SOLUTION OF PROGRESSIVE-ALPHABET CIPHER

with

STANDARD PLAINTEXT ALPHABET and

UNKNOWN MIXED CIPHER ALPHABET.

The message on page 55 of Book III, Military Cryptanalysis is enciphered with ABC. . . . Z plaintext against HYDRAULIC. . . . Z cipher, as follows:

e n e m y h a s p l a c e d h e a v y i n t e r d i
A K L M D G L Z W S E J N N T Q N G N Y I K H K Y I

c t i o n f i r e u p o n z a n e s v i l l e r o a d
D S E O O E K X G R Z Z Z G K D S B J Y U L H K G Z

d
R

Suppose, with the technique now suggested, we take a long list of probable words and test one after the other, it will soon become evident that one word alone will fit in the spot we have chosen, and it will quickly prove itself, so we will pass all the preliminary trials and come to INTERDICTION at the place we have chosen, because of some repetition in other messages. I place below the cipher text representing this repetition, in four different positions, to represent four sets of repeated letters. The repeated letters are underlined. Under each repetition is placed a portion of our standard alphabet in reverse, as a scale. Beneath each of our chosen repetitions is drawn vertically a standard alphabet. At some point below, and within the limits of our chosen repetition must be fitted the probable word. (See next page).

Cipher text --	Y	I	K	H	K	Y	I	D	S	E	0	0		Y	I	K	H	K	Y	I	D	S	E	0	0
	l	k	j	i	h	g	f	e	d	c	b	a		l	k	j	i	h	g	f	e	d	c	b	a
		l					g									k		i							
		m					h									l		j							
	i	n	t	e	r	d	i	c	t	i	o	n				m		k							
		o					j									n		l							
		p					k									o		m							
		q					l									p		n							
		r					m									q		o							
		s					n									r		p							
		t					o									s		q							
		u					p							i	n	t	e	r	d	i	c	t	i	o	n
		v					q									u		s							
		w					r									v		t							
		x					s									w		u							
		y					t									x		v							
		z					u									y		w							
		a					v									z		x							
		b					w									a		y							
		c					x									b		z							
		d					y									c		a							
		e					z									d		b							
		f					a									e		c							
		g					b									f		d							
		h					c									g		e							
		i					d									h		f							
		j					e									i		g							

Cipher text --	Y	I	K	H	K	Y	I	D	S	E	0	0		Y	I	K	H	K	Y	I	D	S	E	0	0
	l	k	j	i	h	g	f	e	d	c	b	a		l	k	j	i	h	g	f	e	d	c	b	a
											c	b		m					h						
											d	c		n					i						
											e	d		o					j						
											f	e		p					k						
											g	f		q					l						
											h	g		r					m						
											i	h		s					n						
											j	i		t					o						
											k	j		u					p						
											l	k		v					q						
											m	l		w					r						
											n	m		x					s						
	i	n	t	e	r	d	i	c	t	i	o	n		y					t						
											p	o		z					u						
											q	p		a					v						
											r	q		b					w						
											s	r		c					x						
											t	s		d					y						
											u	t		e					z						
											v	u		f					a						
											w	v		g					b						
											x	w		h					c						
											y	x		i	n	t	e	r	d	i	c	t	i	o	n
											z	y		j					e						
											a	z		k					f						

of drawn down alphabet

It will thus be seen that "interdiction" fits into each one of the pair, trio or whatever it happens to be, of repeated letters, and any probable word that fails would be false.

SOLUTION OF PROGRESSIVE-ALPHABET CIPHER

with

UNKNOWN MIXED PRIMARY ALPHABETS

This case is touched upon in Par. 39, e, of MILITARY CRYPTANALYSIS, Part III. I have chosen the brief message appearing on page 55, Par. 39, b, assuming we do not know the primaries. Suppose we correctly assume INTERDICTION, because of it appearing as a repetition appearing in a collection of messages, we first place the components in the following position:

H E N L H H L C V B S S
I N T E R D I C T I O N

First note cipher component of each repeated PT letter; take the components of "I" in same columns below.

H L B ---Thus
E S ---Then for "N"
N V ---Finally for "T"
H Y D R A U L I C B etc

Then same identical components with order of letters reversed, or spelled backwards.

S S B V C L H H L N E H--Thus
N O I T C I D R E T N I

Then bring down the PT component of each repeated cipher "S"

N O ---
I E ---Then "L"
D R I Then "H" Now, a quick comparison
H Y D R A U L I C etc with HYDRAULIC . . . Z will show that each letter in the two groups thus brought down is in the proper position with reference to other letter or letters on the same line; in other words, it is building up the primary. Now, to consolidate any of the scattering groups that may be tied together. From three different lines we get the following:

D R I E
h y d r a u l i c b e f g j k m n o p q s t v w x z

and compare with primary

S

Now, to hook in the balance of our scattered values: There happens to be a common letter "O", so we make the following diagram:

N
O
I
T
H E N L H H L C V B S S
I
D
R H D R
E
T
N
I H D R L I B E N O S T V

note

Now, if our primary is laid vertically across a pair of letters in any column that the intervals are correct; that is, there are seven intervals between "H" and "I", etc. Now, giving us additionally

H I

it ties in more of our stray groups and gives us

I E S

This is probably enough, but if we used all the material in the new diagram at our left, we would have:

Attention is called to the following principle, for what it is worth: The interval between any two sequent cipher text letters is one digit greater than between their plain text components, measured in terms of the primary alphabet. For instance, note the following first five letters of both plain text and cipher in our message, spread to include the intervals of both:

E 6 N 20 E 5 M 12 Y

E 7 O 21 G 6 P 13 U

There may be an occasional case, (tho not in our instant "solution") where we might have an established E - M, with two separate groups with a G in one and P in another. This permits us to tie them together, allowing an interval of 6 instead of 5.

This is in a very nebulous state, but it is hoped it may lead to further development.

Respectfully submitted,

Paul H. Burdick.

P. S. It will be noted that in comparing the interval across other letters, the cipher interval becomes greater for each letter forward. Thus, from PT E to Y the interval is 17, and from cipher E to U it is 21.