Elementary cryptanalysis. Abraham Sinkov

Introduction
Chapter 1 Monoalphabetic Ciphers Using Direct Standard Alphabets
1.1 The Caesar Cipher
1.2 Modular arithmetic
1.3 Direct standard alphabets
1.4 Solution of direct standard alphabets by completing the plain component
1.5 Solving direct standard alphabets by frequency considerations
1.6 Alphabets based on decimations of the normal sequence
1.7 Solution of decimated standard alphabets
1.8 Monoalphabets based on linear transformations

Chapter 2 General Monoalphabetic Substitution
2.1 Mixed alphabets
2.2 Solution of mixed alphabet ciphers
2.3 Solution of monoalphabets in five letter groupings
2.4 Monoalphabets with symbols as cipher equivalents

Chapter 3 Polyalphabetic Substitution

3.1 Polyalphabetic ciphers
3.2 Recognition of polyalphabetic ciphers
3.3 Determination of number of alphabets
3.4 Solution of individual alphabets, if standard
3.5 Polyalphabetic ciphers with a mixed plain sequence
3.6 Matching alphabets
3.7 Reduction of a polyalphabetic cipher to a monoalphabet
3.8 Polyalphabetic ciphers with mixed cipher sequences
3.9 General comments about polyalphabetic ciphers

Chapter 4 Polygraphic Systems
4.1 Digraphic ciphers based on linear transformations matrices
4.2 Multiplication of matrices-inverses
4.3 Involutory transformations
4.4 Recognition of digraphic ciphers
4.5 Solution of a linear transformation
4.6 How to make the Hill System more secure

Chapter 5 Transposition
5.1 Columnar transposition
5.2 Solution of transpositions with completely filled rectangles
5.3 Incompletely filled rectangles
5.4 Solution of incompletely filled rectangles-probable word method
5.5 Incompletely filled rectangles-general case
5.6 Repetitions between messages; identical length messages

Appendix A Table of Digraphic Frequencies
Appendix B Log Weights
Appendix C Frequencies of Letters of the Alphabet
Appendix D Frequencies of Initial Letters of Words
Appendix E Frequencies of Final Letters of Words
Solutions to Exercises
Suggestions for Further Reading
Index
Supplement-Computer Programs by P. L. Irwin
I. Trigraphic Frequency Distributions
II. Index to Coincidence
III. Matching Alphabets
IV. Trigraphic Frequency Distribution for Individual Alphabets of a Periodic Polyalphabetic Cipher
V. Digraphic Frequency Distributions