

Cryptographie : théorie et pratique

Type de contenu : Texte

Titre(s) : Cryptographie : théorie et pratique / Stinson, Douglas Robert

Mention d'édition : 2e éd.

Editeur, producteur : Paris : Vuibert informatique, 2013

Description matérielle : XIV-337 p. ; 24 cm

ISBN : 978-2-7117-4800-6

Note sur les bibliographies et les index : Bibliogr. p 314-327. Index

Note sur le contenu : Manuel

Résumé ou extrait : Cet ouvrage offre une présentation sous forme mathématique précise, de thèmes majeurs de la cryptographie. Cette 2e édition aborde les plus récents standards FIPS : AES, SHA-1, ECDSA ; l'utilisation de réseaux de substitution-permutation pour la conception de chiffrement par blocs et les concepts d'analyse ; les cryptanalyses linéaire et différentielle ; le modèle Random d'Oracle pour les fonctions de hachage ; la sécurité sémantique...

Sujet(s) : cryptographie
sécurité des données
sécurité informatique