U.S. Army Basic Cryptanalysis Field Manual

******

TABLE OF CONTENTS

***

PART ONE - INTRODUCTION TO CRYPTANALYSIS

CHAPTER 1 TERMINOLOGY AND SYSTEM TYPES 1-0
Section I Basic Concepts 1-0
II Cryptographic Systems 1-1

CHAPTER 2 SECURITY OF CRYPTOGRAPHIC SYSTEMS 2-1
Secion I Requirements of Military Systems 2-1
II Cryptanalytic Attack 2-3
III Analytic Aids 2-5

PART TWO - MONOGRAPHIC SUBSTITUTION SYSTEMS

CHAPTER 3 MONOALPHABETIC UNILITERAL SUBSTITUTION SYSTEMS USING STANDARD CIPHER ALPHABETS 3-1
Section I Basis of Substitution Systems 3-1
II Monoalphabetic Uniliteral Substitution 3-3
III Solution of Monoalphabetic Uniliteral Ciphers Using Standard Cipher Alphabets 3-6

CHAPTER 4 MONOALPHABETIC UNILITERAL SUBSTITUTION SYSTEMS USING MIXED CIPHER ALPHABETS 4-1
Section I Generation and Use of Mixed Cipher Alphabets 4-1
II Recovery of Mixed Cipher Alphabets 4-6
III Solution of Monoalphabetic Uniliteral Ciphers Using Mixed Cipher Alphabets 4-18

Knihovna FI MU
4200517632

CHAPTER 5 MONOALPHABETIC MULTILITERAL SUBSTITUTION 5-0

Section I Characteristics and Types 5-0

II Analysis of Simple Multiliteral Systems 5-8

III Analysis of Variant Multiliteral Systems 5-18

PART THREE - POLYGRAPHIC SUBSTITUTION SYSTEMS

CHAPTER 6 CHARACTERISTICS OF POLYGRAPHIC SUBSTITUTION SYSTEMS 6-1

Section I Characteristics of Polygraphic Encipherment 6-1

II Identification of Polygraphic Substitution 6-8

CHAPTER 7 SOLUTION OF POLYGRAPHIC SUBSTITUTION SYSTEMS 7-0

Section I Analysis of Four-Square and Two-Square Ciphers 7-0

II Analysis of Playfair Ciphers 7-12

PART FOUR - POLYALPHABETIC SUBSTITUTION SYSTEMS

CHAPTER 8 PERIODIC POLYAPHABETIC SUBSTITUTION SYSTEMS 8-1

Section I Characteristics of Periodic Systems 8-1

II Identifying Periodic Systems 8-5

CHAPTER 9 SOLUTION OF PERIODIC POLYALPHABETIC SYSTEMS 9-1

Section I System Using Standard Cipher Alphabets 9-1

II Systems Using Mixed Alphabets With Known Sequences 9-8

III Solving Periodics With Unknown Sequences 9-17

CHAPTER 10 APERIODIC POLYALPHABETIC CIPHERS 10-0

PART FIVE - TRANSPOSITION SYSTEMS

CHAPTER 11 TYPES OF TRANSPOSITION SYSTEMS 11-1

CHAPTER 12 SOLUTION OF NUMERICALLY-KEYED COLUMNAR TRANSPOSITION CIPHERS 12-0

CHAPTER 13 TRANSPOSITION SPECIAL SOLUTIONS 13-1

PART SIX - ANALYSIS OF CODE SYSTEMS

CHAPTER 14 TYPES OF CODE SYSTEMS 14-0

CHAPTER 15 ANALYSIS OF SYLLABARY SPELLING 15-0

APPENDIX A FREQUENCY DISTRIBUTIONS OF ENGLISH DIGRAPHS

APPENDIX B FREQUENCY DISTRIBUTIONS OF ENGLISH TRIGRAPHS

APPENDIX C FREQUENCY DISTRIBUTIONS OF ENGLISH TETRAGRAPHS

APPENDIX D WORD AND PATTERN TABLES

APPENDIX E UTILITY TABLES

APPENDIX F CRYPTANALYSIS SUPPORT PROGRAM

GLOSSARY

INDEX