

Table des Matières

	PAGES
Introduction	
CHAPITRE PREMIER. — Généralités et terminologie :	
1. — Les deux parties de la cryptographie	7
2. — Généralités sur le chiffrement	8
3. — Classification des méthodes et procédés de chiffrement	9
4. — Systèmes de chiffrement	10
5. — Règles générales de la science du chiffre	10
6. — Généralités sur le décryptement	12
7. — Cas où le problème du décryptement est entier. Capacité de chiffrement parfait	13
8. — Circonstances pouvant faciliter le décryptement	13
9. — Renseignements sur les libellés. Chiffrement parfait apparent et chiffrement parfait réel	14
10. — Renseignements sur le mode de chiffrement	15
11. — Fautes systématiques de chiffrement	16
12. — Importance de la théorie et conclusion	17
 CHAPITRE II. — Caractéristiques de la langue française :	
13. — Caractéristiques d'une langue. Définition de la fréquence ..	19
14. — Fréquences des lettres en français	20
15. — Caractéristiques des lettres déduites de la fréquence de certains bigrammes	20
16. — Tableau de fréquences des redoublements	21
17. — Autres bigrammes caractéristiques de certaines lettres	21
18. — Fréquences des bigrammes	22
19. — Fréquences des trigrammes	23
20. — Fréquences des mots. Dernières considérations	23
PREMIERE PARTIE	
Transpositions pures	
CHAPITRE PREMIER. — Etude générale des transpositions pures :	
1. — Ancienneté des méthodes de transposition. Leurs définitions ..	27
2. — Caractéristique générale des transpositions pures	27
3. — Suite cryptographique et suite de l'anagramme	28
4. — Méthode générale de décryptement des transpositions	28
5. — Exemple de décryptement par la méthode générale	30
6. — Cas de deux cryptogrammes de même longueur et de même clef	32
7. — Méthode générale par l'emploi de mots probables	33
8. — Autres généralités sur les transpositions	34
9. — Accidents et fautes de chiffrement	35
10. — Capacité de chiffrement parfait des transpositions. Valeur cryptographique de cette catégorie de procédés	36

CHAPITRE II. — **Transposition simple ordinaire à tableau :**

PAGES

11. — Clef de transposition	39
12. — Chiffrement et déchiffrement	39
13. — Remarque sur la disposition de la clef	40
14. — Etude de la suite XP	40
15. — Décryptement	41
16. — Cas d'un tableau complet	41
17. — Méthode du chapeau. Cas d'un tableau presque complet	42
18. — Exemple de décryptement d'un tableau presque complet ..	43
19. — Cas général d'un tableau absolument quelconque	44
20. — Exemple de décryptement analytique	45
21. — Suite du décryptement analytique	46
22. — Exemple de décryptement à l'aide d'un mot probable	48
23. — Autres méthodes d'utilisation d'un mot probable	49
24. — Méthodes empiriques	50
25. — Cas particuliers. Accidents de chiffrement	50
26. — Exemples de décryptement d'après divers accidents de chiffrement :	
a) Les deux clefs sont différentes et n'ont pas la même longueur	51
b) Les deux clefs sont différentes, mais elles ont la même longueur	52
c) Les deux messages ont été chiffrés avec la même clef ..	53
27. — Reconstitution d'une clef claire littérale	54
28. — Remarque sur la possibilité théorique d'utiliser le numérotage de la clef pour aider le décryptement	54
29. — Intérêt pratique de l'étude des transpositions simples	55

CHAPITRE III. — **Transpositions simples améliorées :**

30. — Amélioration possible de la transposition simple ordinaire ..	57
31. — Relevé alternatif des colonnes de haut en bas et de bas en haut	57
32. — Prélèvement en diagonales	57
33. — Tableaux pleins irréguliers	58
34. — Transpositions simples à tableau améliorées par des trous ..	59
35. — Diverses solutions possibles	59
36. — Décryptement des transpositions simples améliorées	61
37. — Transposition double	62
38. — Utilisation d'un texte clef. Tableaux à cases numérotées ..	63
39. — Suites cryptographiques fragmentées	63
40. — Autres procédés de transposition simple. Variante de RICHELIEU. Méthode du Colonel ROCHE	64
41. — Procédé de PORTA	65

CHAPITRE IV. — **Transposition simple par grille :**

42. — Définition de la grille	67
43. — Divers types de grilles	67
44. — Grilles tournantes carrées. Modes classiques d'utilisation (à carrés complets)	68
45. — Décryptement des grilles employées à carrés complets ..	69
46. — Exemples de décryptement	69
47. — Modes d'emploi rationnel des grilles tournantes	71
48. — Avantages comparés de chacun des deux modes d'emploi ..	72
49. — Usage d'une contre-grille	73
50. — Sécurité cryptographique finalement obtenue	73
51. — Mode de formation et nombre de grilles tournantes carrées ..	74
52. — Autres sortes de grilles à fenêtres carrées	74
53. — Grilles indéfinies	74

CHAPITRE V. — **Double transposition :**

	PAGES
54. — Définition et catégories diverses	77
55. — Différents cas de double transposition faite par deux tableaux complets. 1 ^{er} cas : p_1 est un multiple de n_2	78
56. — 2 ^e cas : p_1 est un sous-multiple de n_2	79
57. — 3 ^e cas général : p_1 sur n_2 est égal à a sur b	79
58. — Principe du décryptement	80
59. — Exemple de décryptement	82
60. — Cas particulier de deux transpositions simples successives faites avec la même clef	84
61. — Cas de tableaux incomplets. Capacité de chiffrement parfait réel	84
62. — Autres possibilités de décryptement : Accidents et fautes de chiffrement	86
63. — Reconstitution des clefs numériques d'après une suite XP ..	86
64. — Exemple de reconstitution de clefs numériques	87
65. — Cas général de deux transpositions quelconques	88
66. — Conclusions sur la double transposition et sur la transposition en général	88

DEUXIEME PARTIE

Substitutions puresCHAPITRE PREMIER. — **Définition des clefs de substitution. Alphabets de substitution :**

1. — Ancienneté des procédés de substitution	93
2. — Clefs de substitution. Définition d'une clef simple	93
3. — Valeur cryptographique d'une clef simple	94
4. — Commodité d'emploi des clefs simples. Importance fondamentale des clefs simples littérales	94
5. — Substitutions inverses. Alphabets inverses. Alphabets réciproques	95
6. — Familles d'alphabets. Alphabets classiques normalement ordonnés	96
7. — Alphabets complémentaires. Substitution complémentaire ..	97
8. — Alphabets normalement parallèles. Alphabets non normalement parallèles. Alphabets non-parallèles	97
9. — Alphabets inverses d'une famille d'alphabets parallèles	98
10. — Alphabets semi-ordonnés. Alphabets intervertis. Alphabets chevauchants	98
11. — Mode de formation des alphabets chevauchants à partir d'un alphabet origine	99
12. — Alphabets désordonnés incohérents	100
13. — Modes de formation simple et classique d'après un mot-clef ..	100
14. — Critiques déjà formulées et autres modes de formation proposés par divers auteurs	101
15. — Autres types de clefs simples. Carré de chiffrement (<i>de 25</i>) ..	103
16. — Substitution à double clef. Définition	104
17. — Classification des substitutions pures	104

CHAPITRE II. — **Substitutions simples ordinaires :**

18. — Caractéristiques des substitutions simples ordinaires	107
19. — Substitutions simples classiques (par alphabets normalement ordonnés)	108

	PAGES
20. — Décryptement des substitutions simples ordinaires	108
21. — Exemple de décryptement par la méthode analytique	110
22. — Décryptement par la méthode du mot probable	111
23. — Valeur d'un mot probable en substitution simple ordinaire. Capacité de chiffrement parfait réel	112
24. — Exemple de reconstitution d'un alphabet de substitution établi selon le mode de formation classique	112
25. — Méthode de décryptement par la recherche du mot-clef	113
26. — Utilisation pratique des suites numériques d'étude	115
27. — Exemple de décryptement par la méthode du mot-clef	117
28. — Décryptement des substitutions simples ordinaires d'un autre type	118
29. — Derniers types de substitutions simples ordinaires. Substitu- tion économique de DELASTELLE. Méthode générale de décryp- tement	120
 CHAPITRE III. — Substitutions simples à représentations multiples :	
30. — Généralités sur les substitutions simples littérales à représen- tations multiples	121
31. — Deux catégories de substitutions simples à représentations multiples	121
32. — Utilisation d'un carré de chiffrement	122
33. — Critique de ces procédés	123
34. — Autres procédés de substitution à représentations multiples	123
35. — Autres inconvénients des substitutions simples à représenta- tions multiples	124
 CHAPITRE IV. — Substitutions simples par bigrammes :	
36. — Généralités sur les substitutions simples par bigrammes	127
37. — Equivalence avec deux substitutions simples littérales	127
38. — Exemples de fautes systématiques de chiffrement	128
39. — Procédés de substitution bigrammatique utilisés dans la pra- tique	129
a) Emploi de listes ou de tableaux	129
b) Damiers bigrammatiques de DELASTELLE	129
c) Procédé Playfair	129
40. — Décryptement. Cas du Playfair	130
41. — Possibilités de décryptement par un mot probable ou par le mot-clef du carré de chiffrement	131
42. — Exemple de décryptement	132
43. — Décryptement dans le cas général	135
44. — Substitution bigrammatique par alphabets bifides de DELAS- TELLE	135
45. — Substitutions par polygrammes. Alphabets trifides. Conclu- sion	136
 CHAPITRE V. — Généralités au sujet de la substitution à double clef. Définition. Origines historiques.	
46. — Définition de la véritable substitution à double clef	139
47. — VIGENÈRE, inventeur de la substitution à double clef	140
48. — Les précurseurs de VIGENÈRE :	
a) TRITHÈME	140
b) Gabriel DE COLLANGE	141
49. — BELLASO	142
50. — PORTA	142
51. — VIGENÈRE	143

	PAGES
52. — Derniers perfectionnements apportés à la substitution à double clef	143
a) Variétés classiques (par alphabets normalement ordonnés)	143
b) Variétés employant des alphabets secrets désordonnés	144
53. — Caractéristiques générales des substitutions à double clef ...	144
54. — Méthode générale de décryptement	145
 CHAPITRE VI. — Substitutions à double clef classiques. Généralités :	
55. — Définition des substitutions à double clef classiques	147
56. — Variantes de principe :	148
a) Mode de chiffrement selon VIGENÈRE	148
b) Variante de BEAUFORT	148
c) Variante ALLEMANDE	148
57. — Equations de chiffrement	149
58. — Autres formes du tableau classique :	
a) Tableau à alphabets décalés de gauche à droite	151
b) Tableau à alphabets ordonnés en sens opposé	152
59. — Deuxième variante de chiffrement à l'allemande	152
60. — Usage d'un décalage constant supplémentaire	153
61. — Réglettes classiques de dimension réduite	154
 CHAPITRE VII. — Substitutions à double clef classiques. Variantes de Porta et de Gronsfeld :	
62. — Variante de PORTA	155
63. — Exemple de décryptement par la méthode analytique	156
64. — Décryptement par la méthode du mot probable	157
65. — Tableaux de recherche de mots probables et du mot-clef ...	159
66. — Autre méthode du mot probable	160
67. — Variante de GRONSFELD	161
 CHAPITRE VIII. — Autres variantes d'application de la clef :	
68. — Changement de clef en cours de chiffrement	163
69. — Emploi de lettres nulles	163
70. — Procédé de la clef interrompue :	
a) Usage d'une lettre d'arrêt	164
b) Usage d'une convention supplémentaire	164
71. — Clef apériodisée par des trous	165
72. — Clef claire indéfinie	165
73. — Chiffrements autoclaves	166
74. — Méthode de décryptement du Commandant BASSIÈRES ...	166
75. — Retour à une clef périodique ordinaire	167
76. — Autoclaves ayant pour clef le texte cryptographique. Procédés autochiffants	168
77. — Clef principale cyclique. Cadrons	169
78. — Décryptement par la méthode du Commandant BASSIÈRES ..	169
79. — Variantes de haute sécurité. Variante du Général SACCO ...	171
80. — Variante de ROZIER	171
 CHAPITRE IX. — Autres variétés de substitutions à double clef. Généralités sur le décryptement des substitutions à double clef par alphabets désordonnés :	
81. — Chiffrement par tranches. Cryptographe d'ALBERTI	175
82. — Instruments de chiffrement par alphabets normalement parallèles	176

	PAGES
83. — Instruments de chiffrement par alphabets non normalement parallèles	177
84. — Commodité d'emploi. Tableaux inverses. Tableau réversible de DELASTELLE	178
85. — Réglettes inverses établies à l'aide d'alphabets chevauchants ..	179
86. — Alphabets réellement non-parallèles	179
87. — Usage d'alphabets indépendants	180
88. — Généralités sur le décryptement des substitutions à double clef par alphabets secrets désordonnés	181
CHAPITRE X. — Décryptement des substitutions à double clef par alphabets secrets désordonnés :	
89. — Cas des alphabets normalement parallèles. Principe général d'étude	185
90. — Exemple de décryptement dans le cas d'une clef périodique ordinaire	185
91. — Détermination de la longueur de la clef périodique. Fréquences	186
92. — Utilisation d'un mot probable	187
93. — Utilisation du parallélisme normal et du mot-clef-principale ..	187
94. — Fin du décryptement par la recherche du mot-clef de l'alphabet secret du coulisseau	188
95. — Utilisation des suites numériques d'étude	188
96. — Cas des autres variantes d'application de la clef. Cadrons à un alphabet secret. Autoclaves	189
97. — Cas des alphabets non normalement parallèles. Utilisation du parallélisme vertical	191
98. — Exemple d'utilisation du parallélisme horizontal dans un cas particulier	192
a) Détermination de la longueur de la clef principale	193
b) Réglette fictive d'étude	193
c) Utilisation du mot probable	194
99. — Reconstitution d'un instrument de chiffrement grâce au parallélisme non normal	195
100. — Exemple concret d'une telle reconstitution	196
101. — Cas d'un instrument de chiffrement connu	197
102. — Cas d'alphabets indépendants	198
CHAPITRE XI. — Cryptographes et machines à chiffrer :	
103. — Appareils divers. Cryptographe de WHEATSTONE	201
104. — Cryptographe de BAZERIES	202
105. — Cryptographe de DUCROS	204
106. — Cryptographes à barrettes verticales mobiles	205
107. — Cryptographe portatif et machines à chiffrer HAGELIN	207
108. — Machine allemande ENIGMA. Modèle théorique décrit par GIVIERGE	209
109. — Véritable réalisation de l'ENIGMA	212
110. — Machines tomogrammiques : Modèle HAGELIN à deux voies ..	213
111. — Téléimprimeurs chiffants à cinq moments	214
112. — Réalisations du premier type	215
113. — Téléimprimeur chiffant de SIEMENS	216
114. — Autres machines à chiffrer	217
115. — Conclusions sur les substitutions pures et sur les machines à chiffrer	218

TROISIEME PARTIE

PAGES

**Méthodes combinées — Méthodes codiques
Moyens auxiliaires de chiffrement**

Note préliminaire à la troisième partie	222
CHAPITRE PREMIER. — Substitution simple et transposition :	
1. — Diverses catégories de méthodes combinées	223
A. — Méthodes combinées ordinaires	
2. — Substitution simple et transposition	224
3. — Transposition et substitution à double clef.	
a) Transposition et substitution à double clef	224
b) Substitution à double clef et transposition	225
4. — Exposé d'une méthode particulière de décryptement (M. PAINVIN)	225
5. — Cas général. Choix rationnel de telles combinaisons	226
B. — Méthodes tomogrammiques	
6. — Substitution simple de lettres en bigrammes et transposition .	228
7. — Exemple historique de décryptement	229
8. — Autres méthodes tomogrammiques	234
C. — Méthodes complexes	
9. — Procédés complexes de DELASTELLE	235
10. — Substitutions migrammatiques	236
11. — Autres procédés complexes	238
12. — Principe du décryptement des méthodes complexes	239
CHAPITRE II. — Substitutions codiques :	
A. — Chiffrement simple	
13. — A. Chiffrement simple. Documents codiques divers	241
14. — Capacité théorique et richesse effective d'un code	242
15. — Fonction cryptographique et fonction abrégative des codes ..	243
16. — Influence d'autres caractéristiques de composition et de l'habileté des chiffreurs sur la valeur d'un code	244
17. — Décryptement dans le cas général	244
18. — Groupes de syllabage, groupes caractéristiques	246
19. — Conseils généraux et fin du décryptement	246
20. — Capacité de chiffrement parfait des substitutions codiques non surchiffrées	247
21. — Cas particuliers : Dictionnaires ordonnés ou semi-ordonnés. Dictionnaires à pagination variable	248
22. — Conclusions au sujet des substitutions codiques non surchiffrées	249
B. — Surchiffrement des dictionnaires	
23. — Qualités souhaitables pour un procédé de surchiffrement ...	249
24. — Valeur cryptographique d'un code surchiffré	249
25. — Surchiffrement par transposition	251
26. — Surchiffrement par substitution bigrammatique	253
27. — Surchiffrement par clef additive ou soustractive	254
28. — Principe du décryptement	255
29. — Décryptement dans le cas général	256
30. — Cas d'un code connu. Dernières considérations	258

	PAGES
CHAPITRE III. — Moyens auxiliaires de chiffrement. Jugement final :	
31. — Diverses sortes de moyens auxiliaires de chiffrement	261
32. — Numéros d'ordre secrets. Marquants	262
33. — Moyens auxiliaires de chiffrement et de décryptement fournis par les mathématiques	264
34. — Valeur « mathématique » d'un procédé de chiffrement ou d'une machine à chiffrer	266
35. — Qualités nécessaires aux cryptologues	268
36. — Analyse cryptographique	270
37. — Jugement final sur la cryptographie	271
ANNEXE N° 1. — Petit formulaire de calcul des probabilités :	
A. — Formule d'analyse combinatoire :	
1. — Permutations	277
2. — Permutations avec répétitions	277
3. — Arrangements	277
4. — Arrangements avec répétitions	277
5. — Combinaisons	278
6. — Combinaisons avec répétitions	278
7. — Formule de STIRLING	278
B. — Éléments de la théorie des probabilités :	
1. — Définition d'une probabilité	279
2. — Probabilité unitaire, ou probabilité élémentaire d'une seule épreuve	279
3. — Théorème des probabilités composées	279
4. — Théorème des probabilités totales	280
5. — Cas d'événements qui ne s'excluent pas mutuellement	280
6. — Espérance mathématique	280
7. — Triangle de PASCAL. Cas du jeu de pile ou face	281
8. — Formule de l'alternative généralisée	281
9. — Formule de l'alternative simple (dite formule générale)	282
10. — Probabilité maximum, Loi des grands nombres. Théorème de BERNOULLI. Loi de GAUSS-LAPLACE	282
11. — Conditions d'application	283
12. — Loi des petites probabilités due à POISSON	284
13. — Probabilité des causes, formule de BAYES	284
C. — Exemples simples d'application du calcul des probabilités en cryptographie :	
1. — Utilité de tels calculs. Leur valeur et leur précision	286
2. — Probabilités unitaires en cryptographie	286
3. — Cas des unités de chiffrement	287
4. — Cas des groupes codiques	288
5. — Problème des répétitions	289
6. — Formule de NEWTON	291
7. — Première application pratique : Cas où la loi des grands nombres est applicable	292
8. — Second problème pratique : Probabilité d'un nombre donné de e dans un texte clair	293
9. — Troisième problème pratique : Probabilité pour que le e soit la lettre la plus fréquente	295
10. — Probabilité des fréquences d'une transposition	296
11. — Probabilité des fréquences d'une substitution simple	297
12. — Cas des substitutions à double clef	299
13. — Problème spécial : Etude de la valeur d'un critérium	300
14. — Cas des codes. Conclusions	301

ANNEXE N° 2. — **Une théorie mathématique des systèmes de chiffrement (Shannon).**

1. — Références et limites de la présente étude	303
2. — Bases générales des théories de SHANNON	304
3. — Structure mathématique d'une source d'information. Entropie. Redondance. Equivoque	305
4. — Théorie des télécommunications	306
5. — L'algèbre des systèmes de chiffrement	307
6. — Secret théorique. Secret pratique. Discussion	308
7. — Conditions mathématiques du secret parfait	309
8. — Equivoque dans le cas général. Systèmes idéaux	310
9. — Caractéristique de labeur et secret pratique. Conclusions ...	312
 ANNEXE N° 3. — Caractéristiques statistiques de la langue russe ..	313
 ANNEXE N° 4. — Caractéristiques statistiques de la langue allemande	319
 ANNEXE N° 5. — Caractéristiques statistiques de la langue anglaise.	321
 ANNEXE N° 6. — Caractéristiques statistiques de la langue espagnole	323
 ANNEXE N° 7. — Caractéristiques statistiques de la langue italienne .	325
 Tableau des fréquences des bigrammes en français : Hors-texte <i>in fine.</i>	327
 Tableau des fréquences des bigrammes en russe : Hors-texte <i>in fine.</i>	329