

A classical introduction to cryptography

Type de contenu : Texte

Titre(s) : A classical introduction to cryptography [texte imprimé] : applications for communications security / Serge Vaudenay

Editeur, producteur : New York : Springer science and business media, 2010

Description matérielle : 335 p. ; 24 cm

ISBN : 978-1-4419-3797-1

Note sur les bibliographies et les index : Bibliogr. p. 313-327. Index

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. Éléments 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