Introduction

Chapter I — Generalities and Terminology

1. The two parts of cryptography
2. Generalities on encipherment
3. Classification of encipherment methods and processes
4. Encipherment systems
5. General rules of the science of ciphering
6. Generalities on cryptanalysis
7. Cases where the problem of decipherment is complete. Perfect encipherment capacity
8. Circumstances capable of facilitating decipherment
9. Information from indicators. Apparent perfect encipherment and real perfect encipherment
10. Information on the mode of encipherment
11. Systematic faults of encipherment
12. Importance of theory and conclusion

Chapter II — Characteristics of the French Language

13. Characteristics of a language. Definition of frequency
14. Frequencies of letters in French
15. Characteristics of letters deduced from the frequency of certain bigrams
16. Table of frequencies of doubled letters
17. Other bigrams characteristic of certain letters
18. Frequencies of bigrams
19. Frequencies of trigrams
20. Frequencies of words. Final considerations

Part One

Pure Transpositions

Chapter I — General Study of Pure Transpositions

1. Antiquity of transposition methods. Their definitions
2. General characteristic of pure transpositions
3. Cryptographic sequence and sequel of the anagram
4. General method for cryptanalysis of transpositions
5. Example of cryptanalysis by the general method
6. Case of two cryptograms of the same length and of the same key
7. General method using probable words
8. Other generalities on transpositions
9. Accidents and faults of encipherment
10. Perfect encipherment capacity of transpositions. Cryptographic value of this category of processes

Chapter II — Ordinary Simple Table Transposition

11. Transposition key
12. Encipherment and decipherment
13. Remark on the arrangement of the key
14. Study of the XP sequence
15. Cryptanalysis
16. Case of a complete table
17. Hat method. Case of an almost complete table
18. Example of cryptanalysis of an almost complete table
19. General case of an absolutely arbitrary table
20. Example of analytic cryptanalysis
21. Continuation of analytic decipherment
22. Example of cryptanalysis using a probable word
23. Other methods of using a probable word
24. Empirical methods
25. Particular cases. Encipherment accidents
26. Examples of cryptanalysis according to various encipherment accidents
    a) The two keys are different and do not have the same length
    b) The two keys are different, but they have the same length
    c) The two messages were enciphered with the same key
27. — Reconstruction of a literal plaintext key
28. — Remark on the theoretical possibility of using the numbering of the key to aid decipherment
29. — Practical interest of the study of simple transpositions

Chapter III — Improved Simple Transpositions

30. Possible improvement of ordinary simple transposition
31. Alternate reading of columns from top to bottom and from bottom to top
32. Diagonal extraction
33. Irregular filled tables
34. Simple table transpositions improved by holes
35. Various possible solutions
36. Decipherment of improved simple transpositions
37. Double transposition
38. Use of a key text. Tables with numbered cells
39. Fragmented cryptographic sequences
40. Other simple transposition processes. Richelieu variant. Colonel Roche method
41. Porta process

Chapter IV — Simple Grille Transposition

42. Definition of the grille
43. Various types of grilles
44. Square turning grilles. Classical modes of use (with complete squares)
45. Cryptanalysis of grilles used with complete squares
46. Examples of cryptanalysis
47. Modes of rational use of turning grilles
48. Comparative advantages of each of the two modes of use

Chapter V. Double trasposition.

PART TWO

Pure Substitutions

Chapter I — Definition of substitution keys. Substitution alphabets

Chapter II — Ordinary simple substitutions

18. Characteristics of ordinary simple substitutions
19. Classical simple substitutions (by normally ordered alphabets)
20. Cryptanalysis of ordinary simple substitutions.
21. Example of decryption by the analytical method
22. Decryption by the probable word method
23. Value of a probable word in ordinary simple substitution. Real perfect encryption capability
24. Example of reconstruction of a substitution alphabet established according to the classical formation method
25. Cryptanalysis method by keyword search
26. Practical use of study numerical sequences.
27. Example of cryptanalysis by the keyword method.
28. Cryptanalysis of ordinary simple substitutions of another type.
29. Last types of ordinary simple substitutions.
30. Delastelle's economical substitution. General cryptanalysis method.

CHAPTER III. - Simple Substitutions with Multiple Representations:

31. Generalities on Simple Literal Substitutions with Multiple Representations.
32. Two Categories of Simple Substitutions with Multiple Representations.
33. Use of a Cipher Square .
34. Critique of These Methods .
35. Other Methods of Substitution with Multiple Representations
36. Other Drawbacks of Simple Substitutions with Multiple Representations .

CHAPTER IV. - Simple Substitutions with Bigrams:

37. Generalities on Simple Substitutions with Bigrams
38. Equivalence with Two Simple Literal Substitutions
39. Examples of systematic encryption errors
40. Bigrammatic substitution methods used in practice
    1. Use of lists or tables
    2. Delastelle's bigrammatic checkerboards
    3. Playfair method
41. Cryptanalysis. The Playfair case .
42. Cryptanalysis possibilities using a probable word or the keyword of the cipher square
43. Example of cryptanalysis
44. Cryptanalysis in the general case.
45. Bigrammatic substitution using Delastelle's bifid alphabets
46. Substitutions using polygrams. Trifid alphabets. Conclusion

CHAPTER V. - Generalities on double-key encryption. Definition. Historical Origins.

47. - Definition of the true double key substitution
48. Vigenère, inventor of double key substitution
49. The precursors of Vigenère:
    1. Tritheme.
    2. Gabriel DE Collange.
50. Bellaso
51. Porta

52. Vigenère
53. Latest improvements to double-key substitution:
    1. Classical variations
    2. Varieties employing disordered secret alphabets.
54. General characteristics of double-key substitutions
55. General cryptanalysis method.

CHAPTER VI. - Double-key substitutions a. Generalities:

56. Definition of classical double-key substitutions
57. Variants in principle
    1. Vigenère cipher
    2. Beaufort variant.
    3. German variant
58. Encryption equations
59. Other forms of the classical tableau:
    1. Tableau with alphabets shifted from left to right
    2. Tableau with alphabets ordered in opposite directions
60. Second variant of the German cipher
61. Use of an additional constant offset
62. Classic, smaller-sized rulers

CHAPTER VII. - Substitution with a double key. Variant of Porta and Gronsfeld.

63. Porta variant
64. Example of decryption using the analytical method
65. Decryption using the probable word method
66. Probable word and keyword search tables
67. Another probable word method
68. Gronsfeld variant

CHAPTER VIII. - Another variant of key application.

69. Key change during encryption
70. Use of null letters
71. Interrupted key method:
    1. Use of a stop letter
    2. Use of an additional convention
72. Key deperiodized by holes
73. Indefinite plain key
74. Autokey ciphers
75. Commander Bassières' decryption method
76. Return to an ordinary periodic key
77. Autokeys with the cryptographic text as the key. Self-encrypting methods
78. Cyclic master key. Discs,
79. Cryptanalysis by Commander Bassières' method
80. High-security variants. General SACCO's Variant
81. Rozier's Variant

CHAPTER IX. - Other varieties of double-key encryption. General information on the decryption of double-key encryption using unordered alphabets:

Chapter X — Decipherment of Double-Key Substitutions by Disordered Secret Alphabets

Chapter XI — Cryptographs and Cipher Machines

PART THREE

Combined Methods — Code Methods

Auxiliary Means of Encipherment

Preliminary note to the third part

Chapter I — Simple substitution and transposition

1. Various categories of combined methods

A. Ordinary combined methods

2. Simple substitution and transposition
3. Transposition and substitution with a double key
   a) Transposition and substitution with a double key
   b) Double-key substitution and transposition
4. Presentation of a particular method of decipherment (M. Painvin)
5. General case. Rational choice of such combinations

B. Tomographic methods

6. Simple substitution of letters into bigrams and transposition
7. Historical example of decipherment
8. Other tomographic methods

C. Complex methods

9. Complex procedures of Delastelle
10. Migrammatic substitutions
11. Other complex procedures
12. Principle of the decipherment of complex methods

Chapter II — Code substitutions

A. Simple encipherment

13. Simple encipherment. Various code documents
14. Theoretical capacity and effective richness of a code
15. Cryptographic function and abbreviated function of codes

16. Influence of other characteristics of composition and of the habits of encipherers on the value of a code
17. Cryptanalysis in the general case
18. Syllabication groups, characteristic groups
19. General advice and purpose of cryptanalysis
20. Perfect encipherment capacity of non-superenciphered code substitutions
21. Particular cases. Ordered or semi-ordered dictionaries. Dictionaries with variable pagination
22. Conclusions concerning non-superenciphered code substitutions

B. Superencipherment of dictionaries

23. Desirable qualities for a superencipherment procedure
24. Cryptographic value of a superenciphered code
25. Superencipherment by transposition
26. Superencipherment by bigrammatic substitution
27. Superencipherment by additive or subtractive key
28. Principle of cryptanalysis
29. Cryptanalysis in the general case
30. Case of a known code. Final considerations

Chapter III — Auxiliary Means of Encipherment. Final Judgment

31. Various kinds of auxiliary means of encipherment
32. Secret serial numbers. Indicators
33. Auxiliary means of encipherment and decipherment supplied by mathematics
34. “Mathematical” value of an encipherment procedure or of a cipher machine
35. Qualities necessary for cryptologists
36. Cryptographic analysis
37. Final judgment on cryptography

Appendix No. 1 — Small Handbook of Probability Calculations

A. Formulae of combinatorial analysis

1. Permutations
2. Permutations with repetitions
3. Arrangements
4. Arrangements with repetitions
5. Combinations
6. Combinations with repetitions
7. Stirling’s formula

B. Elements of probability theory

1. Definition of a probability
2. Unit probability, or elementary probability of a single trial
3. Theorem of compound probabilities

4. Theorem of total probabilities
5. Case of events that do not mutually exclude each other
6. Mathematical expectation
7. Pascal triangle. Case of the heads-or-tails game
8. Formula of the generalized alternative
9. Formula of the simple alternative (called the general formula)
10. Maximum probability. Law of large numbers. Bernoulli's theorem. Gauss–Laplace law
11. Conditions of application
12. Law of small probabilities due to Poisson
13. Probability of causes, Bayes' formula

C. Simple examples of application of probability calculations in cryptography

1. Usefulness of such calculations. Their value and their precision
2. Unit probabilities in cryptography
3. Case of encipherment units
4. Case of code groups
5. Problem of repetitions
6. Newton's formula
7. First practical application: case where the law of large numbers is applicable
8. Second practical problem: probability of a given number of e's in a plaintext
9. Third practical problem: probability that e is the most frequent letter
10. Probability of the frequencies of a transposition
11. Probability of the frequencies of a simple substitution
12. Case of double-key substitutions
13. Special problem: study of the value of a criterion
14. Case of codes. Conclusions

Appendix No. 2. — A Mathematical Theory of Ciphering Systems (Shannon)

1. References and limits of the present study
2. General foundations of Shannon's theories
3. Mathematical structure of an information source. Entropy. Redundancy. Equivocation
4. Theory of telecommunications
5. The algebra of ciphering systems
6. Theoretical secrecy. Practical secrecy. Discussion
7. Mathematical conditions of perfect secrecy
8. Equivocation in the general case. Ideal systems
9. Work characteristic and practical secrecy. Conclusions

Appendix No. 3. — Statistical characteristics of the Russian language

Appendix No. 4. — Statistical characteristics of the German language

Appendix No. 5. — Statistical characteristics of the English language

Appendix No. 6. — Statistical characteristics of the Spanish language

Appendix No. 7. — Statistical characteristics of the Italian language

Table of bigram frequencies in French: outside the text, at the end.

Table of bigram frequencies in Russian: outside the text, at the end.
