SOLVING CIPHER SECRETS

Edited by M. E. Ohaver

TRY YOUR WITS ON THE GREAT CODES AND CRYPTOGRAMS IN WHICH MEN HAVE MASKED THEIR MESSAGES OF LIFE AND DEATH

It has been a common belief that it was possible to construct a cipher that could not be solved without the key. Several such have been submitted to Flynn's at various times. Jules Verne, the great writer of mystery stories, believed that he had found one in the Gronsfeld cipher. Mr. Ohaver shows his error in this issue and explains how the correct key can be found out of the several million possible combinations. But by the time you have solved the specimens he offers some of you will be inclined to think that Jules Verne was right.

We've been flooded with Nihilist ciphers in response to our dare that was hidden in code. Three of them appear in this issue for our readers to try their skill on. If you sent one you may find your name and the keyword of your cipher at the end of this week's department.

One of the many writers who followed Poe's lead in using the cipher in fiction was the famous French author, Jules Verne.

This writer was a great admirer of Poe, not only mentioning him several times in his works, but even going to the length of writing his "Sphinx of Ice" as a sequel to Poe's "Narrative of A. Gordon Pym."

The best known instance of cipher in Verne's works is probably the cryptogram in his "Giant Raft." This is in Gronsfeld cipher, a system of secret writing invented by a German count of that name, and mentioned in the "Schola Stenographica" of Gaspar Schott, published in 1655.

The Gronsfeld cipher is a form of the still older Vigenère chiffre carré, and, like its parent system, was for many years considered absolutely indecipherable without the key. As a matter of fact, both of these ciphers are readily so deciphered.

Of these two systems, however, the Gronsfeld is the easier to decipher. And it is treated of first in these columns for the reason that an extension of the principles used in deciphering it can also be used in breaking the more difficult Vigenère cipher.

While the Gronsfeld cipher is so devised that its use requires but a simple mental operation, in effect it is a cipher of the double key variety. The primary or fixed key consists of ten different cipher alphabets, and the secondary or variable key of
a number that selects certain ones of these alphabets for use in a certain order.

Thus to use this cipher the correspondents must first agree upon some number as their private key, for it is by its means that their message is securely locked, as they

The first step is to write as in line (a) the key number over the message (b) so that each letter will have one figure above it, repeating the key in regular order as many times as the length of the message may require.

The cipher substitute for any letter may now be found by counting forward in the alphabet the number of places indicated by the figure which acts as its individual key.

This process, which in actual practice may be done mentally, is here illustrated at (c). The letter N will be the substitute for M with the key 1, it being the first to follow it in alphabetical order. The 6th letter from E is A, the first word MEET of the message being thus written NIGA in cipher.

In earlier times it was customary to re-suppose, from the prying eyes of those who would share their secrets.

To illustrate, suppose that they have decided upon the number 14275 as their key, and that their message is, MEET ME ON THE SIXTH AS ARRANGED.

The key number over the message (b) so that each letter will have one figure above it, repeating the key in regular order as many times as the length of the message may require.

The cipher substitute for any letter may now be found by counting forward in the alphabet the number of places indicated by the figure which acts as its individual key.

If Z should be reached before the full count is made, the alphabet is considered to be in cyclical arrangement, Z being followed by A, B, C, and so on. The 7th letter in advance of T is therefore A, the first word MEET of the message being thus written NIGA in cipher.

In earlier times it was customary to re-suppose, from the prying eyes of those who would share their secrets.

To illustrate, suppose that they have decided upon the number 14275 as their key, and that their message is, MEET ME ON THE SIXTH AS ARRANGED.

The cipher substitute for any letter may now be found by counting forward in the alphabet the number of places indicated by the figure which acts as its individual key.

If Z should be reached before the full count is made, the alphabet is considered to be in cyclical arrangement, Z being followed by A, B, C, and so on. The 7th letter in advance of T is therefore A, the first word MEET of the message being thus written NIGA in cipher.

This tabular arrangement not only facilitates the use of the cipher with the key, but is also especially convenient in deciphering without it. The substitute for any letter
is found at the intersection of the column indicated by such letter in the normal alphabet at the top, and of the row indicated by the key number at the left.

In a cipher of the Gronsfeld type an immense number of key combinations is possible. A cryptogram in a key of ten figures, for example, might have been enciphered with any one of $10^{10}$, or $10,000,000,000$ different keys.

Popular accounts, as a rule, greatly emphasize such figures as proving beyond a doubt that a given cipher system is absolutely indecipherable without the key.

In the case of the 10 figure key just mentioned the number of keys is so great that if written on pieces of paper an inch long and placed end to end they would reach twice around the world. And any one trying them at the rate of one per minute and working 24 hours per day would need 2,000 years to finish them all.

Nevertheless, these tremendous figures do not daunt the cryptanalyst in the least. For he does not base his methods of solution upon a trial of each one of the many possible keys, but in a determination by special processes of the one particular key.

A number of methods may be used singly or in combination in resolving the Gronsfeld cipher. It is quite possible to determine the key mathematically before a single word of the message has been read and without previous knowledge of the language in which it may be written.

Some of these more advanced methods may be detailed in future articles if we think they would be of general interest. But for the present we shall confine ourselves to the more elementary, and to what, historically speaking, was the earliest procedure used on ciphers of this type.

We have already shown that any one in possession of the key and message could form the cipher, and conversely that any one with the key and cipher could decipher the message. Similarly, if the cipher and message are both at hand, by finding the numerical differences between the corresponding letters, the key can be discovered.

It was upon this last mentioned principle that early cryptographers based their methods of solving this and similar ciphers. Assuming that a certain word occurred in the message, they compared this word with the cipher group supposed to be its equivalent, and thus discovered a portion, or, in some cases, all of the key.

Solution by this method is facilitated by normal word divisions in the cipher, but can also be applied when the writing is continuous. Suppose we expose this method by deciphering the above short illustrative cipher.

Unless a certain longer word is suspected to be present in the message, the shorter and more common words should at first be tried. But for trial with a three-letter word, as THE, the cryptogram should be taken in successive groups of three adjoining letters, or trigraphs, as shown below:

<table>
<thead>
<tr>
<th>GROUP:</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIPHER:</td>
<td>NIG</td>
<td>IGA</td>
<td>GAR</td>
<td>ARF</td>
<td>RFS</td>
<td>PSP</td>
<td>SPA</td>
<td>PAM</td>
<td>AMF</td>
</tr>
<tr>
<td>WORD:</td>
<td>the</td>
<td>the</td>
<td>the</td>
<td>the</td>
<td>the</td>
<td>the</td>
<td>the</td>
<td>the</td>
<td>the</td>
</tr>
<tr>
<td>KEY:</td>
<td>-12</td>
<td>-7</td>
<td>1</td>
<td>-8</td>
<td>751</td>
<td>etc.</td>
<td>etc.</td>
<td>etc.</td>
<td>etc.</td>
</tr>
</tbody>
</table>

Beginning with the first group, NIG, of the cipher, we discover that while it is possible for IG to equal HE enciphered with a key of 12, NIG cannot be THE because N is further than a count of 9 from its supposed substitute T.

Similar negative results with successive groups continue until we reach AMF, which we find could be THE enciphered with 751. A search of the rest of the cipher uncovers two further possibilities, WKE and YIE, which could be THE enciphered with the keys 330 and 510 respectively.

Each one of these three hypotheses may be run down separately. Those founded on error will give negative results. In the present case, assuming that we have eliminated all but 751, we will first demonstrate
how these figures may be used in determining the period of the cipher: the number of figures that constitute its key; then show how the rest of the key can be discovered.

**GROUP:**

1 2 3 4

**KEY:**

751 751 751 751

**CIPHER:**

NIG IGA GAR ARF

**MESSAGE:**

gdf bbz zvq tme

In glancing over the results in the last row for likely combinations, the only groups which might be parts of words appear to be tme, kar, and yno.

The 6th group, yno, being 3 groups from THE, the base of our operations, indicates a period of 3, which would require group 3, zvq, to be a usable combination of letters. And the 5th group, kar, would in like manner indicate a period of 4, which would require group 1, gdf, to be usable. Both of these theories have to be discarded, however, as both zvq and gdf are unpronounceable combinations of letters.

To find the period, the three-letter groups are now deciphered by means of the figures 751 of our supposed key, the results being carefully notated.

<table>
<thead>
<tr>
<th>GROUP</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEY</td>
<td>751 751 751 751</td>
<td>751 751 751 751</td>
<td>RFS  FSP  SPA  PAM  AMF</td>
<td>etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIPHER</td>
<td>NIG  IGA  GAR  ARF</td>
<td>RFS  FSP  SPA  PAM  AMF</td>
<td>etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MESSAGE</td>
<td>gdf  bbz  zvq  tme</td>
<td>kar  yno  lyz  ivl  THE</td>
<td>etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Finally, to discover the two remaining figures of the key, try to complete some of the partially deciphered words.

At the end of the cipher the word AR RanGE D suggests itself, and the two-letter group, SP, is most likely AT, IN, or ON, forming the sequence AT THE, IN THE, or ON THE. By trial SP cannot be either AT or IN, but with the key 42 it can be ON. And this same key works with the word ARRANGED.

Substituting these newly found figures throughout, and deciphering with the now completed key, 14275, reveals the entire message.

In working by this method, frequently Do you accept his challenge?

Try your hand at these:

**CIPHER No. 1.** (Gronsfeld)

<table>
<thead>
<tr>
<th>XKGWF</th>
<th>DPDWY</th>
<th>IRVRL</th>
<th>YIHRV</th>
<th>DGFUC</th>
<th>RHYIH</th>
<th>HLCRP</th>
<th>QHVCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERJWJ</td>
<td>JNXVG</td>
<td>GWPIX</td>
<td>KGXPO</td>
<td>HLGWT</td>
<td>ZLRGX</td>
<td>DRWVG</td>
<td>IUKIF</td>
</tr>
<tr>
<td>QSWRC</td>
<td>FQRNL</td>
<td>XWGIE</td>
<td>XVLPL</td>
<td>UKIQK</td>
<td>LIWSI</td>
<td>VMFWA</td>
<td>HPYZV</td>
</tr>
<tr>
<td>IFQSE</td>
<td>RJKMC</td>
<td>VDBQO</td>
<td>SFWLR</td>
<td>WXBOH</td>
<td>HKLIW</td>
<td>LXPIS</td>
<td>HHDPI</td>
</tr>
<tr>
<td>UZIOV</td>
<td>DTLBZ</td>
<td>CXORX</td>
<td>WJZTM</td>
<td>SDOIB</td>
<td>FSVVF</td>
<td>VQNXU</td>
<td>YMBGR</td>
</tr>
<tr>
<td>PIFPR</td>
<td>HFPGC</td>
<td>IDMJ</td>
<td>WADUN</td>
<td>UKIZT</td>
<td>JUELH</td>
<td>FXFUZ</td>
<td>DPPYPI</td>
</tr>
<tr>
<td>XKCFE</td>
<td>PMQKX</td>
<td>UEWEK</td>
<td>TORJW</td>
<td>JJELE</td>
<td>POSEG</td>
<td>MVVWJ</td>
<td>FXBGX</td>
</tr>
<tr>
<td>JDPRP</td>
<td>JXXSV</td>
<td>KLOWL</td>
<td>LUBJW</td>
<td>LAPYS</td>
<td>XIQCR</td>
<td>FRVWG</td>
<td>LB.</td>
</tr>
</tbody>
</table>

**CIPHER No. 2.** (Gronsfeld)

You will find this one much more difficult.

<table>
<thead>
<tr>
<th>NAQMT</th>
<th>XIXPI</th>
<th>CTDMF</th>
<th>RUVLG</th>
<th>AMUJS</th>
<th>AILZN</th>
<th>BQQWY</th>
<th>KFRJN</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTCUW</td>
<td>XUMIW</td>
<td>GHKEM</td>
<td>VMMSG</td>
<td>HZJMY</td>
<td>BQUJS</td>
<td>AVESJ</td>
<td>G.</td>
</tr>
</tbody>
</table>

The solutions and keys to the above Gronsfeld ciphers will be given in our next article.
In our last article in *FLYNN's* for May 16 we mentioned that the cryptogram offered for solution was enciphered in one of Poe's original alphabets. The fact is, it was the identical alphabet used by Poe in his famous tale, "The Gold Bug."

Since the Gold Bug cipher did not contain all the letters of the alphabet, this cipher alphabet is necessarily incomplete. Fortunately, our own message did not require any of the missing letters, with the one exception of Q, which we represented in cipher by itself.

Here is the Gold Bug key:

```
A B C D E F G H I J K L M N 
2 8 1 6 3 4 9
```

And here is the solution to the cipher:

"FEW PERSONS CAN BE MADE TO BELIEVE THAT IT IS NOT QUITE AN EASY THING TO INVENT A METHOD OF SECRET WRITING WHICH SHALL BAFFLE INVESTIGATION, YET IT MAY BE ROUNDLY ASSERTED THAT HUMAN INGENUITY CANNOT CONCOCT A CIPHER WHICH HUMAN INGENUITY CANNOT RESOLVE."

**ABOUT THE NIHILIST CIPHERS**

In response to our recent challenge in *FLYNN's* for March 28 to solve Nihilist ciphers without the key, we were literally deluged with ciphers from all parts of the continent.

The Nihilists, in their palmiest days, never wrote so many ciphers. And the Russian Cipher Bureau, had they intercepted even a part of the secret communications sent to this office, would have thought that they had a young revolution on their hands.

Our correspondents, as well as the many readers who did not respond to the invitation, are no doubt anxious to learn if we really deciphered these messages without the key.

We are therefore appending a partial list of those who submitted ciphers, together with their key words. Lack of space will not permit publication of all these messages in full. But the fact that we have determined the key words is, of course, evidence that these ciphers have been broken.

Speaking of key words, they form the most curious collection of words imaginable. In this list may be found long words and short ones, ordinary words and rare ones, words that are pronounceable, and some that are only meaningless combinations of letters.

To illustrate this last, Mr. E. W. Bowden, of Barrington, Rhode Island, came across with SFRIQ. His message was: "WHY CANNOT MY DEALER GET FLYNN'S EVERY WEEK?" Very well, Mr. Bowden, we will try to remedy this little trouble at once.

Mr. Arthur L. Cadieux, Crookston, Minnesota, played us a cruel joke. He wrote: "My keyword is hard, but is contained in the message." When we had solved his cipher we found that he hadn't been talking through his hat. His key was HARD, for a fact.

Many of our secret correspondents had pleasing things to say in their ciphers about *FLYNN's* in general, and the cipher department in particular. Most of the latter called for more frequent installments of this department. And some asked that the ciphers be made more difficult of solution.

We refer these latter fans to the ciphers in this issue. The No. 2 Gronsfeld in particular should give them a very uneasy hour or two if they succeed in solving it at all.
And those in the former class have no doubt already noticed that the cipher articles are coming along more frequently.

A great many fans used the names of persons, or of cities, States, or countries as their keys. In some instances these were their own, but just as often otherwise.

An average of one correspondent out of six used the name of the editor of this department, either with or without initials. Mr. Donald C. Burgess, of Parsons, Kansas, chose COOLIDGE. And Mr. John Bracken, Perth Amboy, New Jersey, picked on RICHARD, a certain Richard, by the way, namely, Richard Emright, well known to readers of FLYNN'S.

But for an odd key word, take a look at Mr. Sam Brinkley's TOOTHPICKS. The chances are, Sam, that you were at the dining table when you thought of that key. How about it?

Many of those who submitted ciphers inquire if we have a special method of solving the Nihilist cipher. In answer to these we will say that we not only have a special method that has never been made public, but also that we have about decided to let them in on the secret. More about this, however, next time.

For the benefit of all those who would like to try their hand at solving the Nihilist cipher without the key word, we append the following juicy specimens:

CIPHER No. 3 (Nihilist)

60-48-56-63-74-60-57-73-46-54-85-60-
84-80-39-37-25-87-79-64-59-48-36-65-66-
60-54-68-58-66-45-87-68-67-78-36-56-53-
87-88-58-60-30-76-63-77-87-58-59-58-33-

CIPHER No. 4 (Nihilist)

69-27-57.

CIPHER No. 5 (Nihilist)

37-55-80-66-79-44-63-48-25-60-57-47-48-
57-47-74-78-56-76-58-63-55-88-40-47-70-
76-76-57-45-77-30-65-83-78-65-27-58-84-
66-70-64-66-35-56-59-67-47-77-47-47-
88-67-97-57-43-40-88-49-47-48-75-47-87-

The above ciphers have been selected from those submitted by correspondents. No. 3 is from Mr. James W. Duffy, Cincinnati, Ohio; No. 4 is from Mr. J. K. Manning, Morrisonville, Illinois; and No. 5 is from Mr. Foster F. V. Staples, Attorney at Law, Portsmouth, Virginia.

Now we don't say that these ciphers cannot be solved, for they have already yielded up their secrets. But we just dare you to do it yourself, that's all.

Send in as many solutions as you can get to the ciphers in this issue, even if you only succeed in solving one. And look for another bloc of our Nihilistic friends, with their key words, in our next article.

Anonymous, Porterville, California. CIPHER.
Charles E. Ballard, Brooklyn, New York. OHAVER.
H. C. Barr, Joplin, Missouri. EXCELLENCE.
Elsie M. Bell, Syracuse, New York. MEHOAVER.
Neil C. Bierce, Police Headquarters, Portsmouth, New Hampshire. REGULATOR.
E. W. Bowden, Barrington, Rhode Island. SPRIQ.
John Bracken, Perth Amboy, New Jersey. RICHARD.
Sam Brinkley, Greensburgh, Pennsylvania. TOOTHPICKS.
Walter C. Busby, Jr., Oaklawn, Rhode Island. MHAVER.