FIELD MANUAL
NO 34-40-2

HEADQUARTERS
DEPARTMENT OF THE ARMY
Washington, DC, 13 September 1990

BASIC CRYPTANALYSIS

TABLE OF CONTENTS

Page

PREFACE iv

INTRODUCTION v

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

Section I Requirements of Military Systems 2-1

II Cryptanalytic Attack 2-3

III Analytic Aids 2-5

DISTRIBUTION RESTRICTION: Distribution authorized to U.S. Government agencies only to protect technical or operational information from automatic dissemination under the International Exchange Program or by other means. This determination was made on 5 March 1990. Other requests for this document will be referred to Commander, United States Army Intelligence School, Fort Devens, ATTN: ATSI-ETD-PD, Fort Devens, MA 01433-6301.

DESTRUCTION NOTICE: Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

*This publication supersedes TM 32-220, 20 August 1970.

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
CHAPTER	5	MONOALPHABETIC MULTILITERAL SUBSTITUTION SYSTEMS	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 POLYALPHABETIC 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	Systems 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 A-1

APPENDIX B FREQUENCY DISTRIBUTIONS OF ENGLISH TRIGRAPHS B-1

APPENDIX C FREQUENCY DISTRIBUTIONS OF ENGLISH TETRAGRAPHS C-1

APPENDIX D WORD AND PATTERN TABLES D-0

APPENDIX E UTILITY TABLES E-1

APPENDIX F CRYPTANALYSIS SUPPORT PROGRAM F-0

GLOSSARY Glossary-0

REFERENCES References-1

INDEX Index-0