Arithmétique modulaire et cryptologie

Type de contenu : Texte

Type de médiation : sans médiation

Titre(s) : Arithmétique modulaire et cryptologie

Auteur(s) : Meunier, Pierre (1944-....)

Editeur, producteur : Toulouse : Cépaduès-éd., impr. 2010
(31-Toulouse; Impr. Messages)

Description matérielle : 179 p. : couv. ill. ; 21 cm

ISBN : 978-2-85428-954-1

EAN : 9782854289541

Classification décimale Dewey : 513.6 23

Résumé ou extrait : La cryptologie, science des écritures secrètes, peut schématiquement être configurée de manière duale à l'aide du couple : cryptographie-cryptanalyse : la cryptographie ayant pour objet la création de procédés techniques de codage les plus sûrs possibles, la cryptanalyse, au contraire, cherchant à élaborer des protocoles mathématiques permettant de casser les cryptosystèmes. La plupart de ces objectifs sont atteints grâce à la subtilité et l'élégance de l'arithmétique modulaire. Cet ouvrage est issu d'un enseignement en mathématiques Spéciales MP* résultant à la fois d'un approfondissement en algèbre destiné aux candidats des ENS et d'une adaptation des mathématiques disponibles en Spé MP* aux techniques de codage et de décodage numériques. [4e de couv.]

Sujet(s) : Arithmétique Arithmétique modulaire Cryptographie

Sujet - Nom commun : Arithmétique modulaire
Cryptographie