

Tome 2 : Mathématiques, espionnage et piratage informatique

Codage et cryptographie, par Joan Gómez.

L'intégrité et la confidentialité des communications dépendent de codes complexes dont la conception repose sur les mathématiques.

Ce livre propose un voyage stimulant au coeur de l'arithmétique de la sécurité et du secret, en s'arrêtant, entre autres, sur les chiffrements qui ont décidé du destin des nations et sur le langage de communication des ordinateurs.

Sommaire :

Préface

Chapitre 1 – Jusqu'où va la sécurité de l'information ?

Les codes, les chiffres et les clés

Clés privées et clés publiques

Le "télégramme Zimmermann"

Le bureau 40 se met au travail

Chapitre 2 – La cryptographie de l'Antiquité au XIXème siècle

La sténographie

La cryptographie par transposition

Rendre à César ce qui appartient à César

16 = 4 – L'arithmétique modulaire et les mathématiques du chiffre de César

En jouant aux espions

Au-delà du chiffre affine

L'analyse de fréquences

Un exemple en détail

Le chiffre polyalphabétique

La contribution d'Alberti

Le carré de Vigenère

Classer des alphabets

Le cryptanalyste anonyme

Chapitre 3 – Des machines qui encodent

Le code Morse

A 80 kilomètres de Paris

La machine Enigma

Décrypter le code Enigma

Les britanniques prennent le relais

Autres codes de la Seconde Guerre mondiale

Les "radiocodeurs" navajos

Les voies de l'innovation : le chiffre de Hill

Chapitre 4 – Dialoguer avec des zéros et des uns

Le code ASCII

Le système hexadécimal

Systèmes de numération et changements de base

Codes contre la perte d'informations

Les “autres” codes : les normes de l'industrie et du commerce

Les cartes de crédit

Les codes-barres

Le code EAN-13

Chapitre 5 – Un secret de polichinelle : la cryptographie à clé publique

Le problème de la distribution de clé

L'algorithme de Diffie-Hellman

Les nombres premiers au secours : l'algorithme RSA

L'algorithme RSA en détail

Pourquoi devrions-nous avoir confiance en l'algorithme RSA ?

Une assez bonne confidentialité

Authentification des messages et des clés

Les fonctions de hachage

Les certificats de clé publique

Mais alors, peut-on acheter sur Internet en toute sécurité ?

Chapitre 6 – Un futur quantique

Le traitement quantique

Le chat qui n'était ni vivant ni mort

Du bit au qubit

La fin de la cryptographie ?

Ce qu'enlève la mécanique quantique, la mécanique quantique le donne

Le chiffre indéchiffrable

32 centimètres de secret absolu

Annexe

Bibliographie

Index analytique