Do It Yourself!

Polybius square:

| E | N | I | G | M | A |

|---|---|---|---|---|---|

| A | A | D | F | G | V |

| D | X | B | C | E | H |

| F | I | K | L | M | N |

| G | O | P | Q | R | S |

| V | T | U | W | X | Y |

**Encrypted message:**

VFDGXVGFDXVXFGGXGFFV

Transposition key:

3142

—————————————————

To solve the ADFGVX Cipher puzzle, follow these steps:

1. Create the Polybius square using the keyword "ENIGMA", writing the message to encrypt.

2. Replace each letter in the message with its corresponding ADFGVX letters from the Polybius square.

3. Combine the ADFGVX letters into a single string and apply the transposition key to the string by writing the letters in the order specified by the key.

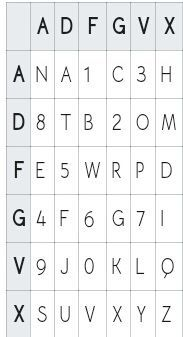
4. Divide the string into pairs of letters, and use the Polybius square to convert each pair into a plaintext letter.

Modern History

In the years following World War I, new ways for encryption were built on the foundation laid by the ADFGVX. The use and invention of the Enigma machine by Germans during World War II sparked revolutionary advancements. The enigma incorporated transposition and substitution, much like the ADFGVX cipher, but used electromechanical technology to improve the complexity and security. 

After the war, computer technology pushed these same techniques to modern public key cryptography, requiring a shared secret key. These led to the development of modern methods such as RSA and elliptic curve encryption, which help secure sensitive data today.

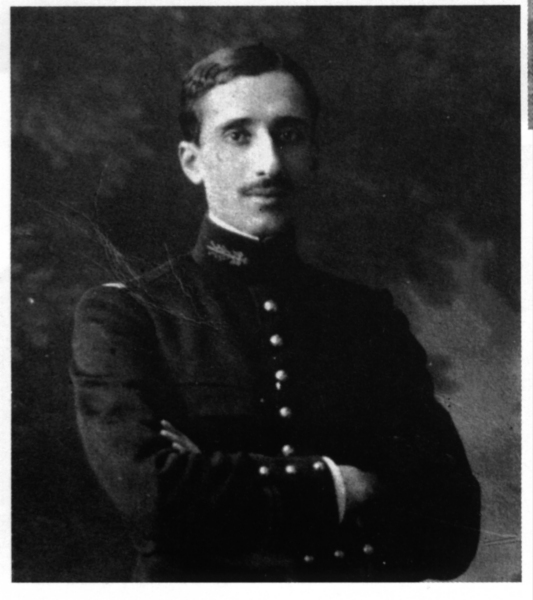
ADFGVX



History

ADFGVX was a cipher used by the German army during World War I. It was invented by Lieutenant Fritz Nebel and used by the German army during the Battle of the Meuse in 1916. The cipher was named after the six letters used in its alphabet: A, D, F, G, V, and X.

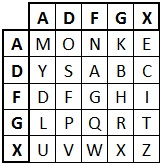
The ADFGVX cipher combined a substitution cipher and a transposition cipher. The substitution was accomplished by replacing each plaintext letter with a pair of letters from the ADFGVX alphabet. The transposition was achieved by writing the letters in columns under the letters of a keyword, then reading them off row by row.

The cipher was considered very secure at the time and was used by the German army to communicate sensitive information. However, the cipher was eventually broken by the French cryptanalyst Georges Painvin, who used a combination of frequency analysis and mathematical techniques to crack the code.

Despite its eventual downfall, the ADFGVX cipher remains an important historical example of cryptography, and its complexity and effectiveness in the early 20th century are still studied and appreciated by modern cryptographers.

General Information

ADFGX was a cipher used during World War I by the German army to encrypt their messages. The V was added to the ADFGX cipher to create the ADFGVX cipher in order to increase the security of the encryption.

The ADFGX cipher used a grid of 5 rows and 5 columns, and the five letters A, D, F, G, and X were used to label the rows and columns. This meant that each letter in the plaintext was replaced by a pair of letters in the ciphertext, which made the cipher more difficult to crack than simple substitution ciphers.

However, the ADFGX cipher was still vulnerable to cryptanalysis, especially with the development of frequency analysis techniques. Therefore, the German army introduced the ADFGVX cipher, which used a 6x6 grid instead of a 5x5 grid, and added the letters V and X to the set of letters used in the cipher. This increased the possible combinations of letters, making the cipher much more secure and resistant to attacks.

Instructions

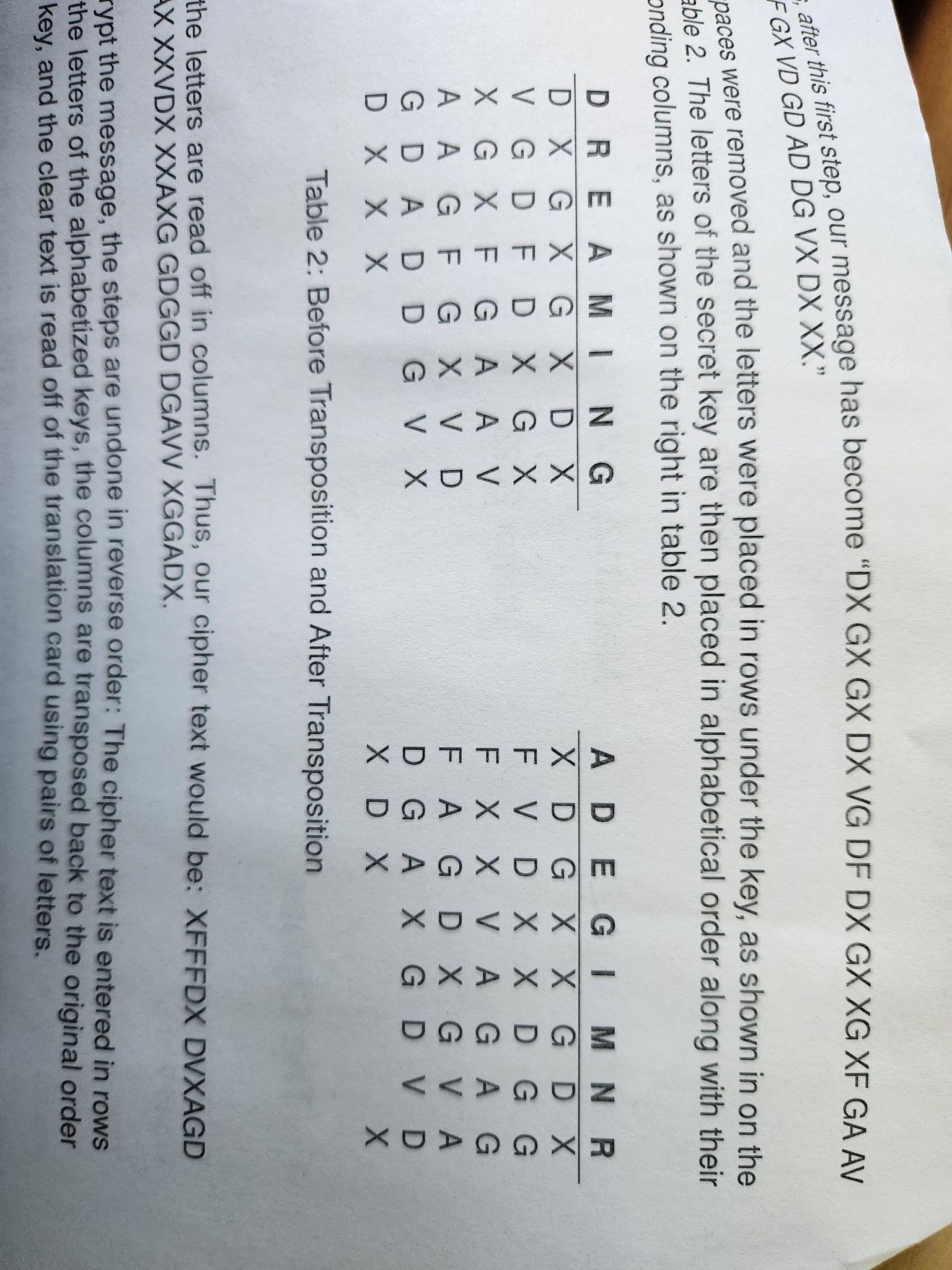
How do we use the ADFGVX cipher to encrypt a message we want to keep secret? Well, we just need to follow these steps.

Step 1: Find an ADFGVX translation card, your keyword (usually short) and choose the message you would like to encrypt. For this example we’ll use “Attack the left flank at 1200”.

Step 2: Remove all spaces from your message, our example turns into “attacktheleftflankat1200”

Step 3: Find the corresponding row and column(in that order) that matches the letter. Our message with the card on the front of this pamphlet turns into, “AD DD DD AD AG VG DD AX FA VV FA GD DD GD VV AD AA VG AD DD AF DG VF VF”.

Step 4: Put your now encrypted message through a transposition table using your keyword and organize the keyword’s letters alphabetically, like this example does:



Step 5: Read off the newly encrypted message down the columns. The example would be “XFFFDX DVXAGD GDXGAX XXVDX XXAXG GDGGD DGAVV XGGADX”.