ENCRYPTION VIA ONETIME PADS

Thanks to Pete McCollum

This article presents an example of how message encryption was typically done by CIA communicators using a "one-time pad" (OTP). A retired CIA old-timer kindly provided the descriptions.

A one-time pad is essentially a pad of paper on which each page has a unique set of random letters. The sender and receiver have identical pads. Each letter on the pad is used to determine a single letter of the enciphered message.

Since the letters on the pad are random, there is no formula that can be determined by studying the letters. Assuming that the pad is not compromised, and each page is used only once, then the OTP system is unbreakable.

The disadvantage of the OTP system is that a copy of the pad must be securely delivered to the person on each end of the communication. The key letters on the pad, and the messages themselves, are typically written in 5-letter groups.

This helped the communicators to collate and verify the length of the message, and if something was misunderstood, the receiving person could ask for a certain group to be repeated, etc.

"OTP is a very simple yet completely unbreakable symmetric cipher.

To use a one time pad you need 2 copies of the "pad" which will vary in size from something around 8 x 10 inches, or approximately half that size.

There are two pads issued to each user. One for encipher and one for decipher, and the key text is printed in red for encipher and black for decipher.

Each page of the pad is sealed and must not be opened until actually enciphering or deciphering [if a page is not sealed, it must be assumed that the page has been compromised - Pete].

Typically the pads are set up in blocks of five letter random groups.

The key text may not be reused and pages should be destroyed after each use."

To use the OTP, a method is needed for correlating a letter of plain text with the next letter of the key text (from the pad), to produce a letter of enciphered text.

The method used is called a "Vigenere's Tableau", or Vigenere's square.

The table has the alphabet in the left-most column, and also across the top.

For each row, there is a shifted-reverse alphabet.

So, the "A" row lists the alphabet backwards, beginning with Z.

The "B" row begins with Y and ends with "DCBAZ", etc. The first 3 rows of the table look like this:

ABCDEFGHIJKLMNOPQRSTUVWXYZ
A ZYXWVUTSRQPONMLKJIHGFEDCBA
B YXWVUTSRQPONMLKJIHGFEDCBAZ
C XWVUTSRQPONMLKJIHGFEDCBAZY

To encipher the first letter in a message, go to the row corresponding to the plain-text letter, then go to the column indicated by the first letter on your OTP.

The letter at the row-column intersection is the enciphered letter.

Note that the Vigenere's table itself does not contain any 'secret' information - it simply provides the mechanism for combining plain and key text into enciphered text.

For example, suppose that the message is "Dead drop Alpha three AM tonight" :

DEADD ROPAL PHATH REEAM TONIG HTXXX ----- (plain text)
BNJEX KQPBC LZCXV PKTUY QFHNG QWERT ----- (text from OTP)
VIQSZ YVVYM ZTXJX TLCFP QGFEN CKYLJ ----- (enciphered text)

One of the two disks that comes with the GRA-71 burst coder device has an extra reversed alphabet enscribed on it, thus allowing it to be used in place of a printed table.

The red mark on the coder is aligned with the red letter on the wheel indicating the desired row of the table, then the 2nd and 3rd members of the triad are read from the white letters directly below the red mark.

New students of the OTP encryption scheme were given a card, about 3" X 6", which had the complete Vigenere's table printed on the front, and a "memory aid" on the back.

The back is a set of certain 3-letter combinations ("triads") taken from the main table. The triads on the back of the card are chosen because they are relatively easy to remember. The more triads that can be memorized, the faster the radio operator can finish his job.

Here is a sample from the back of the card:

MEMORIZE THESE

Five minutes daily spent in studying these combinations will pay
dividends in the time saved in encoding and decoding.

AIR FOG SOT
BAY HAS SUN
CUD HOE TAG

An experienced radio operator would memorize the entire table, and could take a look at the plain text, and key text, identify the triad from memory, and thus encipher as he sent code.

A less-experienced operator would have to write down the enciphered message before sending it.