

LOGIQUE MATHÉMATIQUES INFORMATIQUE


L

M

I

INTRODUCTION AUX MÉTHODES DE LA CRYPTOLOGIE

B. BECKETT

MASSON 

2-005-189-1

LOGIQUE MATHÉMATIQUES
INFORMATIQUE

INTRODUCTION AUX MÉTHODES DE LA CRYPTOLOGIE

Brian BECKETT

Traduit de l'anglais par
Philippe BÉGUIN, Philippe KLEIN et Éric HENAULT

*Ouvrage traduit avec le
concours du Centre national
des lettres*

MASSON Paris Milan Barcelone Mexico 1990

Table des matières

Introduction	viii
1 Jeux de caractères et substitution	1
2 Codage par transposition et alphabets transposés	12
3 La sécurité par codage	28
4 Mathématiques appliquées à la cryptologie	47
5 Congruences et arithmétique modulaire	57
6 Décalages, inversions et polyalphabets	73
7 Nombres premiers et inverses multiplicatifs	91
8 Logarithmes et exponentielles	107
9 Systèmes cryptographiques à clé publique	124
10 Codes polyalphabétiques et à clé automatique	142
11 Codes polygraphiques	160
12 Codes matriciels	176
13 Matrices et systèmes d'équations	193
14 La faiblesse du linéaire	202
15 Codes binaires	230
16 Le Standard de Codage des Données (D.E.S.)	249
17 Historique et idiosyncrasies de la cryptologie, la cryptologie « à faire soi-même »	284
Lectures complémentaires	327
Index	329