



## Éléments de cryptographie Par Daniel TANT

Editeur : A. Pédone à Paris

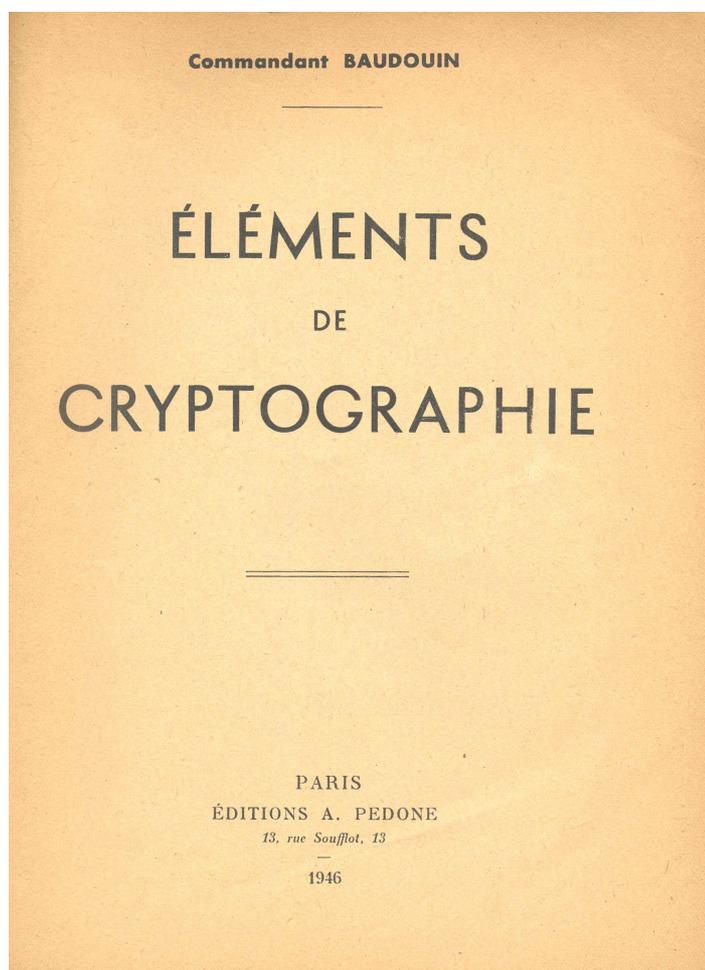
Auteur : commandant Baudouin

Date : 1946 (réédition de 1939)

Edité après la Seconde guerre mondiale, le papier est de mauvaise qualité, ce qui est regrettable car ce livre contient la formation de base mais aussi le perfectionnement du chiffreur aux méthodes classiques.

Non seulement c'est par une méthode simple et claire que l'on apprend les principes de la cryptographie manuelle (avant les machines à rotors) mais chaque chapitre est complété par une méthode de décryptement pour obtenir le message en clair sans connaître les codes.

Il est complété par 5 tableaux donnant les fréquences des bigrammes.



## TABLE DES MATIÈRES

### PREMIÈRE PARTIE. — GÉNÉRALITÉS

	Pages
Chap. I. — <b>Généralités sur le chiffre.</b> Le Chiffre. Définitions. Procédés de chiffrement. Conventions de chiffrement. . . . .	13
Chap. II. — <b>La Cryptographie.</b> Définitions. Qualités nécessaires au cryptologue. Méthodes de décryptement. Notion de fréquence. Notion de mot probable. Caractéristiques de la langue française. . . . .	22

### DEUXIÈME PARTIE. — PROCÉDÉS DE SUBSTITUTION

Chap. III. — <b>Substitution simple à représentation unique lettre à lettre.</b> Exposé du procédé. Alphabets de substitution. Emploi d'une clef pour établir un alphabet de chiffrement. Caractères analytiques de la substitution simple. Décryptement des substitutions simples (méthode analytique, méthode du mot probable). . . . .	39
Chap. IV. — <b>Substitution par bigrammes.</b> Exposé du procédé. Tableaux de bigrammes. Substitution orthogonale et diagonale par bigrammes système Playfair. Décryptement des substitutions par bigrammes. Etude de la substitution par bigrammes système Playfair (caractéristiques du procédé, méthode de décryptement, exemples, recherche de la clef). . . . .	54
Chap. V. — <b>Répertoires, codes et dictionnaires.</b> Généralités. Décryptement des répertoires et codes ordonnés. Cas des répertoires et codes désordonnés. Démarquage d'un code. . . . .	82
Chap. VI. — <b>Substitution simple à représentations multiples.</b> Exposé du procédé (alphabet réduit, carré de 25, appareil à bande, tableau de cent cases, emploi d'un livre ou d'un texte imprimé). Méthode de décryptement des substitutions simples à représentations multiples (Exemples. Cas de l'appareil à bande. Reconstitution de l'appareil). . . . .	100
Chap. VII. — <b>Substitutions à double clef à alphabets normalement ordonnés du type Vigenère.</b> Principe et caractéristiques du procédé. Procédé Gronsfeld. Procédé Vigenère. Carré de Vigenère. Emploi d'une réglette ou d'un cadran. Interprétation algébrique du système Vigenère. Procédé Beaufort. Décryptement des substitutions doubles à alphabets normalement ordonnés. Exemples de décryptement (méthode analytique, méthode du mot probable). Cas particuliers (clef très longue, absence de répétitions). Procédés dérivés du système Vigenère. Variante de Rozier. . . . .	122
Chap. VIII. — <b>Substitutions à double clef du type autoclave.</b> — Exposé du procédé. Décryptement des systèmes autoclaves. Cas où le texte clair sert de clef autoclave. Cas où le cryptogramme sert de clef autoclave. Exemples de décryptement. Cas du chiffrement en Beaufort. . . . .	150

Chap. IX. — <b>Substitutions à double clef à alphabets incohérents et parallèles</b> — Exposé du procédé. Réglettes. Méthode de décryptement. Symétrie de position. Exemples de décryptement. Autre mode d'emploi de la réglette. Cas du mot probable. . . . .	164
Chap. X. — <b>Substitutions à double clef à alphabets incohérents et non parallèles</b> . — Principe du procédé. Emploi d'une réglette. Appareils à réglettes verticales mobiles. Exemple de décryptement. Carré de Vigenère à alphabets incohérents et non parallèles. . . . .	181
APPENDICE. — Alphabets chevauchants. Propriété fondamentale des alphabets chevauchants. . . . .	198

## TROISIÈME PARTIE. — PROCÉDÉS DE TRANSPOSITION

Chap. XI. — <b>Transposition simple à tableau</b> . — Exposé du procédé. Tableau complet. Tableau incomplet. Eléments du tableau. Notion de suite des nombres. Suite de l'anagramme. Suite XP. Notion de coupure. Décryptement des transpositions simples. Cas du tableau complet. Cas où l'on dispose de plusieurs télégrammes de même longueur. Cas où la longueur de la clef est connue. Cas du mot probable. Cas de plusieurs télégrammes ayant une partie commune. Cas général. . . . .	207
Chap. XII. — <b>Transpositions par grille</b> . — Généralités. <i>Grilles du type ordinaire</i> . Grilles tournantes. <i>Grilles tournantes carrées</i> (Grille paire et impaire, loi des positions conjuguées, suite des nombres). Méthode de décryptement. Propriétés géométriques des grilles tournantes carrées. Nombre de grilles tournantes différentes qu'il est possible de construire dans un carré de côté $n$ . <i>Grilles tournantes circulaires</i> . Etude du procédé. Exemple de décryptement. Systèmes complexes. Grilles circulaires à hélice. Formes possibles. Exemple de décryptement. . . . .	236
Chap. XIII. — <b>Procédés de transposition dérivés du système des grilles</b> . — <i>Tableau à cases numérotées</i> . Etude du procédé. Exemple de décryptement. <i>Transposition par clef texté</i> . Etude du procédé. Exemple de décryptement. . . . .	274

## QUATRIÈME PARTIE. — ANALYSE CRYPTOGRAPHIQUE

Chap. XIV. — <b>Essai d'analyse cryptographique</b> . — Position du problème. Comment, à partir de l'étude analytique du cryptogramme, préciser le procédé de chiffrement utilisé. Examen préalable. Notion d'unité chiffrante. Tables analytiques. . . . .	291
Chap. XV. — <b>Matériaux de base</b> . — Langues française, allemande, anglaise, espagnole, italienne. Fréquences individuelles de lettres. Bigrammes de lettres les plus fréquents. Tableaux de fréquence des bigrammes. Classification des bigrammes. Trigrammes de lettres les plus fréquents. Rappel de quelques notions simples d'analyse combinatoire. . . . .	314