PART SIX

Analysis of Code Systems

CHAPTER 14

TYPES OF CODE SYSTEMS

14-1. The Nature of Code Systems

As explained in Chapter 1, the key feature that distinguishes a code from a substitution cipher is that a code will substitute for words as well as characters.

a. Codes range in size from small charts or lists on a single sheet of paper to books as large as an unabridged dictionary.

b. Plaintext values are replaced by code groups or code words. A code group or word may replace anything from a single character to a whole sentence.

c. Since codes can compress whole sentences into a small code group, not all codes are used for security purposes. Some are used for economy instead, by replacing common sentences and phrases with a single group. For example, radio operators use Q and Z signals as a brevity code. Q and Z signals are three letter code groups beginning with Q or Z that stand for common communications procedures. A single code Q or Z signal replaces sentences or phrases such as QSA, *My signal strength is* ... and ZNN, *I have nothing now.* Operators memorize the Q and Z signals that they commonly use and the result is quicker, more economical communications.

d. Some codes are used for prearranged messages only. Limited in size and purpose, a single code group may be transmitted as a signal to begin a preplanned attack, for example. Prearranged message codes are sometimes referred to as pamcodes. Prearranged message codes may also take the form of innocent communications, so that an apparently harmless message contains a secret meaning. The message, *Les sanglots longs des violons de l'automne,* a harmless sentence in French, signaled the French underground in World War II that the Allied invasion of France was to begin soon. Codes with an innocent appearance but a secret meaning are known as open codes.

e. Prearranged message codes can only be used for limited, preplanned purposes. General purpose codes which can be used for any communications are more common. All general purpose codes must include within them, a provision for spelling words that are not included in their vocabulary. Even when very large book codes are used, proper names will sometimes need to be encoded that are not in the code's vocabulary. General purpose codes thus share some of the characteristics of substitution ciphers.

f. Codes are at their weakest when they are used to spell words. Most codes are broken into through spelling. Large codes attempt to defeat this weakness by providing many variants for letters and common syllables. The letter E might be encoded by 10 different code groups in a large code, for example. Other code groups would represent common syllables with E in them like RE, ER, EN, and ENT. In this respect, codes are similar to syllabary squares, and the initial approach to analysis can be similar between syllabary squares and codes.

g. When a high degree of security is required using codes, there are two approaches to increasing the security of codes. One is to use very large book codes, since the larger the code, the more secure it is. The other is to further encipher the code to produce an enciphered code. Any of the cipher procedures discussed earlier in this manual can be used, but the most common is to use polyalphabetic encipherment. Repeating keys and long-running keys may be used. It is one way to combine the advantages of brevity with the added security of polyalphabetics, although such procedures are time-consuming to use. They cannot be used practically in rapidly changing combat situations, for example, when speed of communications is important. Large codes and enciphered codes were common earlier in this century when a high degree of security was desired. Today, with advances in electronics, cipher machine and computer based systems are more common when a high degree of security is required.

14-2. Book Codes

Codes too large to be printed on just one or two pages are called book codes. They may range from small pamphlets to large bound books.

a. The code values in book codes may consist of letters, numbers, or a combination of letters and numbers. Usually, the code groups are a constant length, but there are occasional exceptions. Code values used primarily for voice communications will sometimes consist of pronounceable words rather than regular length groupings of characters. We will refer to only code groups in the rest of this chapter and the next, but you should understand that comments about code groups also apply to code words.

b. The simplest book codes consist of a single orderly listing of code groups and their meanings. The code groups are listed in the book in alphabetical or numerical order, and their meanings are also in a logical order. This single listing is used for encoding and decoding, and is called a one-part code. The plaintext values may be strictly alphabetical in arrangement or may be separated into separate sections for words, letters and syllables, and numbers. Occasionally, they will be arranged topically with such things as units in one section, weapons systems in another, place-names in another, and so on. The key feature of one-part codes is that when the code groups are listed in order, their plaintext meanings will also be in a logical order. A sample portion of a one-part code is shown below.

CODE GROUP:	PLAINTEXT:
AAB	A
ABD	AB
ACF	ABANDON
ADH	ABOUT
AEJ	ACCIDENT
AFL	ACTION
AGN	ACTIVE
AHP	ACTIVITY
...	...
...	...

c. The orderly structure of one-part codes makes them easy to use, but greatly reduces their security. The analyst can use the structure to narrow down possible meanings for code groups. More secure codes are randomly arranged, and are necessarily printed in two parts. One section lists the code groups in order, and it is used for decoding. The other section, containing exactly the same information, lists the plaintext values in order, and is used for encoding. This type of code is called a two-part code. Portions of the encoding and decoding sections of a two-part code are shown below. Note that one group occurs in common between the two parts.

ENCODING SECTION:		DECODING SECTION:	
KTOL	A	ABAB	RESISTANCE
YNIF	A	ABEC	SIZE
ACEJ	AB	ABID	CHEMICAL
VAUW	ABANDON ING S	ABOF	T-72
WHOD	ABILITY	ABUG	QUALITY
AOUT	ABLE	ACAH	15
LWOQ	ABLE TO	ACEJ	AB
TEER	ABOUT	ACIK	VERIFY ING S
...	...	...	...
...	...	...	...

14-3. Matrix Codes and Code Charts

Small codes can be conveniently printed in the form of a small coordinate matrix system.

a. Typically 10 by 10 or larger, matrix codes, also known as code charts, can contain letters, syllables, numbers, and a small vocabulary of words. They are very easy to use, and communicators can be trained in their use quickly and easily. They also offer more security than most simple ciphers.

b. Code charts are easily changed from one cryptoperiod to the next by simply changing the coordinates, while retaining the same matrix.

c. They are a very close relative to the syllabary square cipher. If the syllabary square shown in Chapter 5 contained some words as well as letters, syllables, and numbers, it would be a code instead of a cipher.

d. One type of code chart places two plaintext values in each cell—an upper value and a lower value. The lower values are all words. The upper values are all numbers, letters, or syllables. Two of the cells are set aside as shift values to indicate whether to read the upper values or lower values in the code groups that follow. A sample chart of this type is shown in Figure 14-1. This example uses letters for coordinates, and has variants on each row and column. The word *ARTILLERY*, for example, could be encoded as TF, TI, QF, or QI. The cells MU and UU are begin and end spell indicators. The bottom values in each cell are used until a begin spell group is sent. Then the top values are used until the end spell group is used to shift back to the lower values.

	C,D	E,H	F,I	J,K	T,L	M,O	U,V	Y,G	Z,N	P,Q	X,R	W,S	B,A
M,H	ØØØ Action, ive, ivity, s	Ø2 Addition, al	15 Advance, d, ing, s	45 After	A Aggressor, ive (ly), s	AD Air	Spell/fig. Begins	AL Airborne	AM Aircraft/ Airplane, s	AN Ammunition	AND Antiaircraft	AR Antitank	ARE Area (of)
T,Q	ØØ Armor, ed	Ø3 Arrive, al, d, ing, s	16 Artillery	5Ø Assemble, d, ing, s	AS Attack, ed, ing, s	AT Attempt, ed, ing, s	B Azimuth (in degrees)	BA Battalion, s	BE Battery, ies	BY Begin/start, ed, ings, s	C Bomb, ed, er, ing, s	CA Bridge, d, ing, s	CAN Capture, d, ing, s
K,Z	Ø Casualty, ies,	Ø4 Command er, ing, s	17 Communicate, d, ing, ion, s	55 Company, ies	CE Complete, d, ing, ion, s	CH Concentrate, d, ing, ion, s	CO Contact, ed, ing, s	D Coordinate, d, ing, ion, s	DA Corps	DAY Counterattack, ed, ing, s	DE Cross, ed, es, ing	DI Defend/de-fense, s (of)	DO Delay, ed, ing, s
O,L	1 Destroy, ed, ing, s	Ø5 Detach, ed, ment (of), s	18 Dispose, al, d, ition, s	E Division, s	EA Dump, s	ED East (of)	EE Encounter, ed, ing, s	EN Enemy's	ENT Engineer, s	ER Enlisted Man/Men	ERS Equip, ment, ped, ping	ES Escape, d, ing, s	EST Estimate, d, ing, s (at)
R,X	2 Expect, ed, ing, s (at)	Ø6 Fight, er, ing, s	19 Fire, d, ing, s	ET Flank, s	F Force, d, ing, s	FO Forward	FOR Friend, ly	G From	H Front, al, s	HA Fuel, s	HE Gun, s	I Has/have	IL Headquarters
S,P	3 Heavy, ily	Ø7 Hill, s (No.)	2Ø Hold, ing, s/held	IN Hostile, ity, ities	ING Hour, s	ION How	IS Identify, ied, ies, ing, ication	IT Immediate, ly	IVE Infantry	J Inform, ation, ed, ing, s	K Install, ation, ed, ing, s	L Junction, s (of)	LA Land, ed, ing, s
W,N	4 Large	Ø8 Left (of)	21 Line, s (of)	LE Locate, d, ing, ion, s	LI Machine gun, s (nest)	LO Main	LY Map, ped, ping, s	M Mechanize, d	MA Message, nger, s	ME Mile, s (from), (to)	MENT Mine, d, ing, s	MI Mission, s	MY Morning
A,B	5 Mortar, s	Ø9 Move, d, ing, ment, s	22 Near	N Night	NA No/not/nothing/negat	ND North (of)	NE Number, s, (of)	NI Objective, s	NO Observe, ation, d, ing, s	NOT Occupy, ied ies, ing	NT Officer, s	O Operate, d, ing, ion, s	OF Order, ed, ing, s
C,E	6 Over	1Ø Patrol, led, ling, s	23 Penetrate, d, ing, ion, s	ON Plan, ned, ning, s (to)	OR Platoon, s	OU Point, ed, ing s	OUR Position, s	P Post, ed, ing, s	PE Prepare, d, ation, ing, s	Q Prisoner, s	QU Proceed, ed, ing, s, ure	R Radio, ed, s	RA Railway/ Railroad, s
I,G	7 Ready (for) (to)	11 Rear	25 Receive, d, ing, s/receipt	RE Reconnais-sance	RED Refer, ence, red, ring, s (to)	RES Regiment, al, s	RI Reinforce, d, ing, ment, s	RO Replace, d, ing, ment, s	RS Report, ed, ing, s	RT Request, ed, ing, s	S Require, d, ing, isition, s	SA Reserve, d, ing, s	SE Ridge, s
D,J	8 Right (of)	12 River/ Stream	3Ø Road, s/ Route, s	SH Scout, ing, s	SI Section, s/ Sector, s	SO Send, ing, s/sent (to)	ST Shell, ed, ing, s	T Small/ Small arms	TA South (of)	TE Squad, s	TED Strength, s (of)/strong	TER Stop, ped, ping, s	TH Supply, ies (of)
F,V	9 Support, ed, ing, s	13 Tank, s	35 Target, s	TI Today	TION Tomorrow	TO Tonight	TR Troop, s	U Truck, s/ Vehicle, s	UN Unit, s (of)	US Until	V Urgent, cy, ly	W Vicinity (of)	WE Water
U,Y	Ø1 West (of)	14 What/who	4Ø When	X Where	Y Will	Z With	Spell/fig. Ends	Period . Withdraw, al, ing, s	Comma , Woods	Colon : Yard, s (from), (to)	Smcln ; Yesterday	Dash — You, r	Paren ( ) Zone, s (of)

Figure 14-1. Sample code chart.