Methods for The Solution of Running-Key Ciphers

William F. Friedman

Publication No. 16

RIVERBANK LABORATORIES
DEPARTMENT OF CIPHERS
RIVERBANK
GENEVA, ILL.
1918

Letter of Transmissal

Riverbank Laboratories

Geneva, Ill.

Department of Ciphers

January 18, 1918

COLONEL GEORGE FABYAN,

Chicago, Illinois.

My Dear Colonel Fabyan:

I have the honor to transmit to you Publication Number 16, of the Department of Ciphers “Methods for the Solution of Running-Key Ciphers.”

Concerning the possibility of the decipherment of a message or a series of messages enciphered by a running-key, it was said until as recently as three months ago, “It can’t be done” or ”It is very questionable.” It is probably known to you that the U.S. Army Disk in connection with a running-key has been used as a cipher in field service for many years, and is, to the best of our knowledge, in use to-day. I suppose that its long-continued use, and the confidence placed in its safety as a field cipher has been due very probably to the fact that no one has ever taken the trouble to see whether ”It could be done.” It is altogether probable that the enenmy, who has been preparing for war for a long time, has not neglected to look into our field ciphers, and we are inclined to credit him with a knowledge equal to or superior to our own. We have been able to prove that not only is a single short message enciphered by the U.S. Army Disk, or any similar device, easily and quickly deciphered, but that a series of messages sent out in the same key may be deciphered more rapidly than they have been enciphered!

Hence, since not destructive but constructive criticism is the purpose of the Department, we have earnestly endeavored, by pointing out the defects of the old system, to show how the same may be remedied, and how the system may be made more trustworthy. The final paragraphs of this booklet state our conclusions, gained from the results of our investigations.

It is our hope that this booklet will be a source not only of interest to you, but of active benefit in these times when the fate of nations is more than ever dependent upon effective means of secret communication.

Very respectfully,

W. F. Friedman

Director,

Department of Ciphers,
Riverbank Laboratories

METHODS FOR THE SOLUTION OF RUNNING-KEY CIPHERS

RUNNING-KEY CIPHER is the name applied to that system of enciphering which necessitates the use of a book or document, identical copies of which are in possession of the correspondents. The letters of the book text are used as successive key letters in conjunction with any system which will produce a series of twenty-six different alphabets, one for each different letter of the ordinary alphabet of which the running-key text is composed. The possibility of the decipherment of a message or of messages enciphered by such a system has long been considered questionable. As a matter of fact, such a cipher may nearly always be solved; and the solution of a series of messages enciphered by the same running-key is very simple. In order to demonstrate how easy the solution of a series of messages in the same running-key actually is, the following example is given and the underlying principles will follow later.

(1) Solution of a series of messages enciphered by the same running-key and a Vigénère Table (two sliding direct alphabets).

MESSAGES

1.	VBEKT	CLPXZ	VNHQB	VEYIN	IWZSI
2.	SAXTC	DKLTR	YEFWW	NMAEE	KZMZQ
3.	ZNKNI	UNUFV	PNTPW	IXKXQ	WSVRX
4.	HJHAL	CNZEE	KMRQI	QOHRE	IFKCS
5.	OEMPP	ZXYCW	PRRGI	ZTNIF	BSWSX
6.	ORKVT	ZTUIS	VMOGM	FMYSA	EVXKT
7.	GUKHT	BXSEE	KBVJA	UXSPU	NWIRJ
8.	RREHC	OMAET	ROASW	FBAMQ	NLMZQ
9.	BRXKP	OKNIJ	BPCOG	BYNEU	MSWYX
10.	FRLLV	JXHQD	BNVWQ	BGTYU	TTIGJ

Take the first three vertical columns of cipher letters and "set" them in horizontal lines on sliding direct alphabets, thus:

TABLE 1.

Column 1	Column 2	Column 3
Cipher letters	Cipher letters	Cipher letters
VSZHOOGRBF	BANJERURRR	EXKHMKKEXL
WTAIPPHSCG	CBOKFSVSSS	FYLINLLFYM
XUBJQQITDH	DCPLGTWTTT	GZMJOMMGZN
YVCKRRJUEI	EDQMHUXUUU	HANKPNNHAO
ZWDLSSKVFJ	FERNIVYVVV	IBOLQOOIBP
AXEMTTLWGK	GFSOJWZWWW	JCPMRPPJCQ
BYFNUUMXHL	HGTPKXAXXX	KDQNSQQKDR
CZGOVVNYIM	IHUQLYBYYY	LEROTRRLES
DAHPWWOZJN	JIVRMZCZZZ	Key letter T
EBIQXXPAKO	KJWSNADAAA	
FCJRYYQBLP	LKXTOBEBBB	
GDKSZZRCMQ	MLYUPCFCCC	
HELTAASDNR	NMZVQDGDDD	
Key letter O	ONAWREHEEE	
	Key letter N	

Now combine the horizontal row of letters representing the plain-text equivalents of the first column of cipher letters with those representing the second and third columns and the results are as follows:

	1	2	3
Key:	O	N	T
1.	H	O	L
2.	E	N	E
3.	L	A	R
4.	T	W	O
5.	A	R	T
6.	A	E	R
7.	S	H	R
8.	D	E	L
9.	N	E	E
10.	R	E	S

Repeat the preceding process for the succeeding columns:

Add the equivalents to what has already been determined:

	123456
Key:	ONTHEO
1.	HOLDPO
2.	ENEMYP
3.	LARGEG
4.	TWOTHO
5.	ARTILL
6.	AEROPL
7.	SHRAPN
8.	DELAYA
9.	NEEDLA
10.	RESERV

There is no doubt that the messages can now be solved completely. Only such time is needed as it takes to produce, by the foregoing almost automatic method, the equivalents for each vertical column of cipher letters. The messages and key read:

Key:	ONTHE	OTHER	HANDI	NTHEC	ASEOF
1.	HOLDP	OSITI	ONUNT	ILREL	IEVED
2.	ENEMY	PREPA	RESTO	ATTAC	KHILL
3.	LARGE	GUNBE	INGMO	VEDTO	WARDS
4.	TWOTH	OUSAN	DMENA	DVANC	INGON
5.	ARTIL	LERYF	IREDA	MAGED	BASES
6.	AEROP	LANEB	OMBDE	STROY	EDTWO
7.	SHRAP	NELAN	DBIGS	HELLS	NEEDE
8.	DELAY	ATTAC	KONPO	SITIO	NTILL
9.	NEEDL	ARGES	UPPLY	OFGAS	MASKS
10.	RESER	VEAMM	UNITI	ONMUS	TBESE

Now how was this simple solution of an “undecipherable” system achieved, and what are the principles involved?

To illustrate, return to the series of messages just deciphered, which were enciphered by a Vigénère Table, shown in the accompanying Figure 1. Each column of cipher letters is

TABLE 2.

Column 4 Cipher letters	Column 5 Cipher letters	Column 6 Cipher letters
KTNAPVHHKL	TCILPTTCPV	CDUCZZBOOJ
LUOBQWIILM	UDJMQUUDQW	DEVDAACPPK
MVPCRXJJMN	VEKNRVVERX	EFWEBBDQQL
NWQDSYKKNO	WFLOSWWFSY	FGXFCCERRM
OXRETZLLOP	XGMPTXXGTZ	GHYGDDFSSN
PYSFUAMMPQ	YHNQUYYHUA	HIZHEEGTTO
QZTGVBNNQR	ZIORVZZIVB	IJAIFFHUUP
RAUHWCOORS	AJPSWAAJWC	JKBJGGIVVQ
SBVIXDPPST	BKQTXBBKXD	KLCKHHJWWR
TCWJYEQQTU	CLRUYCCLYE	LMDLIIKXXS
UDXKZFRRUV	DMSVZDDMZF	MNEMJJLYYT
VEYLAGSSVW	ENTWAEENAG	NOFNKKMZZU
WFZMBHTTWX	FOUXBFFOBH	OPGOLLNAAV
ZGANCIUUXY	GPVYCGGPCI	Key letter O
YHBODJVVYZ	HQWZDHHQDJ	
ZICPEKWWZA	IRXAEIIREK	
AJDQFLXXAB	JSYBFJJSFL	
BKERGMYYBC	KTZCGKKTGM	
CLFSHNZZCD	LUADHLLUHN	
DMGTIOAADE	MVBEIMMVIO	
Key letter H	NWCFJNNWJP	
	OXDGKOOXKQ	
	PYEHLPPYLR	
	Key letter E	

the result of the encipherment of all the plain-text letters in that column by the same key letter. Therefore, all the cipher letters in one column are an equal distance removed from their respective plain-text letters. That is, the series of plain-text letters HELTAASDNR (Column 1 of the example) with the key letter O and the Vigénère Table give the cipher equivalents VSZHOOGRBF, cipher letters being taken at the intersection of the column determined by the key letter with the horizontal line determined by the plain-text letter. (See page **??**). The same result will be obtained, but by a longer proces, explained below, which is known as "running down".

The statement made above namely, that all the cipher letters in one column are an equal distance removed from their respective plain-text letters means then, that if, when the key letter is O, the cipher equivalent of plain-text letter H in this example is V, that is, fourteen letters removed from H in a direct alphabet, then the cipher equivalent of plain-text letter E is likewise fourteen letters removed from E, giving the cipher letter S; text L giving Z, etc. In fact, all the cipher equivalents of this column of letters may be found by writing the series of plain-text letters in a horizontal line and then continuing beneath each letter the direct alphabet. Thus:

	HELTAASDNR
1.	IFMUBBTEOS
2.	JGNVCCUFPT
3.	KHOWDDVGQU
4.	LIPXEEWHRV
5.	MJQYFFXISW
6.	NKRZGGYJTX
7.	OLSAHHZKUY
8.	PMTBIIALVZ
9.	QNUCJJBMWA
10.	ROVDKKCNXB
11.	SPWELLDOYC
12.	TQXFMMEPZD
13.	URYGNNFQAE
14.	VSZHOOGRBF

On the other hand, given the cipher letters, the plain-text equivalents may be found either by reversing the process or by continuing the same process; for, if the direct alphabet ending with Z is continued by repeating the alphabet, or if it is printed in circular form on a revolving disk, it may be regarded as a continuous, circulating series of letters, and it therefore follows that if H leads to V, then V will lead to H. This process of continuing the sequence of a series of letters constituting an alphabet, which is known as "running down", may be greatly facilitated by the use of the devices shown in Plate 1.[1].

The Sliding Poly-Alphabet, A, consists of a series of twenty-six direct alphabets printed upon cardboard strips which are mounted upon celluloid; the strips are all movable, running either in grooves or on tracks, the two pieces of plate glass provided with set-screws at the corners holding the strips firmly, yet loosely enough so that they easily slide up and down. There is in addition a direct alphabet at the extreme left, and a reversed at the extreme right. The sliding strips bear upon their reverse sides other alphabets, i.e., reversed, French or Spanish, etc. Now when a line of cipher is "set" at the top,

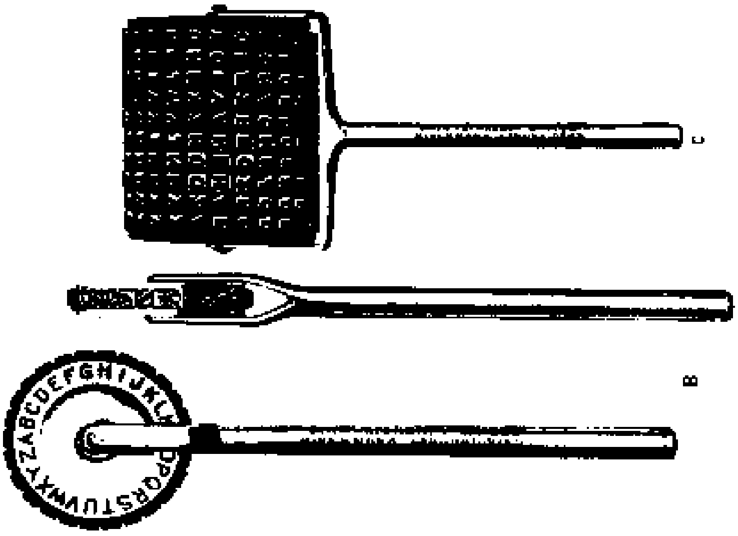
[1] De kwaliteit van Plate 1 in de copie waarvan deze heruitgave is gemaakt, is onvoldoende voor een zinvolle reproductie van het "Sliding Alphabet".

Fig. 1.

VIGÉNÈRE TABLE.

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

Plate 1



that is, when the sliding strips are moved so that a given number (up to twenty-six) of cipher-text letters are brought into one horizontal line, the successive horizontal lines of equivalents, called *generatrices*, are indicated automatically, and thus a vast amount of writing is eliminated. In an alphabet containing twenty-six letters, there are twenty-five generatrices, the twenty-sixth generatrix becoming identical with the letters at the starting point. The second device, the Poly-Alphabet Wheel, B, the idea for which the Riverbank Laboratories is indebted to Lieutenant P.H. Burdick, produces the same results. It makes use of a revolving rubber stamp containing the letters of the direct alphabet equally spaced on the perimeter of the wheel. In order to "run down" a series of cipher letters it is only necessary to start each column with the cipher letter which is to be "run down." The letters all being equidistant from each other, the successive letters all appear upon horizontal lines, or in other words, the successive generatrices are printed. This method possesses some advantageous features which the other does not, the most important being, first, that the apparatus is much smaller and can be carried about easily; secondly, that once a group of cipher letters is "run down," the results are permanently indicated and may be referred to or re-examined at any future time; and thirdly, since the letters are all movable, they may be arranged in accordance with any mixed alphabet sequence.

The third device, the Poly-Alphabet Roller, C, makes use of a series of ten endless rubber belts containing the letters of the direct alphabet equally spaced. These belts fit snugly upon the drum, but may be moved with reference to each other so as to contain ten cipher letters in one line. The device is then inked and rolled upon a sheet of paper.

From the above it follows that since all the letters of the first column have been enciphered by the same key letter, and are hence an equal distance removed from their respective plain-text letters, that the process of "running down" should produce one generatrix which will contain all of the plain-text equivalents for the cipher letters of this column. Hence, if the correct generatrix can be found for each column of the above series of messages, then the plain-text equivalents for each column and the decipherment of all of the messages are at hand. The problem thus resolves itself into the selection of the correct generatrix from among all the generatrices of each column. Since English text consists largely of the letters ETOANIRSHD, the generatrix sought in the case of each column will be the one which contains the greatest number or best assortment of these high-frequency letters.

The "running down" process in the case of the first three columns in the series of messages above gave the following generatrices:

It was necessary then to select from among these twenty-five generatrices for each column the correct generatrix. The generatrices which contain the greatest number of high-frequency letters, and therefore the most likely, are given in Table 4.

The letters in the generatrix which is to be chosen from among the possibilities of the first column generatrices, must be joined to the letters in the generatrix to be chosen fom among the possibilities of the second column generatrices; those of the second generatrix must be joined to those of the third, etc. Experiment is necessary to find the generatrices which will give the highest number of good combinations, remembering that these combinations must be the beginnings of words.[2] Not much delay will be experienced

[2] With respect to the correct generatrix of the first column, it should be borne in mind that, since the order of frequency of initial letters differs considerably from that of the interior of words, it will often happen that a generatrix containing a high percentage of E, A or O is not the correct one. The order of frequency of initial letters given by Hitt is T, O, A, W (B, C) (S,D). See: Hitt, Parker A., Manual for the Solution of Military Ciphers, 1916, p. 9.

TABLE 3.

GENERATRICES OF					
	Column 1		Column 2		Column 3
	Cipher letters		Cipher letters		Cipher letters
	VSZHOOGRBF		BANJERURRR		EXKHMKKEXL
1	WTAIPPHSCG	1	CBOKFSVSSS	1	FYLINLLFYM
2	XUBJQQITDH	2	DCPLGTWTTT	2	GZMJOMMGZN
3	YVCKRRJUEI	3	EDQMHUXUUU	3	HANKPNNHAO
4	ZWDLSSKVFJ	4	FERNIVYVVV	4	IBOLQOOIBP
5	AXEMTTLWGK	5	GFSOJWZWWW	5	JCPMRPPJCQ
6	BYFNUUMXHL	6	HGTPKXAXXX	6	KDQNSQQKDR
7	CZGOVVNYIM	7	IHUQLYBYYY	7	LEROTRRLES
8	DAHPWWOZJN	8	JIVRMZCZZZ	8	MFSPUSSMFT
9	EBIQXXPAKO	9	KJWSNADAAA	9	NGTQVTTNGU
10	FCJRYYQBLP	10	LKXTOBEBBB	10	OHURWUUOHV
11	GDKSZZRCMQ	11	MLYUPCFCCC	11	PIVSXVVPIW
12	HELTAASDNR	12	NMZVQDGDDD	12	QJWTYWWQJX
13	IFMUBBTEOS	13	ONAWREHEEE	13	RKXUZXXRKY
14	JGNVCCUFPT	14	POBXSFIFFF	14	SLYVAYYSLZ
15	KHOWDDVGQU	15	QPCYTGJGGG	15	TMZWBZZTMA
16	LIPXEEWHRV	16	RQDZUHKHHH	16	UNAXCAAUNB
17	MJQYFFXISW	17	SREAVILIII	17	VOBYDBBVOC
18	NKRZGGYJTX	18	TSFBWJMJJJ	18	WPCZECCWPD
19	OLSAHHZKUY	19	UTGCXKNKKK	19	XQDAFDDXQE
20	PMTBIIALVZ	20	VUHDYLOLLL	20	YREBGEEYRF
21	QNUCJJBMWA	21	WVIEZMPMMM	21	ZSFCHFFZSG
22	ROVDKKCNXB	22	XWJFANQNNN	22	ATGDIGGATH
23	SPWELLDOYC	23	YXKGBOROOO	23	BUHEJHHBUI
24	TQXFMMEPZD	24	ZYLHCPSPPP	24	CVIFKIICVJ
25	URYGNNFQAE	25	AZMIDQTQQQ	25	DWJGLJJDWK

TABLE 4.

MOST PROBABLE GENERATRICES OF					
	Column 1		Column 2		Column 3
	Cipher letters		Cipher letters		Cipher letters
	VSZHOOGRBF		BANJERURRR		EXKHMKKEXL
1	WTAIPPHSCG	9	KJWSNADAAA	3	HANKPNNHAO
12	HELTAASDNR	13	ONAWREHEEE	7	LEROTRRLES
13	IFMUBBTEOS	17	SREAVILIII	16	UNAXCAAUNB
20	PMTBIIALVZ	23	YXKGBOROOO	20	YREBGEEYRF

in finding that the 12th generatrix of the first column, the 13th of the second, together with the 7th of the third give the combinations already quoted on page **??**, and repeated below:

	1	2	3
1.	H	O	L
2.	E	N	E
3.	L	A	R
4.	T	W	O
5.	A	R	T
6.	A	E	R
7.	S	H	R
8.	D	E	L
9.	N	E	E
10.	R	E	S

As a further check the key letters in the case of these three columns are sought. There are three ways of finding the key letters. The first is by reference to a Vigénère Table; the second is by the use of two sliding direct alphabets; the third is by the use of the Sliding Poly-Alphabet referred to on Page **??**, or some similar device, by a method described below; and in all three cases a little experiment is necessary to determine which method of enciphering was used. There are eight different ways of using a Vigénère Table, but only three of them are encountered frequently enough to warrant mention, though the principles discussed in this booklet apply to all.

(1) The original Vigénère method, taking the cipher letter at the intersection of the vertical column determined by the key letter and the horizontal line determined by the plain-text letter in the first column on the left. Ex. Key M, plain-text S: cipher E.

(2) Proceeding down the key-letter column to the plain-text letter and following the horizontal line thus determined to the extreme left (the method first used by Beaufort). Ex. Key M, plain-text S: cipher G.

(3) Finding the plain-text letter in the first horizontal line, proceeding down the column thus determined to the row containing the key letter, thence out to the extreme left (another method devised by Beaufort). Ex. Plain-text S, key M: cipher U. This method gives exactly the same results as the sliding of a direct alphabet against a reversed, the principle used in the U.S. Army Disk, and will be discussed under section 2 on page 16.

Now all the alphabets resulting from the application of method (1) or (2) to the Vigénère Table may be produced more quickly by the use of two sliding direct alphabets. In the case of these two examples, the sliding alphabets would be in the position indicated below:

Beaufort, or Method (2) Key M, plain-text S: cipher G

```
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
            ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Vigénr̀e, or Method (1) Key M, plain-text S: cipher E