

# 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
Section II	Cryptographic Systems . . . . .	1-1
CHAPTER 2	SECURITY OF CRYPTOGRAPHIC SYSTEMS . . . . .	2-1
Section I	Requirements of Military Systems . . . . .	2-1
Section II	Cryptanalytic Attack . . . . .	2-3
Section 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

<b>CHAPTER</b>	<b>3</b>	<b>MONOALPHABETIC UNILITERAL SUBSTITUTION SYSTEMS USING STANDARD CIPHER ALPHABETS</b> . . . . .	3-1
	<b>Section</b>	<b>I</b> Basis of Substitution Systems . . . . .	3-1
		<b>II</b> Monoalphabetic Uniliteral Substitution . . . . .	3-3
		<b>III</b> Solution of Monoalphabetic Uniliteral Ciphers Using Standard Cipher Alphabets . . . . .	3-6
<b>CHAPTER</b>	<b>4</b>	<b>MONOALPHABETIC UNILITERAL SUBSTITUTION SYSTEMS USING MIXED CIPHER ALPHABETS</b> . . . . .	4-1
	<b>Section</b>	<b>I</b> Generation and Use of Mixed Cipher Alphabets . . . . .	4-1
		<b>II</b> Recovery of Mixed Cipher Alphabets . . . . .	4-6
		<b>III</b> Solution of Monoalphabetic Uniliteral Ciphers Using Mixed Cipher Alphabets . . . . .	4-18
<b>CHAPTER</b>	<b>5</b>	<b>MONOALPHABETIC MULTILITERAL SUBSTITUTION SYSTEMS</b> . . . . .	5-0
	<b>Section</b>	<b>I</b> Characteristics and Types . . . . .	5-0
		<b>II</b> Analysis of Simple Multiliteral Systems . . . . .	5-8
		<b>III</b> Analysis of Variant Multiliteral Systems . . . . .	5-18

## PART THREE ● POLYGRAPHIC SUBSTITUTION SYSTEMS

<b>CHAPTER</b>	<b>6</b>	<b>CHARACTERISTICS OF POLYGRAPHIC SUBSTITUTION SYSTEMS</b> . . . . .	6-1
	<b>Section</b>	<b>I</b> Characteristics of Polygraphic Encipherment . . . . .	6-1
		<b>II</b> Identification of Polygraphic Substitution . . . . .	6-8
<b>CHAPTER</b>	<b>7</b>	<b>SOLUTION OF POLYGRAPHIC SUBSTITUTION SYSTEMS</b> . . . . .	7-0
	<b>Section</b>	<b>I</b> Analysis of Four-Square and Two-Square Ciphers . . . . .	7-0
		<b>II</b> Analysis of Playfair Ciphers . . . . .	7-12

## PART FOUR ● POLYALPHABETIC SUBSTITUTION SYSTEMS

<b>CHAPTER</b>	<b>8</b>	<b>PERIODIC POLYALPHABETIC SUBSTITUTION SYSTEMS</b> . . . . .	8-1
	<b>Section</b>	<b>I</b> Characteristics of Periodic Systems . . . . .	8-1
		<b>II</b> Identifying Periodic Systems . . . . .	8-5
<b>CHAPTER</b>	<b>9</b>	<b>SOLUTION OF PERIODIC POLYALPHABETIC SYSTEMS</b> . . . . .	9-1
	<b>Section</b>	<b>I</b> Systems Using Standard Cipher Alphabets . . . . .	9-1
		<b>II</b> Systems Using Mixed Alphabets With Known Sequences . . . . .	9-8
		<b>III</b> Solving Periodics With Unknown Sequences . . . . .	9-17
<b>CHAPTER</b>	<b>10</b>	<b>APERIODIC POLYALPHABETIC CIPHERS</b> . . . . .	10-0

## **PART FIVE ● TRANSPOSITION SYSTEMS**

<b>CHAPTER 11</b>	<b>TYPES OF TRANSPOSITION SYSTEMS . . . . .</b>	<b>11-1</b>
<b>CHAPTER 12</b>	<b>SOLUTION OF NUMERICALLY-KEYED COLUMNAR TRANSPOSITION CIPHERS . . . . .</b>	<b>12-0</b>
<b>CHAPTER 13</b>	<b>TRANSPOSITION SPECIAL SOLUTIONS . . . . .</b>	<b>13-1</b>

## **PART SIX ● ANALYSIS OF CODE SYSTEMS**

<b>CHAPTER 14</b>	<b>TYPES OF CODE SYSTEMS . . . . .</b>	<b>14-0</b>
<b>CHAPTER 15</b>	<b>ANALYSIS OF SYLLABARY SPELLING . . . . .</b>	<b>15-0</b>
<b>APPENDIX A</b>	<b>FREQUENCY DISTRIBUTIONS OF ENGLISH DIGRAPHS . . . . .</b>	<b>A-1</b>
<b>APPENDIX B</b>	<b>FREQUENCY DISTRIBUTIONS OF ENGLISH TRIGRAPHS . . . . .</b>	<b>B-1</b>
<b>APPENDIX C</b>	<b>FREQUENCY DISTRIBUTIONS OF ENGLISH TETRAGRAPHS . . . . .</b>	<b>C-1</b>
<b>APPENDIX D</b>	<b>WORD AND PATTERN TABLES . . . . .</b>	<b>D-0</b>
<b>APPENDIX E</b>	<b>UTILITY TABLES . . . . .</b>	<b>E-1</b>
<b>APPENDIX F</b>	<b>CRYPTANALYSIS SUPPORT PROGRAM . . . . .</b>	<b>F-0</b>
<b>GLOSSARY . . . . .</b>		<b>Glossary-0</b>
<b>REFERENCES . . . . .</b>		<b>References-1</b>
<b>INDEX . . . . .</b>		<b>Index-0</b>