



Manuel de cryptographie

Avec 112 figures graphiques et tableaux.

Auteur : général L. Sacco, ancien chef de bureau du chiffre de l'armée italienne.

Copyright 1951

Editions Payot Paris.

375 pages.

Préface du lieutenant-colonel R. Léger. Edition française par le capitaine J. Brès.

Voici un ouvrage de référence pour les chiffreurs confirmés. Ce livre très technique contient les méthodes de chiffrement classiques avec des méthodes de décryptement. Il est complété par les tableaux des fréquences de lettres et des bigrammes utiles pour les décrypteurs.

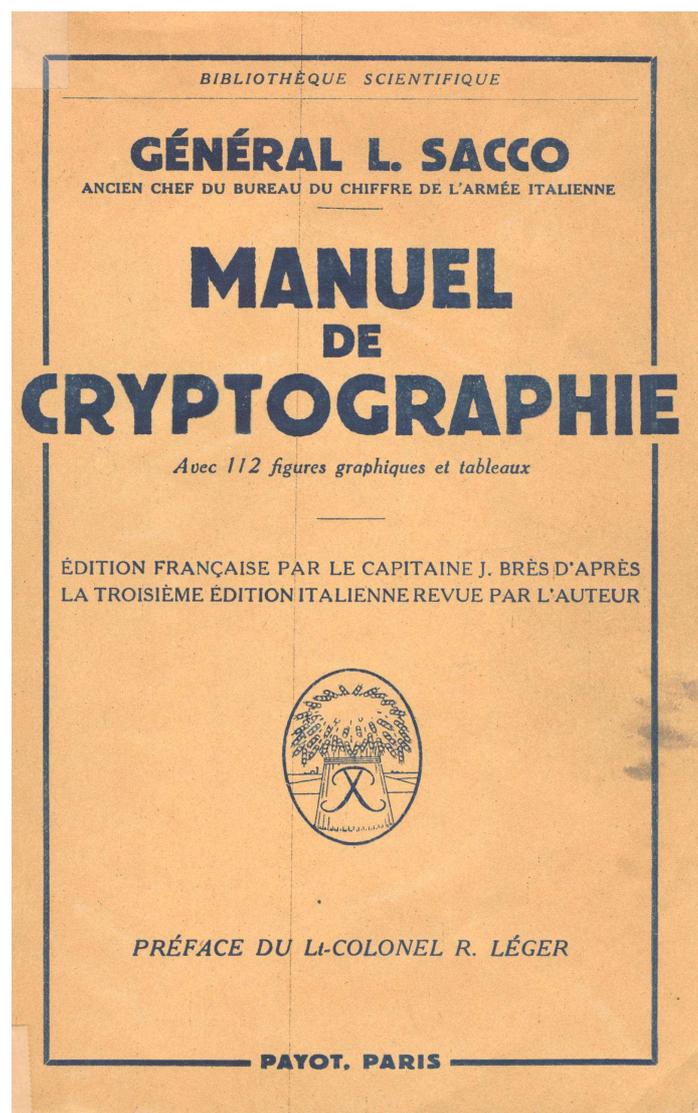


TABLE DES MATIÈRES

	Pages
INTRODUCTION	13
1. — Généralités	13
2. — Différents genres d'écritures secrètes.....	14
PREMIÈRE PARTIE	
ÉCRITURES CHIFFRÉES	
CHAP. I ^{er} . — <i>Généralités</i>	15
3. — Définitions fondamentales	15
4. — Éléments essentiels et opérations fondamentales du chiffrement	16
5. — Systèmes littéraux et à répertoire	16
CHAP. II. — <i>Principaux systèmes de chiffrement par lettres</i> ..	16
6. — Constitution des groupes chiffrés	16
7. — Chiffrement des nombres et des signes de ponc- tuation.....	17
8. — Clefs numériques et littérales	17
CHAP. III. — <i>Systèmes de transposition littérale</i>	18
9. — Généralités	18
10. — Transposition simple.....	18
11. — Transposition avec clefs.....	19
12. — Transposition avec grilles.....	21
13. — Grilles rotatives	21
14. — Grilles indéfinies (Sacco)	24
15. — Double transposition avec clef	26
CHAP. IV. — <i>Systèmes de substitution littérale</i>	27
16. — Généralités	27
17. — Règles de formation des alphabets chiffnants...	28
CHAP. V. — <i>Systèmes monoalphabétiques</i>	31
18. — Chiffrements monoalphabétiques simples	31
19. — Systèmes monoalphabétiques avec nulles et ho- mophones.....	32
20. — Chiffrement monoalphabétique par polyphones ...	34
CHAP. VI. — <i>Systèmes polyalphabétiques</i>	35
21. — Généralités	35
22. — Les chiffres de L. B. Alberti, de J. B. Bellaso et de J. B. Della Porta.....	36
23. — Table carrée, dite de Vigenère	40
24. — Chiffre militaire de poche.....	41
25. — Le chiffre de Sestri, dit de Beaufort, et les tables régulières.....	43

26. — Tables dérivées d'un seul alphabet désordonné .	44
27. — Manières d'allonger et d'interrompre la clef de chiffrement.....	47
A) Allongement de la clef	47
B) Interruption de la clef.....	48
28. — Déplacement du début de la clef	49
29. — Listes alphabétiques incohérentes.....	49
30. — Systèmes autochiffrants (autoclaves)	52
a) Autochiffrement au moyen du clair	52
b) Autochiffrement au moyen du chiffré.....	52
c) Autochiffrement totalisateur	52
CHAP. VII. — <i>Appareils pour chiffrement polyalphabétique.</i> ..	52
31. — Règles et cercles ou disques chiffrants.....	52
32. — Appareils polyalphabétiques à rondelles	58
CHAP. VIII. — <i>Substitution de polygrammes</i>	60
33. — Généralités	60
34. — Chiffre de Playfair.....	61
CHAP. IX. — <i>Substitutions de fractions de lettres</i>	64
35. — Généralités	64
36. — Chiffre Pollux	64
37. — Chiffre à damiers (Collon).....	65
38. — Chiffre de campagne allemand	68
39. — Chiffres Delastelle	69
CHAP. X. — <i>Double chiffrement littéral.</i>	71
40. — Généralités	71
41. — Substitution littérale et transposition simple avec clef	72
42. — Substitution par bigrammes et transposition.....	73
43. — Autres combinaisons de systèmes.....	74
CHAP. XI. — <i>Machines cryptographiques.</i>	74
44. — Généralités.....	74
45. — Machines chiffrantes monogrammatiques polyalphabétiques	76
A) Machines non autochiffrantes	78
a) Machine Kryha	78
b) Machine Hagelin (Teknik) - Suédoise	79
c) Machine Enigma.....	83
B) Machines autochiffrantes	86
a) Disque de Wheatstone	87
b) Machine Ducros.....	88
c) Machine Giovannuzzi.....	88
d) Machine multiple à chaînes.....	90
46. — Machines chiffrantes tomogrammiques, cryptotélégraphiques et cryptotéléphoniques.....	94
A) Machines cryptotélégraphiques.....	96
a) Dispositif Vernam	96
b) Téléimprimeur chiffrant Olivetti	96
c) Téléchiffreur Siemens	99
d) Dispositif Jammet	100
e) Systèmes à double fréquence.....	101
B) Machines cryptotéléphoniques.....	106
a) Inversion de fréquence.....	107
b) Transposition d'élément ou changement de phase.....	108
c) Déplacement de fréquence et changement de phase.....	110
d) Substitution d'amplitude.....	115
C) Systèmes cryptotéléidographiques.....	116
Système Belin.....	116

47. — Machines polygraphiques.....	116
a) Machines polygraphique Henkels	116
b) Machine Lester S. Hill	118
CHAP. XII. — Codes, dictionnaires ou répertoires chiffants...	120
48. — Généralités.....	120
49. — Les deux sortes de Codes	121
50. — Codes paginés.....	121
51. — Codes télégraphiques commerciaux.....	122
52. — Codes désordonnés	124
53. — Deuxième chiffrement ou surchiffrement des Codes	125
54. — Surchiffrement par transposition.....	126
55. — Surchiffrement par substitution alphabétique. Clefs additives ou soustractives.....	126
56. — Surchiffrement mixte par transposition et substitution.....	128
57. — Surchiffrement par polygrammes. Tables chiffantes	128
58. — Tableaux à groupes de lettres ou de nombres.....	128
59. — Surchiffrement avec mots prononçables.....	130
60. — Choix des mots chiffants.....	131
61. — Emploi des tableaux de surchiffrement.....	133

DEUXIÈME PARTIE

DÉCRYPTEMENT DES CRYPTOGRAMMES

CHAP. XIII. — Principes fondamentaux du décryptement.....	135
62. — Généralités.....	135
63. — Bases linguistiques de la cryptographie.....	136
64. — Circonstances qui peuvent favoriser le décryptement	137
65. — Etudes préliminaires sur les divers systèmes cryptographiques.....	138
66. — Méthode générale de travail.....	139
CHAP. XIV. — Données caractéristiques des principales langues.	140
67. — Généralités	140
68. — Langue française	141
69. — Langue italienne.....	143
70. — Langue espagnole.....	145
71. — Langue allemande.....	146
72. — Langue anglaise.....	148
73. — Langue serbo-croate.....	149
74. — Langue russe.....	151
CHAP. XV. — Résolution des systèmes de transposition.....	152
75. — Caractéristiques des cryptogrammes de transposition	152
76. — Solutions communes à tous les systèmes de transposition	154
77. — Transposition simple rectangulaire.....	158
78. — Transposition simple avec clef à rectangle complet.	158
79. — Transposition avec clef à rectangle incomplet.....	162
80. — Transposition avec clefs, de cryptogrammes ayant une partie commune	165
81. — Transposition par grilles rotatives.....	170
82. — Cryptogrammes provenant de grilles rotatives incomplètes	172
83. — Cryptogrammes obtenus par grilles continues	172
84. — Cryptogrammes de double transposition.....	173

CHAP. XVI. — <i>Caractéristiques des cryptogrammes de substitution littérale</i>	174
85. — Généralités	174
86. — Caractéristiques des cryptogrammes monoalphabétiques.....	174
87. — Caractéristiques des cryptogrammes polyalphabétiques à clef fixe ou à clef interrompue.....	175
88. — Caractéristiques des cryptogrammes polyalphabétiques autochiffrés avec le clair.....	176
89. — Caractéristiques des cryptogrammes polyalphabétiques autochiffrés avec le chiffré.....	178
CHAP. XVII. — <i>Décryptement des cryptogrammes de substitution littérale</i>	179
90. — Cryptogrammes monoalphabétiques	179
A) Textes continus sans espaces chiffrés.....	179
B) Textes continus avec espaces chiffrés ...	183
91. — Cryptogrammes polyalphabétiques à clef littérale courte.....	183
a) Détermination de la période, longueur de la clef.....	184
b) Calcul des présences, des moyennes fréquences quadratiques et des coïncidences.....	184
c) La confrontation des alphabets.....	186
d) Les symétries de position	187
e) Alphabets incohérents. Séparation des voyelles. Consonnes adjacentes.....	188
f) Identification des voyelles et des consonnes	189
92. — Exemple de decryptement de cryptogramme polyalphabétique à clef littérale courte.....	190
93. — Méthode générale de Kerckhoffs pour tous les systèmes polyalphabétiques à clef littérale....	193
94. — Décryptement des cryptogrammes autochiffrants.	197
A) Autochiffrement avec le clair.....	197
B) Autochiffrement avec le chiffré	200
95. — Cryptogramme mixte de transposition et substitution. Appareils à rondelles.....	201
A) Cryptogrammes mixtes	201
B) Appareils à rondelles.....	202
96. — Reconstitution des clefs et des alphabets.....	203
CHAP. XVIII. — <i>Décryptement des systèmes de substitution polygrammiques</i>	209
97. — Caractéristiques des systèmes polygrammiques...	209
98. — Décryptement du chiffre de Playfair.....	210
CHAP. XIX. — <i>Décryptement des systèmes de substitution « tomogrammique » (ou par fractions de lettres)</i>	218
99. — Caractéristiques des systèmes de substitution « tomogrammique ».....	218
100. — Décryptement du chiffre Pollux.....	219
101. — Décryptement du chiffre à damier, type Collon.	221
102. — Décryptement du chiffre de campagne allemand.	223
103. — Décryptement du chiffre Delastelle.....	225
A) Chiffre bifide.....	226
B) Chiffre trifide.....	235
CHAP. XX. — <i>Décryptement des systèmes à répertoires</i>	236
104. — Caractéristiques des cryptogrammes provenant de répertoires non surchiffrés	236
105. — Caractéristiques des cryptogrammes obtenus par surchiffrement de répertoires.....	237
106. — Considérations générales sur le decryptement des répertoires.....	238

107. — Décryptement des répertoires paginés non surchiffrés.....	240
108. — Décryptement des répertoires désordonnés non surchiffrés.....	243
109. — Décryptement des répertoires surchiffrés.....	246
110. — Décryptement des répertoires surchiffrés, le répertoire étant connu.....	247
111. — Décryptement des répertoires surchiffrés, le répertoire étant inconnu.....	250
112. — Conclusion sur les répertoires ou codes chiffants.	252
CHAP. XXI. — <i>Décryptement des machines à chiffrer</i>	253
113. — Généralités.....	253
114. — Décryptement des machines polyalphabétiques.	253
A) Machines non autochiffantes.....	253
B) Machines autochiffantes.....	257
115. — Décryptement des machines cryptotélégraphiques.	261
A) Système Jammes.....	261
B) Téléchiffreurs Olivetti et Siemens.....	263
C) Systèmes à double fréquence.....	264
116. — Machines polygrammiques.....	272
A) Machine Lester-S. Hill.....	272
B) Machine Henkels.....	273

TROISIÈME PARTIE

EMPLOI DES DIVERS SYSTÈMES CRYPTOGRAPHIQUES

CHAP. XXII. — <i>Court propos sur les différents systèmes et sur leur emploi</i>	274
117. — Généralités.....	274
118. — Différentes communications destinées à être chiffrées et caractéristiques des chiffres respectifs.....	274
119. — Moyens de chiffrement pour les communications politico-militaires.....	275
120. — Moyens de chiffrement pour les communications militaires des grandes unités.....	276
121. — Moyens de chiffrement pour les communications militaires des petites unités (inférieures à la Division).....	277
122. — Règles générales pour l'emploi du chiffre et pour les correspondances à chiffrer.....	278
123. — Règles pour l'utilisation des moyens de chiffrement.....	279
124. — La distribution des clefs pour les machines à chiffrer.....	280

QUATRIÈME PARTIE

AUTRES CORRESPONDANCES SECRÈTES

CHAP. XXIII. — <i>Correspondances dissimulées, conventionnelles et invisibles</i>	282
125. — Généralités.....	282
126. — Systèmes télégraphiques conventionnels.....	282
127. — Systèmes épistolaires dissimulés.....	283
128. — Encres sympathiques.....	286

CINQUIÈME PARTIE

NOTE HISTORIQUE

CHAP. XXIV. — <i>Les chiffres diplomatiques et militaires</i>	287
CHAP. XXV. — <i>La littérature cryptographique</i>	295
CHAP. XXVI. — <i>Les décrypteurs célèbres et les Bureaux de décryptement</i>	310

APPENDICE

I. — Sur les équations cryptographiques.....	316
A) Règles et cercles chiffnants (N. 1 à 16)..	316
B) Tambours chiffnants (N. 17 à 24).....	331
C) L'autochiffrement totalisateur (N. 25 à 30).....	339
D) Sur le chiffrement algébrique et polynomique (N. 31 à 40).....	343
II. — Présences. Moyenne fréquence quadratique. Alphabets réciproques.....	353
41. — Présences.....	353
42. — Moyenne fréquence quadratique.....	354
43. — Calcul du nombre possible d'alphabets réciproques.....	355

BIBLIOGRAPHIE

I. — Liste des ouvrages.....	357
II. — Liste des codes télégraphiques les plus connus.....	371
INDEX ALPHABÉTIQUE.....	373

TABLES

N. 1 - 2 - 3 - 4	Langue française.
N. 5 - 6 - 7 - 8	— italienne.
N. 9 - 10 - 11 - 12	— espagnole.
N. 13 - 14 - 15 - 16	— allemande.
N. 17 - 18 - 19 - 20	— anglaise.
N. 21 - 22 - 23 - 24	— serbo-croate.
N. 25 - 26	— russe.
N. 27	Graphique des fréquences littérales pour les langues : latine, portugaise, hollandaise.
N. 28	Graphique des présences et des moyennes fréquences quadratiques pour 7 langues.