PART ONE

Introduction to Cryptanalyst

CHAPTER 1

TERMINOLOGY AND SYSTEM TYPES

Section I

Basic Concepts

1-1. Cryptology

Cryptology is the branch of knowledge which concerns secret communications in all its aspects. Two major areas of cryptology are *cryptography* and *cryptanalytics.*

1-2. Cryptography

Cryptography is the branch of cryptology concerned with protecting communications from being read by the wrong people. Codes and ciphers that are used to protect communications are called cryptographic systems. The application of codes and ciphers to messages to make them unreadable is called encryption. The resulting messages are called cryptograms. The people who create and use cryptographic systems are called cryptographers.

1-3. Cryptanalytics

Cryptanalytics is the branch of cryptology concerned with solving the cryptographic systems used by others. The objects of cryptanalysts are to read the text of encrypted messages and to recover the cryptographic systems used. The text is recovered for its potential intelligence value. The systems are recovered for application to future messages in the same or similar systems.

1-4. Signal Communications

In military applications most encrypted messages are sent by electronic means rather than physically carried or mailed. The electronic means include those sent by wire and those transmitted by radio. Whether wire or radio is used, they can be sent by telephone, telegraph (Morse code), teletypewriter, facsimile, or computer. The electronic means provide greater speed than physical means, but make the communications more vulnerable to intercept by others.

Section II

Cryptographic Systems

1-5. Ciphers and Codes

There are two major categories of cryptographic systems, called ciphers and codes. Nearly all military systems fall into one or the other of these categories or a combination of the two. Cipher systems are those in which the encryption is carried out on single characters or groups of characters without regard to their meaning. Codes, on the other hand, are more concerned with meanings than characters. The basic unit of encryption in a code system is a word or phrase. When a message is encrypted by a code system, code groups primarily replace words and phrases. Code groups may also replace single characters where necessary, but the substitution for complete words is the key distinction that separates a code from a cipher. Because of this, the cryptanalytic approaches to codes and ciphers are quite different from each other.

a. Messages encrypted by a cipher system are said to be enciphered. Similarly, messages encrypted by a code system are encoded. The resulting text is called ciphertext or code text. When a cryptogram is translated back into readable form or *plaintext,* it is said to be decrypted, or more specifically, decoded or deciphered.

b. The term code in this manual is given the formal meaning as explained above and in more detail in Part Six. You will often see and hear the term *code* used with other meanings that do not apply here. Code, in its more general sense, can mean any cryptographic system or any system of replacing one set of values with another. The terms Morse code, binary code, Baudot code, and computer code are examples of the more general usage of the term.

1-6. Enciphered Codes

Some code systems are further encrypted by a cipher system to produce a hybrid type called enciphered codes. This second encryption process is called superencryption or superencipherment. Such systems are normally much more secure than singly encrypted systems, but because of the added complexity take longer to encrypt and are more prone to errors.

1-7. Other Means of Security Communications

Although most military requirements to secure communications are met through the use of codes and ciphers, there are other approaches that can be used in special situations. One such approach is the use of concealment systems. In a concealment system, the plaintext is hidden within another longer text by a predetermined rule or pattern. Other approaches to concealing messages are to use invisible inks or to reduce a message photographically to a dot-sized piece of film. Another approach is to transmit a message from a tape played so fast that it sounds to the ear like a burst of static on the radio. Security for all these methods depends on concealing the fact that a secret message is being sent at all. Once the existence of the communications is suspected or anticipated, the security is significantly lessened.

1-8. Types of Ciphers

There are hundreds of types of cipher systems ranging from very simple paper-and-pencil systems to very complex cipher machine or computer enciphered systems. These can be categorized as either transposition or substitution or a combination of the two.

a. Transposition. In a transposition system, the plaintext characters of a message are systematically rearranged. After transposing a message, the same characters are still present, but the order of the letters is changed.

b. Substitution. In a substitution system, the plaintext characters of a message are systematically replaced by other characters. After the substitution takes place, the order of the underlying plaintext is unchanged, but the same characters are no longer present. In the simplest substitution systems, the replacement is consistent; a given plaintext character always receives the same replacement character or characters. More secure systems change the replacements so that the equivalents change each time the same character is encrypted.

1-9. Substitution Cipher Alphabets

In everyday usage, an alphabet is a list of the letters used by a language. They vary by language. Many European and Latin American languages share the same alphabet as ours or have minor variations. Russian, Greek, Arabic, and Oriental languages have recognizably different alphabets. The term *cipher alphabets* has a slightly different meaning. Instead of a list of characters, a cipher alphabet has two parts; a list of plain-text characters and their cipher equivalents. In the simplest ciphers, an English cipher alphabet will have 26 plaintext letters and 26 ciphertext equivalents, as in the example below.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	Z	C	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W

p: send help
c : BLMI ULGS

In the example, *p:* designates plaintext and *c:* designates ciphertext. For clarity, the plaintext is shown in lower case and the ciphertext in capitals. A more secure alphabet may have more ciphertext equivalents than plaintext characters to provide for some variation in encipherment. Whether or not there is variation, a single alphabet system is called a *monoalphabetic* system. A system which gains more security by systematically using more than one alphabet is called a *polyalphabetic* system.