Journal of Criminal Law and Criminology

Volume 27
Issue 1 *May-June*

Article 6

Summer 1936

Cryptography in Criminal Investigations

Don L. Kooken

POLICE SCIENCE

Editor: FRED E. INBAU

CRYPTOGRAPHY IN CRIMINAL INVESTIGATIONS*

DON L. KOOKEN†

EXAMPLES OF DECIPHERING

Example 1:

TATMS TTABN EVRAK MONVI IIXBE LLIHN OBTOI
ALION AENAE OADLL NSENT SFORT BSERM TTAQH
TGRSO REDOL SEIEW EVESY RKRFE WOTWE EOEIN
NTACE QRGEE NANDT OOYCO LEYTN TCTOF OGRAT
UAHTE YTRIH

This cryptogram consists of one hundred and fifty letters. It is recognized as a transpositional cipher[1] because of the high frequency of the letters E, T, O, and A. Also, fragments of words are recognizable. For example, the second word TTABN reversed is NBATT, and coupled with the first word of the second line ALION it yields

* Concluded from previous issue. The reader will find it helpful to refer occasionally to the first part of this article, particularly to the frequency tables on pp. 907-909 (Vol. 26, No. 6).

† Supervising Lieutenant, Indiana State Police.

1 "Cryptograms may be roughly divided into two classes: transpositional and substitutional. In the former class the letters or words of the plain text are retained but are rearranged according to a prearranged plan so as to produce chaos. In the latter class the letters of the plain text are represented by other letters, numerals, characters, or symbols, according to a predetermined scheme or key. Since the method of analysis of the two classes will differ, the initial problem confronting the decodist is the determination of the class of cryptogram under examination." P. 906.

NBATTALION. The fifth word of the second line SFORT, the third word of the fourth line NANDT, and the last word YTRIH (reversed HIRTY), all indicate the transpositional cipher.

One hundred and fifty letters suggest rectangles 2 x 75, 3 x 50, 5 x 30, 6 x 25, or 10 x 15. The interval between the words TTABN and ALION is thirty letters. The same interval is noted between the words NANDT and YTRIH. The message is accordingly rewritten in the form of a rectangle 30 x 5, thus:

```
TATMS TTABN EVRAK MONVI IIXBE LLIHN
OBTOI ALION AENAE OADLL NSENT SFORT
BSERM TTAQH TGRSO REDOL SEIEW EVESY
RKRFE WOTWE EOEIN NTACE QRGEE NANDT
OOYCO LEYTN TCTOF OGRAT UAHTE YTRIH
```

Referring to the second column of words beginning with the word TTABN we note that by reading the horizontal lines alternating between the reverse and normal order, we obtain: "N BALTALION HQ AT TWO TWENTY EL." An examination of the first column of words soon discloses that it is read by following the vertical lines first down and then up. This column reads: "TO BROOKS BATTERY C FROM SIMEO."

The third column of words was found to have been written following the alternate diagonal pattern—EVATE RANGE TO RAKE SECTION OF. In the fourth column the words MONVILLE and ROAD are immediately recognized and it is soon discovered that this column has been written by means of a spirial pattern—MONVILLE TARGON ROAD LOCATED. The fifth column is found to follow the pattern of column one—IN SQUARE SIX EIGHTEEN BETWEE, and column six has been written in the same manner as column two—NHILLS FORTY SEVEN AND THIRTY. The message reads, therefore: "To Brooks Battery C, From Simeon Battalion Hq. At two twenty elevate range to rake section of Monville Targon road located in square six eighteen between hills forty seven and thirty."

Example 2:

```
2442 6352 5564 1534 2414 1532 3214 1234 1514 6463 1322 1214
5342 4214 5342 5114 2364 1263 2464 6324 1442 6354 5351 4324
6424 4242 6113 4343 5114 1353 5442 3413 5143 1524 4224 5351
4343 6251 3425 4234 5513 5354 6434 1451 6314
```

The above message was transmitted by telegraph and consisted of forty-five groups of four figures each, or a total of one hundred

and eighty numerals. The numerals used are from one to six. Apparently two or more numerals are used to represent each letter of the plain text. One hundred and eighty is divisible by two, three, and four; therefore we will first re-write the message by dividing it into groups of two figures each:

24 42 63 52 55 64 15 34 24 14 15 32 32 14 12 34 15 14 64 63 13
22 12 14 53 42 42 14 53 42 51 14 23 64 12 63 24 64 63 24 14 42
63 54 53 51 43 24 64 24 42 42 61 13 43 43 51 14 13 53 54 42 34
13 51 43 15 24 42 24 53 51 43 43 62 51 34 25 42 34 55 13 53 54
64 34 14 51 63 14

An examination of this grouping discloses that there are twenty-one different pairs of two figures each. The frequency of their use is as follows:

Pairs	Times Used	Pairs	Times Used
12	3	42	10
13	5	43	6
14	10	51	7
15	4	52	1
22	1	53	6
23	1	54	3
24	8	55	2
25	1	61	1
32	2	62	1
34	6	63	6
		64	6

It is noted that the initial digits of the pairs are from one to six and that the final digits are from one to five. This fact suggests a rectangular table 5 x 6 which would provide space for the representation of thirty characters, thus:

	1	2	3	4	5	6
1						
2						
3						
4						
5						

The pairs 14 and 42 each are used ten times and either pair can represent the letter E.[2] It is noted that the pairs 11, 21, 31, and 41 are not used, and if we blank the squares on the above table indicated by these pairs we will have twenty-six squares left in which

[2] See frequency table, p. 907.

to place the letters of the alphabet. The pair 51 occurs seven times which is favorable to the letter A. If we place the letter A in square 51, B in square 61, and drop down to the second line writing in the letters C, D, E, F, G, and H from right to left the letter E will fall into space 42. Continuing in this manner, alternating the order with each line, the following table is formed:

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

With this table the solution of the message is found to be: "Send your stuff thru tonight. Meet me at Johnsons ten p. m. Also see Bill at Imperial. Use small car. Very important."

The message could have been solved by following the popular method for the solution of substitution ciphers, that is, by consideration of the frequency of pairs. The choice of digits, however, so clearly indicated that a table had been used that the reconstruction of the table provided a short cut to the solution.

Example 3:

SAWT NIEM EHGI YAMG
NOVU AELN EUTO SUAT
SCTR HESE RIED OEME
AAXP RDAL ECTY ETZR

The above message was intercepted en route to a person suspected of being involved in a smuggling ring. A frequency count indicated that the message was of the transpositional class and the total of sixty-four letters suggested rectangles of 2 x 32, 4 x 16, or a square 8 x 8. However, the distribution of vowels in the rectangles did not appear favorable, and because of the square 8 x 8 we are of the opinion that a grille had been used.[3]

The message should be inscribed in the form of a square and the

[3] See example of grille on p. 911.

outline of the square divided into sixty-four equal spaces, inscribed on a piece of tracing paper:

1 2

S A W T N I E M

E H G I Y A M G

N O V U A E L N

E U T O S U A T

S C T R H E S E

R I E D O E M E

A A X P R D A L

E C T Y E T Z R

4 3

The corners of the square on the tracing paper are numbered to correspond with those on the foregoing message. Scanning the first line of the square we note the letters WE. This is a logical word to start a message so the squares in which these letters occur are checked on the tracing with black pencil. The tracing is now given a half turn bringing corner 3 of the tracing to coincide with corner 1 of the message. The checked squares show the letters CT. Scanning the 7th line for the letter to precede CT we are attracted by the letters XA suggestive of the word EXACT. Line 6 has three Es so we omit checking the letter E for the present and check only the squares XA. This checking in this position is done with red pencil.[4] Returning the square to original position we find that the red-checked squares cover the letters HA. Looking to line three we are attracted by the letters VE which will complete the word HAVE. These squares are checked with black pencil. Again turning the tracing paper a half turn, we obtain the E for completing EXACT. We also note that in line five the word THE appears. However, there are too many Es, so by checking back we determine that the E in the word HAVE occurs in line 4 instead of line 3. This correction is then made and we check with red pencil the squares in which the letters TH appear. We now bring corner 2 of the tracing over corner 1 of the message and in the squares checked in black and red we have E OU R REA Y. This suggests YOU ARE

[4] The different colors are used in checking so that the position of the openings in the grille can be determined for each of its four positions.

READY and the letters Y A E and D are checked in with a green pencil.

Turning the tracing another half turn we have NGMENTS COMPL which immediately suggest the words "Arrangments[4a] complete" and we check the additional letters A in the first line and ETE in the last line, using a brown pencil for this purpose. Returning the tracing to its original position we now find that we have the grille completed, and by turning one quarter turn at a time we read: "We have outside arrangments complete. Signal us the exact time you are ready Z."

Example 4:

FBOJG MJZTU ALWKM SBWAS NBJDU JLWAG BABAA WAMKW EKMPM ANBOJ
AUOST QQBLU FWQDU KAMZM KKUJF QBGUY MBAMK OVKQW QOQWB AWAFB
OJBJL MJQTM KOVKQ WQOQM LSBBL KUQKU GMCJW ZMDMI OBQML NBJQT
MSBBL KBJLM JMLEF

The foregoing message of 165 letters appears to be a substitutional cipher because of the large number of low frequency letters. A frequency count gave the following result:

Letters	Times Used	Letters	Times Used
A	13	N	3
B	19	O	9
C	1	P	1
D	3	Q	14
E	2	R	0
F	5	S	5
G	4	T	4
H	0	U	9
I	1	V	2
J	13	W	11
K	11	X	0
L	10	Y	1
M	19	Z	3

According to this table, either B or M may represent the letter E,[5] but scanning the message for trigrams ending in B and M, which would represent the word THE, we find there are no duplications of a trigram ending in B, while the trigram QTM occurs twice. Therefore we will assume that Q equals T, T equals H and M equals E. An examination of the frequency table substantiates this assumption. B is the letter of next highest frequency and we will

[4a] The word "arrangements" was misspelled in the message; hence "arrangments."

[5] See frequency table, p. 907.

temporarily place it as equal to the letter O. We next note the combination MJ preceding the word QTM (the) in the 22nd word of the message. As this is apparently a word ending and the common letter paired with E in word endings is the letter R we will assume that J equals R. This selection is borne out by the fact that J occurs thirteen times, which is about right for the letter R. Making these subsitutions we are next attracted by the combination FB OJBJL MJQTM (-O-ROR-ERTHE). It requires but little imagination to make of this combination YOUR ORDER THE and we now have F equal to Y, O equal to U and L equal to D. The substitutions are made and we now note the combination of the last four words; with substitutions made they are THE-OOD-ORDERED. It is very plain that S equals G and K equals S. Making the additional substitutions we now note two similar combinations in the 17th, 18th, and 19th and the 23rd, and 24th words. These are KOVKQWQOQWB and KOVKQWQOQML with substitutions made they are S- -ST-TUT- and S- -ST- TUTED these are plainly the words SUBSTITUTION and SUBSTITUTED. We now have O equals U, V equals B, W equals I and A equals N. After making these substitutions the other letters of the message are self evident and the complete encipherment is: "Your merchandise going forward in Monon nine six seven four naught today. It was necessary to make one substitution in your order, the substituted goods at same price we quoted for the goods ordered. XY."

Example 5:

ETBRC ULOMT SCHTN RHNOR XSOUE FESWO DCHAE SALTG
ROTRS ORGOH USIKO ODIRN HENCF RNWAW DCYAO TIFOX
NSGSR MCLDI IATRG TBGRR

The above message was taken from the person of a bootlegger. It consists of 100 letters and a frequency count resembles the normal English frequency; therefore it is concluded that it is a transposition cipher. The vowel count and the count of common consonants likewise bear out this fact. The number of letters (100) suggests rectangles of 2 x 50, 4 x 25, 5 x 20 and 10 x 10. Of these factors 10 appears to be one of the most likely combinations to serve as a key for transposition. Therefore, we arrange the message in a square of ten letters as follows:

(1) E T B R C U L O M T
(2) S C H T N R H N O R
(3) X S O U E F E S W O

(4) D C H A E S A L T G
(5) R O T R S O R G O H
(6) U S I K O O D I R N
(7) H E N C F R N W A W
(8) D C Y A O T I F O X
(9) N S G S R M C L D I
(10) I A T R G T B G R R

Since the vowel count indicates that the vertical columns are near normal, we must rearrange the horizontal lines. Examining the first column we note the letter X in line 3, I in line 10, S in line 2, all of which could combine to form the word SIX. In this same order, and in the same relative positions, the other vertical columns yield CAS, HTO, TRU, NGE, RTF, HBE, NGS, ORW, and RRO. These look favorable as parts of words. Examining the remaining letters in column one we find that we can form the word HUNDRED. This provides the arrangement of all the lines except lines 4 and 8, both of which begin with the letter D. However, an examination of succeeding columns soon indicates that line 8 belongs last and that the order or transposition of horizontal lines is in this order, 2, 10, 3, 7, 6, 9, 4, 5, 1, 8. The rearranged square is now:

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

Reading down the vertical columns the message is: "Six hundred cases scotch tonight by trucks. Arrange for escort from South Bend. Carlings will go forward tomorrow night. X."

Example 6:

UFDQM BLFXF DFZKC GCHVN DFCFZ GNHFW KBVNE VUFCN
BWHTN OCCNO VFRBR UJCIK EEDQM WABUF NSURB YQETB
VBEIR JEVBU RUHFE FNBJV BNFMQ FXJNB EMUFE VBGGH
FOMBT PGHMC QSTFJ DMDUI XOVYD FRHEU GPBUB HFJCN
FEPGA CQKUC BFQFC GGCGD ALGSM JEVNC EVBUN OBNPI
ATBMQ

This message containing 205 letters was taken from the person of a man suspected of operating with a band of bank robbers. A frequency count disclosed the following:

Letters	Times Used	Letters	Times Used
A	4	N	14
B	19	O	5
C	14	P	4
D	8	Q	8
E	13	R	6
F	22	S	3
G	11	T	5
H	8	U	13
I	4	V	11
J	7	W	3
K	4	X	3
L	2	Y	2
M	9	Z	2

The abnormal frequency count suggests that the message is of the substitutional class. From this count it appears that more than one alphabet has been used. This conclusion is reached because the letter of highest frequency "F" occurs only 22 times. In a message of this length the letter "E" should occur at least 30 times. We also note that the letters C, E, G, N, U, and V all occur between 11 and 14 times, while in a normal table we should not have more than five letters in this range. Therefore, we will examine the message for repeated digrams, trigrams, and telvagrams. We find the digram BU occurring 4 times; EV five times; HF four times; UF four times; and VB five times. EVBU and JEV each occur twice. The following tabulation of the intervals between repeated groups is made:

EVBU to EVBU.104, or 2x2x2x13
JEV to JEV.....100, or 2x2x5x5
BU to BU..... 21, or 3x7
BU to BU..... 64, or 2x2x2x2x2x2
BU to BU..... 40, or 2x2x2x5
EV to EV..... 52, or 2x2x13
EV to EV..... 28, or 2x2x7
EV to EV..... 72, or 2x2x2x3x3
EV to EV..... 4, or 2x2.

HF to HF.....65, or 5x13
HF to HF.....27, or 3x3x3
HF to HF.....36, or 2x2x3x3
UF to UF.....32, or 2x2x2x2x2
UF to UF.....44, or 2x2x11
VB to VB..... 7, or 1x7
VB to VB.....12, or 2x2x3
VB to VB.....16, or 2x2x2x2
VB to VB.....76, or 2x2x19

Since the factor 2 x 2 is common to the majority of the intervals counted, it is concluded that four different alhpabets have been used. The message should be re-written in lines of four letters each, the lines being numbered for the purpose of reference:

	a	b	c	d		a	b	c	d		a	b	c	d		a	b	c	d
(1)	U	F	D	Q	(14)	R	B	R	U	(27)	Q	F	X	J	(40)	F	J	C	N
(2)	M	B	L	F	(15)	J	C	I	K	(28)	N	B	E	M	(41)	F	E	P	G
(3)	X	F	D	F	(16)	E	E	D	Q	(29)	U	F	E	V	(42)	A	C	Q	K
(4)	Z	K	C	G	(17)	M	W	A	B	(30)	B	G	G	H	(43)	U	C	B	F
(5)	C	H	V	N	(18)	U	F	N	S	(31)	F	O	M	B	(44)	Q	F	C	G
(6)	D	F	C	F	(19)	U	R	B	Y	(32)	T	P	G	H	(45)	G	C	G	D
(7)	Z	G	N	H	(20)	Q	E	T	B	(33)	M	C	Q	S	(46)	A	L	G	S
(8)	F	W	K	B	(21)	V	B	E	I	(34)	T	F	J	D	(47)	M	J	E	V
(9)	V	N	E	V	(22)	R	J	E	V	(35)	M	D	U	I	(48)	N	C	E	V
(10)	U	F	C	N	(23)	B	U	R	U	(36)	X	O	V	Y	(49)	B	U	N	O
(11)	B	W	H	T	(24)	H	F	E	F	(37)	D	F	R	H	(50)	B	N	P	I
(12)	N	O	C	C	(25)	N	B	J	V	(38)	E	U	G	P	(51)	A	T	B	M
(13)	N	O	V	F	(26)	B	N	F	M	(39)	B	U	B	H	(52)	Q			

A frequency count of the four columns (a, b, c, d) is as follows:

	a	b	c	d
A	3	0	1	0
B	7	5	4	4
C	1	6	6	1
D	2	1	3	2
E	2	3	8	0
F	4	11	1	6
G	1	2	5	3
H	1	1	1	5
I	0	0	1	3
J	1	3	2	1
K	0	1	1	2
L	0	1	1	0
M	5	0	1	3
N	5	3	3	3
O	0	4	0	1
P	0	1	2	1
Q	4	0	2	2
R	2	1	3	0
S	0	0	0	3
T	2	1	1	1
U	6	4	1	2
V	2	0	3	6
W	0	3	0	0
X	2	0	1	0
Y	0	0	0	2
Z	2	0	0	0

According to the frequency count B should be the letter E in column *a;* F in column *b,* E in column *c,* and F or V in column *d.*

However, in considering individual columns the frequency cannot be depended upon to any great degree, because the separation of the plain text into four parts will often bring about an uneven distribution of the letters. Therefore, we will examine the repeated digrams and trigrams:

EV is found repeated five times in columns *c* and *d*, considered together. If we assume that EV represents TH of the plain text, then E in column *c* equals T, and V in column *d* equals H. We now note that B in column *a* follows EV in lines 23, 30, and 49. As B is the letter of highest frequency in column *a* we can assume that it represents the letter E in that column. We now have one letter in each of the columns *c*, *d*, and *a*. Turning to column *b* we tentatively select F (the letter of highest frequency) to represent E and we note that the digram FD occurs in lines 1 and 3 and the digram FC occurs in lines 6, 10, and 44. According to normal frequency FC should represent ER and FD should represent EN. We now have the following:

PLAIN TEXT

		a	b	c	d
E	equals	B	F		
T	"			E	
H	"				V
R	"			C	
N	"			D	

With the above letters tentatively identified we try Vigenere's table[6] without satisfactory results. Beaufort's table[7] likewise fails to produce a solution. Porta's table[8] is not considered for in column *a*, E is equal to B and both letters are in the same half of the alphabet which never occurs in ciphers where Porta's table is used. It is apparent that irregular alphabets have been used. We return, therefore, to the examination of the message, first substituting the letters already identified. With these letters already identified, in column *c* the letter of next highest frequency is G, occurring 5 times. We will assume it to be the letter E and make the substitutions accordingly. We note that the digram GH occurs twice in lines 30 and 32. Assuming this to be EN will make H in column *d* equal to N. The next combination that attracts attention is UenQ in line 1, verN in line 10, vsNS in line 18. The letter U in the first

[6] See pp. 912-916.
[7] See pp. 915, 916.
[8] See p. 914.

column must be a consonant. The consonants most frequently preceding E and R and S. The frequency table would favor S, and therefore the first line becomes senQ. The frequency table indicates that Q occurs twice in column *d*. This suggests Q as representing D. Making this substitution we now have in line 16 EEnd, and we are tempted to substitute A for E in column *b*. Tabulating our substitutions at this point we have:

		a	b	c	d
E	equals	.	B.	F.	G
T	"	.			E
H	"	.			V
R	"	.			C
N	"	.			D.
A	"	.	E		
S	"	.	U		
D	"	.			Q

Referring to line 10 (serN) and line 11 (eWHT), N of column *d* suggests I, and W of column *b* suggests S, completing "series HT." Line 8 (FsKB) and line 9 (VNth) immediately preceding "series" must be the word "fourth." This gives us K of column *c*, equal to F, B of column *d* equal to O, V of column *a* equal to U, and N of column *b* equal to R. These substitutions are made throughout the message. It takes but little imagination to make line 7 (ZGNn) and line 8 (Fsfo) equivalent to Zbon and dsfo. From that point working backward we have lines 5 (CHVi), 6 (DerF), and 7 (Zbon) reading Chli bert ybon. Returning now to the beginning of the message, lines 1, 2, and 3 (sendMBLtXenty) suggests "sending twenty," while lines 16, 17, and 18 (EandMsAoseoS) become cand ispo seof. Line 20 (QaTo) and line 21 (untI) will read Qamo unts by substituting M for T in column *c*, and S for I in column *d*. Line 4 (yKrG) and line 5 (CHli) comprise a five letter word to complete "sending twenty KrG H liberty bonds." K of column *b* is used only once; G of column *d* occurs three times; C of column *a* is used but once; and H of column *b* occurs only once. It is here that a knowledge of the special situation surrounding the interception aids in the solution. Criminals, and bank robbers in particular, use the word "grand" to mean $1000. Therefore we have KrGCH representing "grand." This then makes K of column *b* equal to G, G of column *d* equal to A, C of column *a* equal to N, and H of column *b* equal to D. Making these substitutions we now pass on to lines 11 (esHt), 12 (NOrC), and 13 (NOlt). The HT in line 11 suggests BY, and it is now apparent that NO equals ai, and that C

in column *d* represents M. Continuing on, the balance of the message is soon deciphered. The solution is as follows: "Sending twenty grand Liberty bonds fourth series by air mail tonight. We can dispose of small amount of the Liggett and Hercules. Can't use the Bendix or Zenith Fredericks. Will be in Cleveland Friday at the Statler; after the fifth at the Lowrey, St. Paul." And the four cipher alphabets used were as follows:

	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
1st	N	D	E	F	B	G	H	J	M			Q		C	R		S	T	U	A	V		X	Y		I
2nd	E	G	D	H	F	J	K	L	O	Q	S	U	R	B	A	T		N	W	C					.	P
3rd	B	H	F	J	G	K	L	Q	R		U	V	T	D	N	A		C	X	E			I	M	P	
4th	G		J	Q	K	S	U	V	N			Y	C	H	B			D	I	F	M	P	O		T	

It is noted that KL of the third cipher alphabet is one space to the left of the same letters in cipher alphabet two. This is also true of the letters U and P, while in cipher alphabet four the letters UV and MP are each three spaces to the left of the same letters in cipher alphabet three. This indicates the modified Vigenere's square.[9] As we expect to intercept more messages from the same source we attempt to reconstruct the primary alphabet. It is noted that IMP in cipher alphabet three represents WXY, while in cipher alphabet four MPO T represents UVW Y. Combining, we have IMPO T. Then:

	Plain Text	Cipher Text
Third letter cipher alphabet.....	IMPO T	equals RTAN E
Second letter cipher alphabet.....	IMPO T	equals ORTA C

A further combination results in IMPORTANCE. The primary alphabet, therefore, was: IMPORTANCEBDFGHJKLQSUVWXYZ.

The table or square constructed from the above primary alphabet would be as follows:

[9] See p. 912.

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

Example 7:

If the reader is in doubt as to exactly how a knowledge of the circumstances surrounding the enciphering of a message may facilitate its solution, the following example will serve to illustrate that point . In this case a cryptogram was given the writer by a friend who was a typewriter dealer, and who stated that the message had been enciphered by means of a system of his own invention. The cryptogram was as follows:

YJODP ODIRM VOQJR TRFPO MCSMZ SMMRT PBRTU CRSDU
MYPCZ RZPTO XRISM FURWI SAAUM RSDUJ YPFRV OQJRT

The message consisted of eighty letters, with the following frequency count:

```
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 1 3 4 0 2 0 0 3 4 0 0 8 0 6 6 2 12 6 5 5 2 1 1 3 3
```

In a short message we may expect some deviation from the normal frequency of letters as indicated by the above table. Yet it is apparent that the message is a substitution cipher and we will look to recurring diagraphs, particularly those which may represent ER and EN.

The digrams RT and SM occur three times. The letter R occurring twelve times must be the letter E and the most frequent letter paired with E is R which would make RT equal ER. We note here that the letters R and T are immediately adjacent to the letters E and R on the standard typewriter keyboard. With the knowledge that the message had been prepared by a typewriter dealer we are tempted to try the first few letters of the cryptogram by comparison with the standard typewriter keyboard, taking as the plain text letter the letter immediately to the right of the cipher letter.[10] The first five letters YJODP yields Thiso. Continuing in the same manner we obtain:

Thiso isuen ciphe redoi nxanm anner overy xeasy
ntoxm emori zevan dyequ allyn easyh todec ipher

The italicized letters were nulls introduced between words. Eliminating these the message reads: "This is enciphered in a manner very easy to memorize and equally easy to decipher."

The method used was to substitute for each letter of plain text the first letter to the right and in the same line on the typewriter keyboard. For the plain text letters P, L, and M, which are the finals in the three rows of letters on the keyboard, the initial letters Q, A and Z were substituted.

Telephone Number Ciphers

Example 8:

The use of ciphers for recording telephone numbers is frequently encountered in criminal investigations. The methods used will range from the simple transposition to very complex combinations of transposition and substitution. The large scale operations of organized criminal bands necessitates an extensive use of the telephone, and every precaution is taken to preserve the secrecy of the numbers used. Telephone numbers are valuable as leads to

[10] The standard typewriter keyboard is as follows:

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

the police officer investigating the activities of an organized criminal band. When Ted Newberry, a notorious Chicago gangster, was killed near Chesterton, Indiana, in 1932, a small note-book was found on his person, the contents of which constituted a cipher. Cipher experts of the Chicago Police Department set to work upon the cipher and soon found it to be a complete telephone directory of the syndicate of which Newberry was the head.

The system followed in the Newberry cipher was one of substitution combined with simple transposition. Certain letters were substituted for the digits of the telephone number and then the order was reversed. It is customary to use a key word of ten letters to substitute for the digits 1 to 0. However, in this instance an incoherent key was used. It is interesting to note that in making the selection of letters to be used, Newberry had selected letters that closely resembled the numbers to be represented. His key was as follows:

1	2	3	4	5	6	7	8	9	0
I	V	E	Y	P	G	Z	H	B	O

The letter I is identical with the Roman numeral I which it was used to represent. The lower case V greatly resembles the written figure 2 and the letter E reversed becomes the figure 3, the lower case Y is similar to the figure 4 and the contour of the upper case P inverted conforms to that of the figure 5. The letter G becomes a figure 6 while the letter Z with lower bar removed becomes the numeral 7. The letter H with top and bottom closed becomes the figure 8, the small letter B inverted closely resembles a figure 9 and 0 is identical with zero.

Example 9:

In the simple forms of telephone cipher the letters denoting the exchange are left in plain text and only the telephone numbers proper is enciphered. The method most frequently encountered is to reverse the number; for example, Jackson 2345 would be enciphered Jackson 5432. A number of four digits may be arranged into twenty-four different combinations, and if letters or characters are substituted for the digits before transposition, it is readily seen that the problem of decipherment becomes more difficult.

If the dialing letters of the exchange are reduced to their numerical value according to their position on the dial and included in the transposition the number of possible combinations are greatly

increased. Where two letters are used for dialing purposes, reducing them to their numerical value produces a number of six digits with 720 possible combinations and where three dialing letters are used resulting in a seven digit number the number of possible combinations is increased to 5040.

The following table indicates the numerical value of the standard telephone dial:

ABC	=	2
DEF	=	3
GHI	=	4
JKL	=	5
MNO	=	6
PRS	=	7
TUV	=	8
WXY	=	9
Z	=	0

Thus the exchange letter FRA would equal 372.

The method of attack in the solution of telephone ciphers differs considerably from that employed in the solution of an ordinary cryptogram. In most instances notations are made before and after the enciphered number to identify the subscriber and they often furnish sufficient lead to enable the investigating officer to arrive at a quick solution. However, in the absence of any notation or marks of identification the investigating officer must proceed along different lines. A knowledge of the circumstances surrounding the acquisition of the enciphered numbers and all facts regarding the character and activities of the person from whom the cipher was taken are essential. From these facts and circumstances certain known telephone numbers are selected as most likely to be included, and the attack is from that direction. For example, the following list of numbers were taken from a prisoner (the line numbers and column letters being used for reference purposes only, and not constituting a part of the cipher):

	Cipher						
Line	a	b	c	d	e	f	g
(1)	3	2	2	6	7	8	3
(2)	9	3	7	8	2	1	4
(3)	4	2	7	1	2	6	4
(4)	8	9	2	7	2	9	5
(5)	4	8	3	8	3	3	7
(6)	8	1	2	9	4	1	2
(7)	8	4	2	1	2	1	9
(8)	3	2	6	3	2	2	8
(9)	8	9	5	6	8	2	2

(10) 1 4 6 6 2 8 8
(11) 3 2 2 1 7 6 3
(12) 8 2 6 6 2 4 7

The list of twelve numbers are without marks of identifications. Each number consists of seven digits. The prisoner was operating in a city where three dialing letters are used. From the available information as to the activities of this individual the number ATL 8962 was selected as one most likely to appear in the cipher.

The numbers of the cipher are first rearranged with the digits placed in their conventional order:

	Plain Text						
Line	a	b	c	d	e	f	g
(1)	2	2	3	3	6	7	8
(2)	1	2	3	4	7	8	9
(3)	1	2	2	4	4	6	7
(4)	2	2	5	7	8	9	9
(5)	3	3	3	4	7	8	8
(6)	1	1	2	2	4	8	9
(7)	1	1	2	2	4	8	9
(8)	2	2	2	3	3	6	8
(9)	2	2	5	6	8	8	9
(10)	1	2	4	6	6	8	8
(11)	1	2	2	3	3	6	7
(12)	2	2	4	6	6	7	8

Then the suspected number is reduced to a seven digit figure by changing the exchange letters to their numerical value and we have ATL 8962 = 2858962. Rearranging the digits in their numerical order we have 2256889. Comparing with the rearranged table we find line 9 to be identical; therefore ATL 8962, or 2858962, is enciphered 8956822.

To determine the order of transposition we first eliminate those digits in plain text 2 8 5 8 9 6 2 and of cipher text 8 9 5 6 8 2 2 that occur but once, naamely the digits 5, 6, and 9.

a b c d e f g	Plain text column *c* equals cipher text column c
2 8 5 8 9 6 2	Plain text column *f* equals cipher text column *d*
8 9 5 6 8 2 2	Plain text column *e* equals cipher text column *b*

This may be expressed as follows:

Plain text columns	*a*	*b*	*c*	*d*	*e*	*f*	*g*
Cipher text columns			*c*		*b*	*d*	

Next considering the digit 8, which occurs twice in columns *b* and *d* of the plain text and in columns *a* and *e* of the cipher text, we note that 8 is the second number of the plain text and is a part of the

reduced exchange letters. Inasmuch as the numeral 1 never occurs in the digits representing the exchange, we examine the two columns of cipher text in which the numeral 8 occurs on line 9 and find that in column *a* we have the numeral 1 in line 10; therefore, this column cannot be either column *a*, *b*, or *c* of the plain text. Referring to column *e* of the cipher text, where the second numeral 8 of line 9 appears, we find this column does not contain the numeral 1; therefore, after checking line 9 of the cipher and as rearranged, cipher column *e* becomes column *b* of the plain text, and cipher column *a* becomes column *d* of the plain text.

Therefore:	Plain text columns	*a b c d e f g*
	Cipher text columns	*e c a b d*

The two numerals 2 and 2 are still to be placed. By the same reasoning followed thus far, cipher column *g* is selected as plain text column *a*, because of the absence of the numeral 1 in this column. Then cipher column *f* becomes plain text column *g*.

Therefore:	Plain text columns	*a b c d e f g*
	Cipher text columns	*g e c a b d f*

The solution of the cipher is:

Line		
(1)	FRA	3268
(2)	HAR	9381
(3)	HAR	4216
(4)	JAC	8979
(5)	SEE	4883
(6)	CIC	8191
(7)	WAB	8411
(8)	VAN	3232
(9)	ATL.	8962
(10)	VAN	1468
(11)	FRA	3216
(12)	RAN	8264

Example 10:

The following hypothetical example will illustrate the method of decipherment when letters are substituted for the numerals.

	Cipher						
Line	1	2	3	4	5	6	7
(1).....	Y	H	T	E	Y	A	Y
(2).....	T	S	Y	H	P	C	Y
(3).....	I	E	H	C	H	C	I
(4).....	H	H	A	C	P	Y	A

(5).....H T P M T P E
(6).....P T P E H A E
(7).....H T E E S A A
(8).....Y S E H Y E E
(9).....H T E M Y E H
(10).....Y E T H A S M
(11).....A E I S E T P
(12).....C T Y M T A E
(13).....A A H E T A H

Among the numbers suspected of being in this list we select PUL 6703 as most likely to appear. Reducing the dialing letters to their numerical value we have PUL 6703 equals 7856703.

The numeral 7 is the only one repeated, appearing as digits 1 and 5. Examining the cipher we find only two lines where the 1st and 5th digits are represented by the same letter number; namely lines one, and eight. But in line one the letter Y occurs 3 times and in line eight the letter E occurs three times. Several other suspected numbers are tried with no result. We conclude, therefore, that the method is one in which substitution is combined with transposition. The cipher is then re-written by arranging the letters in each line in the order of the number of times used in each line:

(1).....Y Y Y H T E A
(2).....Y Y T S H P C
(3).....I I H H C C E
(4).....H H A A C P Y
(5).....T T P P H M E
(6).....P P E E T H A
(7).....E E A A H T S
(8).....E E E Y Y S H
(9).....H H E E T M Y
(10).....Y E T H A S M
(11).....E E A I S T P
(12).....T T C Y M A E
(13).....A A A H H E T

Returning to our suspected number PUL 6703, or 7856703, and arranging the digits in the order of their occurrence we have 7785603. Again referring to the cipher we find either line 2 (YYTSHPC), line 11 (EEAISTP), or line 12 (TTCYMAE) could equal the suspected number.

A second suspected number AUS 6227 is selected and reduced to a seven digit number, 2876227, and then rearranged according to

recurrence of digits 2227786. Checking this number against the rearranged table, we find that line 8 (EEEYYSH) and line 13 (AAAHHET) are the only ones that could equal the suspected number.

A comparison is now made between the two suspected numbers 7785603 and 2227786. It is noted that the pair 77 occurs in both. Comparing the lines YYTSHPC, EEAISTP, and TTCYMAE with the lines EEEYYSH and AAAHHET, we find that line 2 (YYTSHPC) and line 8 (EEEYYSH) are the only ones with a common pair (YY). Therefore:

Line 2 (YYTSHPC) = 7785603
Line 8 (EEEYYSH) = 2227786

The next step is to reconstruct the key word. The ten letters used in the cipher are A C E H I M P S T Y. Obviously E equals 2, and Y equals 7. Also, the S H must represent 6 8. This leaves T P C, the equivalent of 5 0 3. The remaining letters M A I apparently represent 1 4 9. With the vowel E as the second letter, we look for a consonant as the first letter and have the group M A I from which to select. Therefore M is chosen as the equal of the numeral 1, leaving A I equal to 4 9. Attention is next directed to S H equals 6 8. With Y already established as equalling 7, we have either S Y H or H Y S equalling 6 7 8. Since the latter looks the more promising, we tentatively consider H to equal 6 and S to equal 8. In the selection of the fifth letter we have the group T P C. The letter P seems most likely to combine with the group H Y S, which leaves T C equalling 0 3. Tabulating the results thus far we have:

```
1 2 3 4 5 6 7 8 9 0    A I = 4 9
M E     P H Y S        T C = 0 3
```

With but two alternatives left for each of the four remaining spaces it is not difficult to complete the key word, which is:

```
1 2 3 4 5 6 7 8 9 0
M E T A P H Y S I C
```

Again returning to the cipher and substituting the proper numerals for the letters of the cipher, we have:

```
(1)   7 6 3 2 7 4 7
(2)   3 8 7 6 5 0 7
(3)   9 2 6 0 6 0 9
(4)   6 6 4 0 5 7 4
(5)   6 3 5 1 3 5 2
(6)   5 3 5 2 6 4 2
```

(7)	6	3	2	2	8	4	4
(8)	7	8	2	6	7	2	2
(9)	6	3	2	1	7	2	6
(10)	7	2	3	6	4	8	1
(11)	4	2	9	8	2	3	5
(12)	0	3	7	1	3	4	2
(13)	4	4	6	2	3	4	6

Comparing the two suspected numbers with this table we have:

Plain Text		Cipher Text
7856703	=	3876507
2876227	=	7826722

A comparison of the columns of the plain text with those of the cipher text indicates that:

Plain Text Columns		Cipher Text Columns
1	equals	3 or 7
2		2
3		5
4		4
5		3 or 7
6		6
7		1

As cipher column 7 contains the numeral 1 in line 10 it is eliminated as a part of the dialing letters and therefore must represent column 5 of the plain text. Consequently the order of transposition is:

Plain text columns	1	2	3	4	5	6	7
equal							
Cipher text columns	3	2	5	4	7	6	1

Transposing according to this formula and reducing the first three numerals to their letter equivalents the solution is:

DOR	2747
PUL	6703
MAN	0909
HOL	0476
KED	1256
KEN	2245
BEV	2446
AUS	6227
BER	1626
FAI	6187
WAB	8334
SEE	1240
MID	2644