionnelle. Algèbre algorithmique. Théorie algorithmique des nombres. Eléments de théorie de la complexité. Cryptographie à clé publique. Protocoles cryptographiques. De la cryptographie à la sécurité des communications.

Sujet - Nom commun : Cryptographie
Sécurité des systèmes