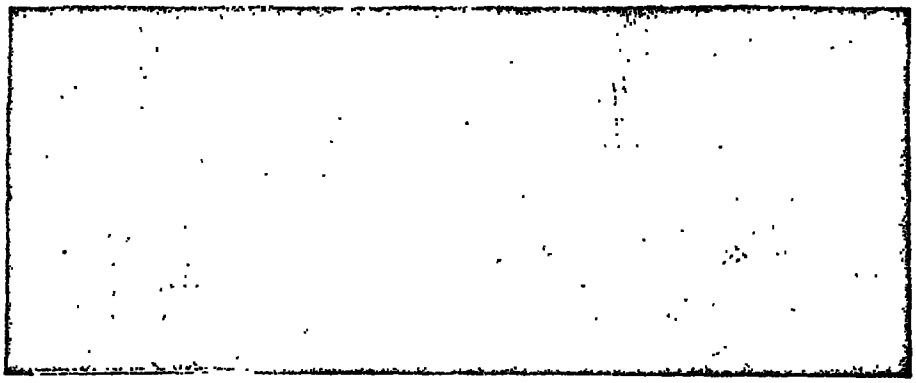
Cryptograms and Their Solution



The Masonic Cipher, Said to Have Been Used by the Freemasons

By HERBERT O. YARDLEY

THE arts of transmitting messages secretly are manifold and many of them are of great antiquity. Æneas Tacticus, a Greek writer on military affairs of the fourth century B. C., enumerates twenty different methods of secret communication. Some of the methods in early use have been made famous by the anecdotes of Plutarch and other ancient writers. The most famous of these devices, perhaps, is that known as the Skytale, which consisted in writing a message on a narrow strip of parchment wound spirally around a wooden rod. When unwound, the letters of the words of the message were so scattered that they did not form intelligible words and could not be read. The method of reading was to rewind the parchment around a rod which was of the same diameter as the first. This was successfully used by Athenian generals.

Another early method is one reported of the great statesman, Themistocles. While he was in exile from his native country, one of his friends, wishing to communicate to him the news that the time was ripe for a revolt and a return to power, shaved the head of one of his slaves, tattooed the message in indelible ink on the bare skin, and having waited long enough for the growing hair to cover the writing, sent the slave to Themistocles with the oral message that he was to shave the slave's head.

Histiæus' Letterhead

HERODOTUS tells of a message sent by Histiæus to Aristagoras by the same method. Since the message was tattooed, it remained on the slave's head, and for this reason the cautious person, to erase evidences of his conspiracy, often put the slave to death after he had accomplished his errand.

The first book printed dealing with cryptography is Chronologica Mystica, taken from the manuscript of Johannes Trithemius—1462–1516—Abbot of Spanheim and Würzburg. Trithemius labored under the suspicion of dealing in unlawful arts, and left to others the hazard of printing his manuscript. It appeared two years after his death, but all copies were burned because his contemporaries were unable to understand some of the mystic symbols and regarded the book as a treatise on magic. For more than forty years the original manuscript lay hidden in a monastery, then appeared again as De Polygraphie, by Gabriel de Collanges, Paris, 1561. This book has 300 pages, is beautifully illustrated, and contains innumerable methods for secret correspondence. Below is an illustration from this book which shows arbitrary sign alphabets used by the early Germans, one by Dorneus, and another by Charlemagne. Another illustration in the book is a disk with a normal A-to-Z alphabet and six reverse normal alphabets. Nearly 400 years after the publication of this cipher we find the United States Army using it at the outbreak of war with Germany.

Hard Reading

THE most difficult cipher given by Trithemius is composed of 376 alphabets, each letter in each alphabet being represented by a different word or phrase.

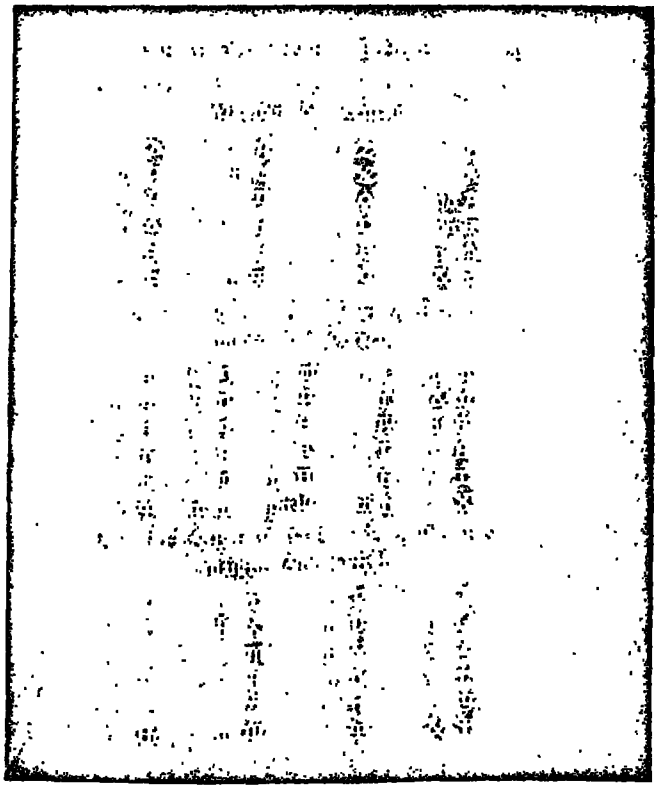
In enciphering the letters of a message the attempt is made to select words which, when placed together, make an intelligible sentence. Trithemius says this can be done, and I presume it can, since the enciphering may select one of 376 words for each letter. The hostile cryptographer is here faced by two problems. He must first determine that the communication contains a hidden meaning, then identify the letter each word stands for. Since each letter has so many different words, his task will be by no means a simple one.

Madame Maria de Victorica, the famous woman spy captured in America during the war, used a modification of this system for cable communication with her masters. The first letter of each word of an unsuspicious business cablegram represented figures, and these, when arranged in groups of five and reversed, were looked up in a code book. The keys were changed often, and were sent to her by means of secret-ink letters smuggled into the United States by neutral seamen and mailed to her through secret cover addresses.

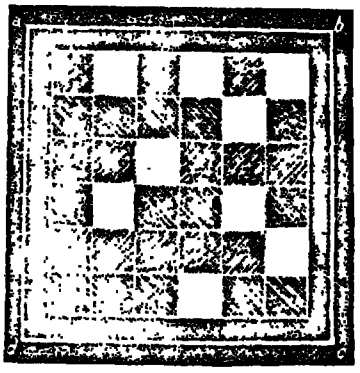
Trithemius was not the only cipher expert of the sixteenth century who was charged with dealing in unlawful arts. The celebrated French mathematician, Viète, nearly lost his head because of his cryptographic skill. During the reign of the French King Henry IV cipher correspondence was intercepted

(Continued on Page 63)

The Wheatstone Cipher, Exhibited in Paris in 1867. The Inner Alphabet Can be Erased and a New One Inserted



Arbitrary Sign Alphabets From De Polygraphie, by Gabriel de Collanges, Paris, 1561



This Stencil Will Solve the Cipher Described on Page 64, if Used in Accordance With Instructions Given

(Continued from Page 60)

"Unless you can hear something ill-natured about her, is that it, dear?" said Georgette.

"Oh, if you imagine I'm jealous!" Lenore gave a stage laugh. "The past is always the past."

"That's just the trouble," Georgette sympathized. "It is! And it stays in one's blood. Memories are ever so much more dangerous than temptations. Don't you agree with me, Roger?"

Lenore rose from the table, trembling with anger, and spoke in a loud, childish voice:

"Come on, Jimmie, let's get out of here! I'm sorry I let you come down today. I really ought to apologize for introducing you to such dreadful people!"

"It seems a very jolly little party to me," Jimmie replied calmly, as he rose. "Will you excuse me?"—to the others. And, as he followed Lenore: "Honestly, I'm having a swell time."

"He takes us for a side show! Damn his impudence," Georgette said. She jumped up, scattering napkin, handkerchief, and a string of beads; they went tinkling to the floor in the unbroken silence.

"Well," she cried, laughing hysterically, "perhaps I'd better pack my bags, before I'm asked to."

"Nonsense, Georgette; sit down," said Roger sternly.

"Not nonsense at all! Lenore's capable of anything! Do you think I don't know how she threw Cecile Carpenter out in the middle of the night?"

"That is not true."

"Oh, you can't hush it up. I wasn't here, but I heard all about it. Everyone knows. She simply ordered Cecile out of the house at three o'clock in the morning—you'd gone to bed, I believe—but the rest were dancing, and Lenore got jealous of Cyril, I suppose ——"

"Georgette, I forbid you ——"

"Well, you can't forbid all Broadway from talking! Oh, you needn't be so ashamed of it, Roger. I know you were married to a lady before, so you are not used to this sort of thing. But it's just a little habit that grows on successful actresses. Sometimes they get spoiled, and begin to believe they're divine: a mere ordinary mortal dares to cross them, so they simply scream 'Get out!' It's quite natural. It would be a great relief, of course, to yell at guests who irritate you, and order them out of your house. I quite understand it."

"So do I," said Roger sternly. "But I don't do it. And neither does Lenore. Will you oblige me, Georgette, by calming down and finishing the week-end here in peace?"

"That's the nearest you've ever come to giving me an invitation, Roger dear! I never thought before that I was truly welcome in your house!"

"Serve coffee on the terrace," Roger told the maid. "Will you come outside?" he said to his guests. "And we'll have coffee with Mr. Dalway and Lenore."

But when they went outside on the terrace, Lenore and Mr. Dalway had gone.

(TO BE CONTINUED)

CRYPTOGRAMS AND THEIR SOLUTION

(Continued from Page 21)

between the Court of Spain and the anti-royalist party in France. The King called for Viète, who discovered the message was enciphered with fifty different arbitrary signs, and turned the decipherment over to His Majesty. When the Spaniards learned of this they took their revenge by accusing the Court of France of having the devil in their employ, and denounced Viète as dealing in black magic before the ecclesiastical tribunal at Rome. Fortunately for Viète, he was as clever at exposition as he was at cryptography, and saved his neck by explaining how he did it.

The seventeenth century was not without its cipher experts. During the siege by the King's troops under the command of the Prince of Condé, of the town of Réalmont—which was defended by the Huguenots—the Prince was on the point of withdrawing, due to the determined resistance of the defenders, when a messenger bearing a cipher dispatch from the town was seized. Antoine Rossignol, the Prince's cipher wizard, solved the message in short order. It was an appeal to the Huguenots of Montauban, telling them that the garrison was almost out of gunpowder, and that the town must surrender if a supply was not immediately sent. The Prince of Condé returned the cipher and its solution to the commander of the town, with the advice that if conditions were as stated further loss of life was scarcely worth while. The commander of the garrison saw the point and surrendered.

One of the oldest and simplest ciphers employed in military operations is the so-called Julius Cæsar cipher. In this each letter of the alphabet is represented by another letter of the alphabet; one, two, three, or four spaces, either preceding or following the original letter. In its simplest form, B equals A, C equals B, D equals E, and so on. Though the invention of this system is attributed to Cæsar, it is known that it was used by the Phœnicians and Carthaginians. It continued in use for hundreds of years, and in a modified form was used by the Germans in 1870–71 and by the British forces during the South African War.

Edgar Allan Poe's Gold Bug is the most famous cryptogram in fiction. Here the letters are represented by arbitrary symbols. This method of secret communication dates back to the ancient Egyptians, who used simple cryptograms to disguise treatises on magic. Poe, the author of the famous line, "Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve," ran a cipher column in his newspaper, defying his readers to devise a cryptogram which he could not read. Just how much Poe knew about the principles of cipher as developed 100 years later, during the World War and after, is not known, but he was clever enough to decipher all messages submitted to him except two which were unfair examples of the art. It is comforting to know that Poe, despite his genius, made mechanical errors. The frequency table for his cipher in the Gold Bug, as originally published, did not agree with the cryptogram. In writing the story, Poe found it necessary to make a slight change in the cryptogram, but failed to make the necessary changes in the frequency table which gave the number of occurrences of each symbol.

Seeking Ciphers in Shakspere

Philip II, of Spain, in 1572, used a curious-looking cipher for correspondence with his brother, John of Austria. The original is in the archives at Simancas, Spain. It is a large table made up of the letters of the alphabet, consonant-vowel digraphs such as *ba, be, bi, bo, bu*, and common trigraphs such as BLE, CRE, PRE. The cipher symbols are letters and one and two figure combinations modified by ? . , ! and the like. To encipher "cryptography" it is first divided C R Y P TO GRA P H Y, and enciphered equals 1 14 18 9 16? 4.. 9 5 18. I should like to see the modern telegrapher copy this over the wire.

There are extant several hundred cipher pages of the Elizabethan period. In one the Queen of England is "Aries" and the King of Spain, "Scorpio." In another cipher the Pope is "Beware" and the Emperor, "Doubt." Father Creighton and Father Parsons are "Weasel" and "Ferret." In still another cipher we find the Queen Mother as "Mean" and the French King, Henry III, "Ignorant." French cavalry are "ells of velvet," and guns, "barrels of salt."

During the World War we found this same type of secret communication among spies. "Uncle has recovered" is "We are no longer under suspicion," and "Uncle is ill" is "We are under suspicion." Sometimes more definite information is conveyed. "Please go to Selfridge's and buy me six blouses on Friday next" means: "Six raiders will bomb Mannheim on Friday next."

More has, perhaps, been written about the biliteral Baconian cipher, attributed to Lord Bacon, than any other single form of secret communication. In this cipher the entire alphabet may be expressed by the two letters *a* and *b* in combinations of five.

A—aaaaa	B—aaaab	C—aaaba	D—aaabb	E—aabaa
F—baaaa	G—baaab	H—baaba	I—baabb	J—bbaaa
K—bbaab	L—bbaba	M—bbbaa	N—bbbab	O—bbbbb
P—aabba	Q—aabbb	R—ababb	S—aabab	T—aaabb
U—abaab	V—abaab	X—aabab	Y—babab	Z—ababa

One of the theories of the Baconians is that the wise men of the past did not dare write their scientific discoveries for fear of being put to death. Thus they left to posterity their knowledge by means of the biliteral cipher. This was done by using two different kinds of type in printing their literary efforts. This theory flourishes because of the fact that books of this period were actually printed with different-shaped type. Those with thin edges are called *a*'s, by the Baconians, and those with thicker lines are *b*'s. Thus, if there are four letters with thin edges—*a*'s—and one with heavier lines—*b*—we have *aaaab*, which equals the letter *b* in the biliteral cipher. Continuing in this fashion, many students have given the world some curious readings. Excavations have actually taken place in England for hidden treasure as a result of these decipherments. One reading from the original of one of Shakspere's plays, if we are to believe the decipherer, is a message from Francis Bacon, who states he is the rightful author and the illegitimate son of Queen Elizabeth. I should add what, no doubt, the reader already knows: The type are different because they were made from imperfect molds during the early forms of printing, and the so-called *a* letters and the *b* letters are so nearly alike that the decipherer may use his own imagination in his selection. Hence these curious decipherments.

Count de Mirabeau, French orator and statesman during the French Revolution, invented a very ingenious cipher, especially for that period. It follows:

```
  1     2     3     4     5
ofxma nibza hclrz eqgtd puyvj
12345 12345 12345 12345 12345
```

The order of the letters may be changed at will. In this cipher each letter is represented by two figures. Instead of writing 32, 22, 51, 31, 41, 34 for "cipher," the figures are written in two columns: 3 2 5 3 4 3 / 2 2 1 1 1 4 Since the figures 6, 7, 8, 9, 0 do not occur, these may be used as nulls—figures that have no meaning—in order to disconcert the hostile decipherer. With the use of nulls, the word "cipher" may read 6 3 2 5 3 7 4 3 / 1 2 2 1 1 2 1 4 The two horizontal lines are now sent as the message: 6325, 3743, 1221, 1214. The advantage of this ingenious system is that it has the appearance of code and would, because of this, offer some difficulty of solution.

Unsolved Codes of the Revolution

The revolutionary ciphers are of varied types, so varied indeed that many writings of Jefferson, Madison and Monroe remain undeciphered, though many attempts have been made to read them. There are also in the Government archives many passages in diplomatic correspondence that still remain a mystery. The attempts at decipherment have been made by historians; to my knowledge, no professional analyst has ever undertaken the task. One of the methods during this period is a table of alphabets used with a key. In a letter to Madison from Edmund Randolph we find: "Let the key word be the name of the Negro boy who used to wait on our common friend, Mr. Jas. Madison." The Negro boy's name was Cupid.

Dictionaries were also used during this period, a numeral indicating the page number, A or B the column, and Roman numerals the line. A code word would then read: "45 A xxiv." Special codes were also made up consisting of letters, syllables, names of persons, places, and the like, and each given a number. This type of small code eventually led to the modern codes used by governments and the business world. Governments, for the most part, are interested in secrecy only. The business world, interested more in economy, uses codes containing 100,000 or more words and phrases which are represented by arbitrary five-letter groups such as *babad, fakaw, glewl, slido*. The cable regulations permit ten letters of this type as one chargeable word. The sentence "When can you ship one thousand bags of coffee?" may be encoded: *Slido*—when can you ship—and *fakaw*—one thousand bags of coffee. *Slido* and *fakaw*, the two code words representing these phrases, are now joined together—*slidofakaw*—and sent as one cable word. Here we have nine words reduced to one.

In written dispatches during the Civil War, the Confederates used arbitrary signs after the manner of the Charlemagne alphabet—shown on

page 21. Instead of one alphabet, several were used, but a whole word at a time was written in one alphabet. In one case the decipherment of an intercepted dispatch was due to the laziness on the part of the writer, who wrote "Alydfl this reaches you." The six letters were arbitrary signs instead of letters. Because of the repetition of *l* in "alydfl," this word was solved as "before." The remainder of the dispatch was then not very difficult to decipher.

Written dispatches, however, are not enciphered, as a rule, during warfare. There are many stories of the disasters that Napoleon and generals of the Franco-Prussian War suffered as a result of this carelessness. Even the Battle of Gettysburg might have had a different outcome had the Confederates taken the precaution to encipher a dispatch which Captain Dahlgren found on a captured Confederate messenger. The message was from President Davis to General Lee, and told him that it was impossible to assemble an army under Beauregard at Culpeper to threaten Washington, as he wished. This dispatch was handed to General Meade on the evening of the second day of the Battle of Gettysburg. Some historians contend that Meade had already issued an order for a retreat, but upon the receipt of the information that Washington was in no danger except for the army in front of him, countermanded the order and continued the battle.

The Rail-Fence Cipher

One of the ciphers used by the Union forces was the Rail Fence transposition cipher. In this, "enemy retreating" is written e e y r e t i n and transmitted: "eeyer, aignm, rtetn." If lines are drawn from *e* to *n* to *e* to *m* to *y*, we have the appearance of a rail fence. In longer dispatches, the words instead of the letters were transposed.

One of the oldest forms of transposition ciphers—one in which the letters of the text are disarranged by a prearranged key—is the stencil cipher, used by the Russian Nihilists. The stencil may contain any number of squares divisible by four. The one shown on page 21 contains thirty-six. By a prearranged key, nine squares are left open. The message "Beware x You are under surveillance x Olga x" is enciphered in the following manner: Write the first nine letters, *B E W A R E X Y O* in the vacant squares and turn the stencil one position clockwise, so that *a* is opposite B. Now write the next nine letters, *U A R E U N D E R*, in the vacant spaces. Turn the stencil one position so that *a* is opposite C, and write *S U R V E I L L A;* then turn it so that *a* is opposite D, and complete the message. The cipher now reads:

nbaecw
uexzae
errrul
eegezx
ainxdy
lelear

The letters from the horizontal lines are now sent in groups of five: *nbaec, wuexz, aaerr, rrlee, gexua, inxdy, lelea, r.*

This method of secret correspondence, in a modified form, was used by Richelieu. The stencil is placed on a sheet of paper and the message written through the holes; in this case the stencil is not turned, being used in only one position. When it is removed, only a few disconnected words appear. It is now left to the ingenuity of the writer to fill in the lines so that they make intelligible sentences. The recipient places a duplicate stencil over the message and sees only the words that are intended to convey the real meaning. This method was also used by German spies during the war in an attempt to defeat the censor, but the awkward language necessary to fill out the message usually betrays the system.

Many newspapers today carry simple cryptograms in their puzzle columns to fill the craving of the American puzzle-bent mind. These show the division of words, *uijt jt b tinomf*, and the like. And many readers have developed amazing skill at their solution, though none I know of ever think of having before them the statistics that would be of assistance. They know in a vague way that *e* is the most frequent letter in English, but not a great deal more. These and most of the other ciphers I have mentioned would not be very difficult for the professional cryptographer to solve. His first step is to index every letter in the message with its prefix and suffix letters. Such charts develop surprising behaviors. But what they indicate cannot be appreciated until we have done the same thing with the English language. Based on a count of 10,000 letters and reduced to a table of 200, we find that the relative frequency of English letters is:

16	3	6	8	26	4	3	12	13	1	2	7	6
a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*

14	16	4	0	13	12	17	6	2	3	0	4	0
n	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*

The most frequent letters are *e t o a n i r s h* and the least *q x z j k v*. The vowels *a e i o u y*, represent about 40 per cent, the high-frequency consonants *h n r s t*, about 34 per cent, and the low-frequency consonants *j k q v x z*, less than 2 per cent.

But we should also know something about digraphs. Based on a count of 20,000 letters, we find that *th* occurs fifty times, and *re* only sixteen. The first thirty high-frequency digraphs are:

th—50	*he*—33	*at*—25	*nt*—24	*st*—20	*ar*—16
er—40	*in*—31	*en*—25	*re*—22	*io*—18	*as*—16
on—39	*ed*—30	*ti*—25	*ti*—22	*le*—18	*de*—16
an—38	*nd*—30	*of*—25	*to*—22	*is*—17	*rt*—16
re—36	*ha*—26	*or*—25	*il*—20	*ea*—17	*te*—16

This table will tell us even more. We learn that "the" will occur eighty-nine times, and "men" only twenty. The first fifteen trigraphs are:

the—89	*tio*—33	*edt*—27
and—54	*for*—33	*tis*—25
tha—47	*nde*—31	*oft*—23
ent—39	*has*—28	*sth*—21
ion—36	*nce*—27	*men*—20

But we should know more than this about the behavior of English letters for the solution of even simple cryptograms. We examine 10,000 words and record the letters they begin and end with. Reduced to terms of 100, we find that though the letter *e* is by far the most frequent letter in English, it begins words only two times. On the other hand, *e* will end words more often than any other letter. The letter *o* is a high-frequency beginning, but a very low-frequency ending. The complete table follows:

Letters	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*
Initial	9	6	6	5	2	4	2	3	3	1	1	2	4
Final	1	–	–	10	17	0	4	2	–	–	1	6	1

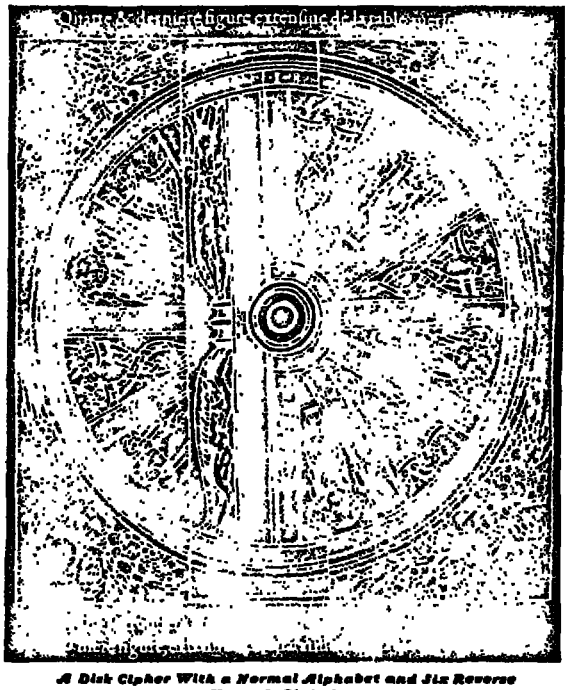
Letters	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
Initial	2	10	2	–	4	5	17	2	–	7	–	3	–
Final	9	4	1	–	8	9	11	1	–	1	–	8	–

Sorting Vowels and Consonants

A prefix-suffix table will tell us something we have never thought much about. We learn that vowels will be followed and preceded by more different letters than will consonants. In other words, *e*, the highest-frequency vowel, will have more different suffixes and prefixes than will *t*, the highest-frequency consonant. We discover that all other high-frequency vowels and consonants behave in the same manner. But what good does this information do us? This discovery enables us in a single substitution cipher of any length almost at once to identify which cipher letters are vowels and which are consonants—a long stride toward solution.

Further statistics will tell us the order of doublets and common three and four letter endings, such as *ing, tion, ment.* We then have before us the frequency of single letters, of digraphs, of trigraphs, of beginnings, of endings, of doublets, and the method for discovering vowels and consonants. With these data we are in a better position to solve a cipher than if we merely had the vague idea that *e* is the most frequent letter.

Germany, during the war, often used transposition ciphers of a mixed columnar type. The key is formed from a word or phrase—for example, "St. Mihiel sector." Consecutive numbers are now placed over the letters of the word key



A Disk Cipher With a Normal Alphabet and Six Reverse Normal Alphabets

in the order in which the letters appear in the alphabet. The numeral 1 is placed over c; 2 over the first e; 3 over the second e; 4 over h; 5 over i, and so on:

11	13	8	5	4	6	2	7	12	3	1	14	9	10
a	z	y	i	h	i	e	l	r	e	c	t	e	r

The message is now written under groups of fives, thus:

11	13	8	5	4	6	2	7	12	3	1	14	9	10
T	h	e	A	m	e	r	i	c	a	n	F	i	r
s	t	A	r	m	y	U	n	d	e	r	G	e	n
e	r	a	l	P	e	r	s	h	i	n	g		

and read off in the vertical columns in the order given by the key: *arn, rur, e, ramy, eal, cye, ias, ean, ie, rn, hee, ...h, ftr, i g.* The message is now sent in groups of five letters. The method of solving single-transposition ciphers of this type was explained in my article in the May sixth issue of THE SATURDAY EVENING POST, which, briefly, is the discovery of the number and length of the columns. These are then brought together and the message is pieced out.

The Double-Transposition Cipher

When the Germans finally discovered that single-transposition ciphers could be solved, they turned to the double transposition. We have a double-transposition cipher if we take the example above and write it under the same key: thus:

11	13	8	5	4	6	2	7	12	3	1	14	9	10
a	r	n	r	n	r	e	e	i	m	m	p	a	r
l	e	y	e	i	n	s	e	a	e	i	e	r	n
t	s	e	e	d	h	h	l	r	f	g	g	x	

Insert at the end of the message a dummy letter—in this case, *x*—and once more read off the vertical columns in the order of the key, *mig, ash, maf, nid, ree, rnh, eel, nyc, arx, rn, nll, iar, res, peg,* and divide into groups of five letters. A comparison of the resulting arrangement of the letters with their original order will show that they have changed their relative positions in such a manner as entirely to preclude any piecing together as is done in solving a single transposition. The presence of the dummy letter in the second transposition further accentuates the disorder.

Though simple in construction, the double-transposition cipher is the most difficult of all practical ciphers to solve. Many attempts have been made to arrive at a formula for their solution, with indifferent success except in cases where the entire rectangle has been filled in. There is, however, one weakness to this cipher. During active engagements in modern warfare hundreds of messages are necessary, some of which are either similar in content or of the same length. When two messages are of the same length, they may be solved by anagrammatizing—a method that is worth describing.

As examples we will take the message already enciphered, and encipher another of the same length and write one below the other:

m	i	g	a	s	h	m	a	f	n	i	d	r	e	e	r
l	m	a	o	f	e	n	e	e	b	l	t	x	f	m	t
n	h	e	e	l	n	y	c	a	r	x	r	n	n	l	l
s	l	o	u	l	x	l	t	r	e	p	i	d	e	l	y

i	a	r	r	e	s	p	e
e	x	h	w	e	n	r	l

As both are of the same length and enciphered in the same key, it follows that the change of position of each letter of the original text for the one, is the same as for the other. Select any pair of letters, vertically, which may be parts of a common digraph of which the preceding and subsequent letters have a small frequency: thus, take $\frac{t}{y}$. The letter Y, if the beginning of a word, will be followed by e or o. After several trials we find $\frac{h}{o}$ which gives us $\frac{th}{yo}$ to which may be added $\frac{e}{u}$ giving $\frac{the}{you}$. As this suggests no additional combinations, we try another pair. If $\frac{r}{x}$ is not a null, it must be preceded by e. As er is a high-frequency digraph, we try $\frac{e}{e}$ which gives us $\frac{er}{ex}$. After several trials, we select $\frac{er\ (i\ or\ e)}{ex\ t}$. *Ext* suggests *text* or *next.* We try $\frac{m}{n}$ and have $\frac{mer\ (i\ or\ c)}{nex\ t}$. Since we are dealing with military ciphers, *meri* suggests American, giving us $\frac{American}{nextmove}$. In this manner all the letters are gradually put back into their proper places. Short bits of sentences and odd words are formed which ultimately resolve themselves into the complete message.

The dummy letters will become apparent only at the very end. The complete solution is:

TheAmericanFirstArmyUnderGeneralPershingX

YourNextMovementWillBeTowardTheLeftFlankP

Now that we have solved the messages, the next step is to discover the key so that all the intercepted messages in this key may be read. This will be found very difficult until we thoroughly familiarize ourselves with transposition ciphers.

For those who have the cipher urge and wish to learn how to recover the key, I suggest they first encipher several messages, and number the text letters consecutively, so that they may better observe the displacement of the letters when run through a double transposition. Since the Germans used a key of ten letters or more, we begin our experiments with this number of columns, and increase the length one at a time until the correct length is determined.

Profiting by Another's Mistakes

But this cipher, like all others, has still another weakness when actually employed. The Germans used it for wireless communication between Berlin and the Balkans and their secret agents in Tripoli. Now and then in the rush of traffic, the encipherer failed to give the message a second transposition, which enabled our experts at G.H.Q. to discover the key in short order. In fact, the professional analyst's success is due in a great measure to the mistakes of the encipherer—a fact that amateurs, in devising ciphers, seem often to fail to take into account.