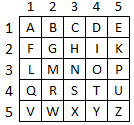
**BIFID QUADRANT CIPHER**

1. **INTRODUCTION**

The researchers propose a hybrid of two existing ciphers, the Bifid Cipher and the Four-Square Cipher, which were invented by French cryptographer Félix-Marie Delastelle. This hybrid cipher shall be called Bifid Quadrant Cipher (BQC).

**Bifid Cipher**

The Bifid Cipher makes use of a Polybius square as its key, a 5 x 5 grid of letters where rows and columns are labeled with numbers 1 to 5. Since there are only 25 squares, the letter "j" is omitted and may be substituted with the letter "i".



For example, to encrypt the word "BAT", the letters are first located in the grid and the coordinates recorded as follows, where the first row corresponds to the row coordinate and the second row corresponds to the column coordinate:

C:\Users\PerryG\Documents\0_MIT\IT Sec\BAT.png

These two sets of numbers are then written side by side, paired into two's, and will be the new coordinates of the cipher text:

1 1 4 2 1 4 → 1,1 4, 2 1,4

1,1 = A; 4,2 = R; 1,4 = D

Cipher text = ARD

**Four-Square Cipher**

The Four Square Cipher uses four 5 x 5 matrices arranged in a square, like its name implies.  Each of the 5 by 5 matrices contains the letters of the alphabet, usually omitting "Q" or putting both "I" and "J" in the same location to reduce the alphabet to fit. In general, the upper-left and lower-right matrices are the "plaintext squares" and each contain a [standard alphabet](https://www.revolvy.com/main/index.php?s=Standard%20alphabet&stype=topics). The upper-right and lower-left squares are the "cipher text squares" and contain a mixed alphabetic sequence.

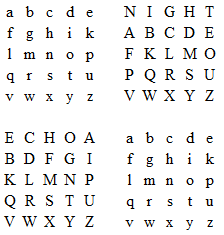
For the specific steps involved in this cipher, the following is used:

Plaintext: BATS

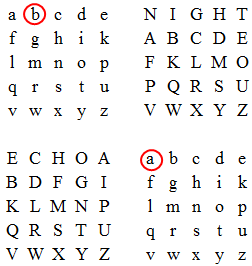
Key 1: NIGHT

Key 2: ECHO

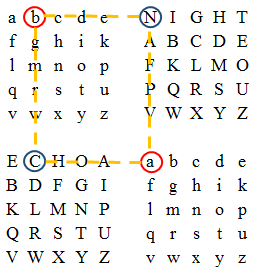
The upper left and lower right matrices shall consist of the alphabet in order, while the upper right and lower left matrices shall consist of key 1 and key 2, respectively.



The plaintext shall be grouped into two's, and shall be located in the upper left and lower right matrices.



The cipher text shall now be located in the upper right and lower left matrices by finding the two letters that would serve as the other two vertices in order to form a square:



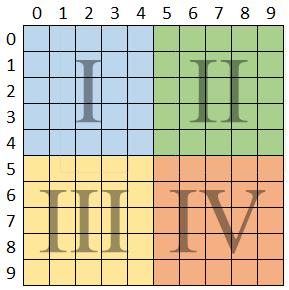
The corresponding cipher text for b is the letter N while the corresponding cipher text for a is the letter C. This process is repeated until the final pair of letters, which would result to the following cipher text:

NCRT

The Bifid Quadrant Cipher combines the coordinate feature of the Bifid Cipher and the four separate 5x5 grids of the Four-Square Cipher, making it into one 10x10 grid.

1. **ALGORITHM**

The Bifid Quadrant Cipher uses two sets of key texts to encrypt the plaintext. Using the concept of the Four-Square Cipher, this cipher uses a 10x10 table that is divided into four quadrants, instead of four separate squares. Each of the quadrants contains a 25-letter set of the alphabet omitting ‘j’.



The rows are columns are both labeled by numbers 0-9. The first key text will then be plotted in quadrants I and II, while the second key text will be plotted in quadrants III and IV.

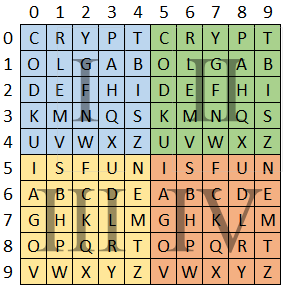
**A. ENCRYPTION**

The first key text will be used to fill in the first and second quadrant, while the second key text will be used to fill in the third and fourth quadrants. In filling in the squares, the letters comprising the key text is placed first. After that, the rest of the alphabet shall be placed in the remaining squares. Because there are only 25 squares, the letter j is omitted and shall be combined with the letter "i". To illustrate the steps more clearly, the following example is used:

Key Text 1: Cryptology

Key Text 2: is fun

Plaintext: Hello World

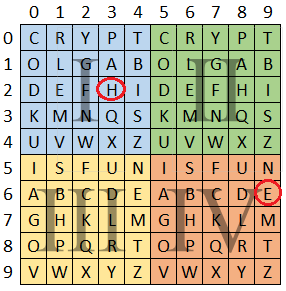


Using this arrangement of the alphabet characters, we can now start plotting to encrypt a message.

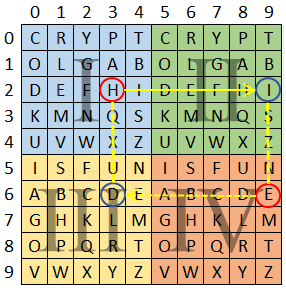
The plaintext is first split into groups of two, otherwise called a digraph. If the plaintext consists of an odd number of letters, one extra letter shall be added to the end, such as X.

H E L L O W O R L D

The first letter is to be located in the first quadrant, while the second letter in the fourth quadrant.



Using the same method as the Four-Square cipher, the corresponding cipher text shall be the other two letters found in the second and third quadrant which would complete the square. The equivalent cipher text of the first letter shall be taken from the second quadrant, while the second letter's cipher text shall be taken from the third quadrant.



In this example, the equivalent cipher text for "HE" is "ID". This process is repeated up to the last digraph, and it will result to the following cipher text:

H E L L O W O R L D

I D A H L V A O A B

The coordinates of the cipher text shall then be written into two rows, in which the first row consists of the row number, and the second row of the column number:

C:\Users\PerryG\Documents\0_MIT\IT Sec\BQC step3.png

To get the cipher text, the second row shall be written after the numbers in the first row:

Cipher Text = 26171918169381608081

**B. DECRYPTION**

The expected cipher text shall be a string of numbers. The following example shall be used to further illustrate the steps involved in decryption:

Cipher text: 26080807299080629471

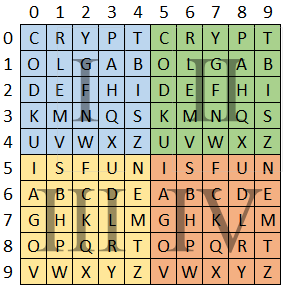
Key 1: Cryptology

Key 2: is fun

The cipher text shall be divided into two, and the second set of numbers shall be written below the first set of numbers.

C:\Users\PerryG\Documents\0_MIT\IT Sec\BQC step3.5.png

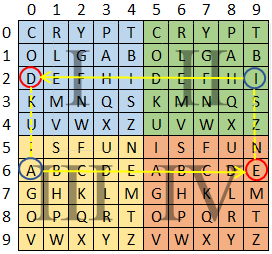
A 10 x 10 grid shall be drawn up, and be filled with the two keys accordingly, with the same process as the encryption.



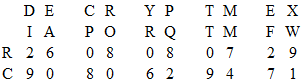
The coordinates are grouped into two's, and shall be plotted in the grid. The first pair of coordinates is plotted in the second quadrant, while the second pair shall be plotted in the third quadrant. This is the text equivalent of the cipher text numbers.

C:\Users\PerryG\Documents\0_MIT\IT Sec\BQC step4.png

The equivalent plaintext shall be found by locating the two letters from quadrants one and two that would complete the square.



The process is repeated until the last pair of coordinates has been translated into the corresponding plaintext.



Plaintext: DECRYPT ME X

In this example, an extra letter is added because the plaintext has an odd number of letters.