SOLUTION OF
PLAIN TEXT AUTO KEY PROBLEM
using
UNKNOWN IDENTICAL PRIMARIES

As stated in Military Cryptanalysis, Part III, Page 48, Par. 32, c, solution is rendered difficult because of the lack of an established method of proving assumed values. While the following presents scant material, because of shortage of time for exhaustive experiments, it is believed it may open the way for reconstructing the primary alphabets because of a law akin to that known as the law of indirect symmetry.

The first word of the enclosed message (sheet 1, pencil number,) reads as follows:

p r i s o n e r s
K E Y G C F M G V adding reference numbers
1 2 3 4 5 6 7 8 9

It will be noted by reference to the scale immediately below, that cipher letters 2 and 3 of the message have the same interval in the primary as plain text letters 1 and 3.

A B H I N G T O B C D E F J K L M P Q R U V X Y Z
1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6

From this scale it will be observed that the interval between p and i is 12 letters and the same interval appears between E and Y. The same rule creates the interval between P.T. Nos. 2 and 4 and C. 3 and 4, i.e., the interval between r and s is 8, and the same between Y and G. Of course, the same interval relationship will be maintained thruout all messages enciphered by this method.

Attention is now directed to sheet No. 2, which graphically illustrates this law. While this type of "box" would ordinarily be used for testing assumed probable words, it is here used as an enciphering "box" to illustrate this type of indirect symmetry. These repetitions were taken from the bottom of sheet 1.

It will be observed that the key word, WASHINGTON, is enciphered in this group. This was arbitrarily done to show how it looms up in the cipher message, and, being alternately spaced, it is a simple matter to insert the obvious letters to complete the key.

Now, checking with the enciphering chart, sheet No. 3, it will be seen, on sheet 2, that in each improvised "box" the column at the left contains the key and the horizontal line at the top contains the plain text letters for encipherment, the resultant cipher letters being within the box in pencil.

Now, note that in the encipherment of key plus plain text, if the key and plain text letters are reversed the same cipher letter results. Key "R" plus P. T. "E" produces cipher "G"; key "E" plus P.T. "R" produces the same cipher letter. In this case, after each individual encipherment the process was reversed, the key taken from the top and plain text from the side, with the resultant red letter. Then, for illustrative purposes, a pencil figure representing an interval, was placed between the red letter and the pencil cipher letter in the same line. Next, the same interval was noted, together with a curved line, between the plain text letters connected by this interval, which, of course, are always alternate.

Attention is here called, for what it is worth, to the fact that from red letter V (in the "Headquarters" box) indicated by arrow from "a" to pencil letter V, indicated by arrow from "b", the sum of the intervals involved is 78, or three times 26. The same total will be found between u and s in the plain text above. This means, if this process of encipherment could be accomplished by some mechanical device resembling the Wheatstone mechanism, with three concentric alphabets of 26 letters each, the hand always moving clockwise down the cipher alphabet, from one chosen cipher letter to the next, it would make three complete revolutions between the letters just noted. Thus, between all repeated cipher letters in a message,

will be found a sum of intervals divisible by 26.

Now, of what value are the findings so far?

A problem, using the same key word, with much the same material, omitting, however, the encipherment of the key word, was sent to Mr. Howell C. Brown, of Pasadena, California, to solve. He solved this problem within six to eight hours, by assuming one or two repetitions like "infantry" or "artillery," and watching for probable sequences in the primary alphabets he was attempting to reconstruct. When he discovered about half a dozen letters in sequence the rest went like a house of cards.

During the decrypting of this test problem, he discovered that in an equation such as noted here, the relation between p and i as compared to that between E and Y, the same thing is true in the interval between p and E and i and Y. That is to say, in all cases such as P.T. 1 and 3 and C. 2 and 3, there is an identical interval between P.T. 1 and C. 2 on the one hand and P. T. 3 and C. 3 on the other hand. This is an additional factor which may assist in checking the assumed probable word.

REF ID:A60209

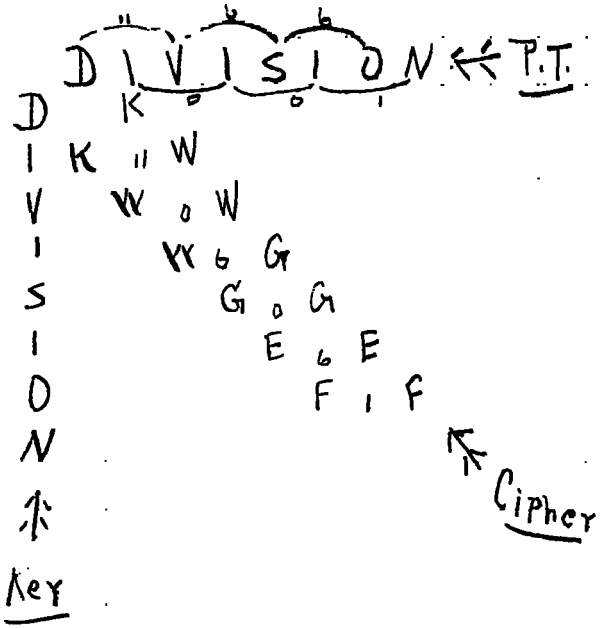
The following message was enciphered by means of PLAIN TEXT AUTO KEY using identical mixed alphabets with key word WASHINGTON.

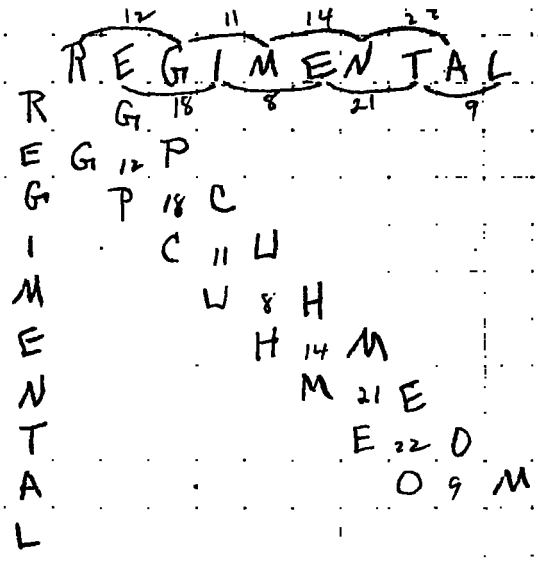
	1.	2.	3.	4.	5.	6.
a.	Prisoner's report that considerable					
	K E Y G C F M G V V G I W S A J C I O M P F T G K X G U C Z					
b.	edamage was done by our dive bombers					
	S X E P P T P E A H F Q F M U T G H K N K W O U M Z W U G V					
c.	to bridge head on Washington road					
	B K M H Y K M P K K F E Q F N A H N T B D F K F Z S B E R U					
d.	tween Brockton and Middleton stop A					
	Q T E Y M J H S P Z V K F G G L S U K V A S Q K F T B K W Q					
e.	lsore porten emyr etreating along W					
	M P C S G I W S A Q M M H K P G Q A G F O D B D T M Y F D G					
f.	ashington road and that their regim					
	A H N T B D F K F Z S B E E G L P C I O J C K L Y J G P C U					
g.	ental headquarters was destroyed a					
	H M E Q M Q K F E I J V U A Q G V S A H F X J B A S G C X E					
h.	ndthe irdivision headquarters was					
	G L P C K L Y N K W W G G E F O K F E I J V U A Q G V S A H					
i.	struck severaltimes by bombs stop N					
	I B A K N Z M J O O G U M X D U H J D T T M Z W D I B K W X					
j.	ewregiment and division makeshi					
	M E R G P C U H M E O M M G L V K W W G G E F V P L A J N T					
k.	fthead quarters established two mi					
	A R C K F E I J V U A Q G V J J B C C Z R G N K X P T O Z U					
l.	lesdirectly south of Newberry stop					
	R S J F K Y G V M X J W C H S C D U P M E B U G J P W B K W					
	1.	2.	3.	4.	5.	6.

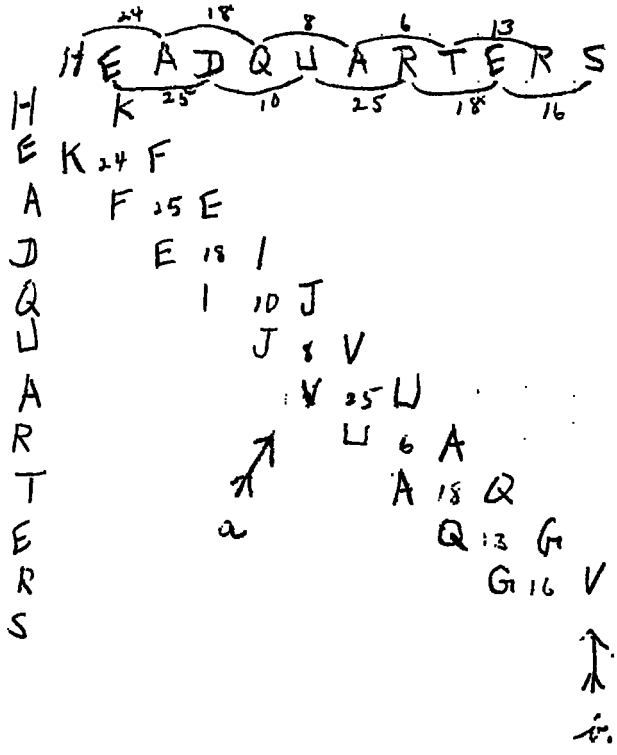
REPETITIONS

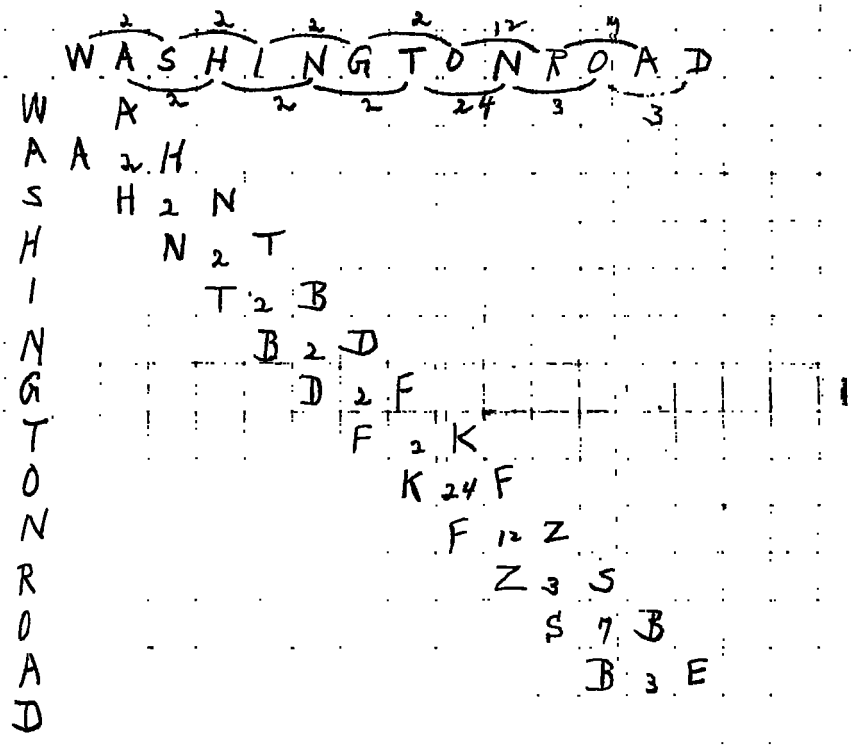
Washington Road, headquarters, regimental, division.

1.


DIVISION
Key
Cipher


REGIMENTAL


HEADQUARTERS


WASHINGTONROAD

P.T. WASHINGTON + ITSELF

P.T. W Primary C.A.S.H.I.N.G.T.O.B.C.D.E.F.J.K.L.M.P.Q.R.U.V.X.Y.Z

A -	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	- 1
	S	C	J	D	E	F	J	T	I	N	K	L	M	P	G	B	Q	R	U	H	O	V	X	A	Y	Z	W
B -	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	- 2
	C	J	Q	R	U	V	K	E	F	X	Y	Z	W	J	M	A	S	H	D	L	I	N	B	G	T	O	
C -	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	- 3
	J	Q	R	U	V	X	L	F	J	Y	Z	W	A	K	P	S	H	I	E	M	N	G	C	T	O	B	
D -	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	- 4
	E	R	U	V	X	Y	M	J	K	Z	W	A	S	L	Q	H	I	N	F	P	G	T	D	O	B	C
E -	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	- 5
	F	U	V	X	Y	Z	P	K	L	W	A	S	H	M	R	I	N	G	J	Q	T	O	E	B	C	D
F -	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	- 6
	J	V	X	Y	Z	W	Q	L	M	A	S	H	I	P	U	N	G	T	K	R	O	B	E	C	D	E	
G -	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	- 7
	T	K	L	M	P	Q	E	B	C	R	U	V	X	D	J	Y	Z	W	O	F	A	S	G	H	I	N	
H -	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	- 8
	I	E	F	J	K	L	B	G	T	M	P	Q	R	O	D	U	V	X	N	C	Y	Z	H	W	A	S	
I -	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	- 9
	N	F	J	K	L	M	C	T	O	P	Q	R	U	B	E	V	X	Y	G	D	Z	W	I	A	S	H	
J -	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	- 10
	K	X	Y	Z	W	A	R	M	P	S	H	I	N	Q	V	G	T	O	L	U	B	C	J	D	E	F	
K -	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	- 11
	L	Y	Z	W	A	S	U	P	Q	H	I	N	G	R	X	T	O	B	M	V	C	D	K	E	F	J	
L -	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	- 12
	A	Z	W	A	S	H	V	Q	R	I	N	G	T	U	Y	O	B	C	P	X	D	E	L	F	J	K	
M -	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	- 13
	P	W	A	S	H	I	X	R	U	N	G	T	O	V	Z	B	C	D	Q	Y	E	F	M	J	K	L	
N -	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	- 14
	G	J	K	L	M	P	D	O	B	Q	R	U	V	C	F	X	Y	Z	T	E	W	A	N	S	H	I	
O -	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	- 15
	B	M	P	Q	R	U	J	D	E	V	X	Y	Z	F	L	W	A	S	C	K	H	I	O	N	G	T	
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	- 16
	Q	A	S	H	I	N	Y	U	V	G	T	O	B	X	W	C	D	E	R	Z	F	J	P	K	L	M	
Q -	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	- 17
	K	S	H	I	N	G	Z	V	X	T	O	B	C	Y	A	D	E	F	U	W	J	K	Q	L	M	P	
R -	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	- 18
	U	H	I	N	G	T	W	X	Y	O	B	C	D	Z	S	E	F	J	V	A	K	L	R	M	P	Q	
S -	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	- 19
	H	D	E	F	J	K	O	N	G	L	M	P	Q	T	C	R	U	V	I	B	X	Y	S	Z	W	A	
T -	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	- 20
	O	L	M	P	Q	R	F	C	D	U	V	X	Y	E	K	Z	W	A	B	J	S	H	T	I	N	G	
U -	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	- 21
	V	I	N	G	T	O	A	Y	Z	B	C	D	E	W	H	F	J	K	X	S	L	M	U	P	Q	R
V -	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	- 22
	X	N	G	T	O	B	S	Z	W	C	D	E	F	A	I	J	K	L	Y	H	M	P	V	Q	R	U	
W -	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	- 23
	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	
X -	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	- 24
	Y	G	T	O	B	C	H	W	A	D	E	F	J	S	N	K	L	M	Z	I	P	Q	X	R	U	V	
Y -	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	- 25
	Z	I	O	B	C	D	I	A	S	E	F	J	K	H	G	L	M	P	W	N	Q	R	Y	U	V	X	
Z -	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	- 26
	I	O	B	C	D	E	N	S	H	F	J	K	L	I	T	M	P	Q	A	G	R	J	Z	V	X	Y	

Z

3