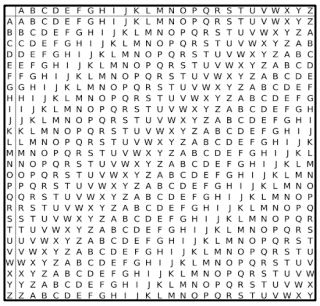
# Background and Problem Statement

When we encountered the problem that we wanted to confess to our lovers by dropping a note without anyone else understanding, how could we make this happen? We came up with an idea that we could use encryption to protect our message.

# Materials and Methods in Detail

## The Encryption

To connect our problem with linear algebra, we chose Hill cipher to encrypt our message. Besides, in order to increase the complexity of encrypted text, we used Hill cipher as our second step. While practicing Vigenere cipher, you create a keyword in order to collocate with the table below for encryption. In the process, it is recommended to make the keyword the same length as the message. After that, use the table below to create the corresponding cipher text after encryption.



For preparation of Hill cipher, you should design a key matrix(n*n) and turn those English letters into numbers. Also, to practice Hill cipher easier, you can divide those numbers into a few parts so that each length of the plaintext vector corresponds to the size of your key matrix(n). The following procedure is to multiply each plaintext vector with the key matrix. By now we get the numbers encrypted by Hill cipher.

## The Decryption

If given the key matrix, finding the inverse matrix of the key as well as dividing the encrypted numbers into n parts, we'll get the plaintext before encryption of Hill cipher. Next, translate those numbers back to English letters, and use the table of Vigenere cipher and the keyword that is given to convert back to the original message.

# Results

In our example, we wanted to encrypt "I love you". Therefore, we create a keyword, "linear", to proceed Vigenere cipher. The encrypted text after the Vigenere cipher is in the following picture.

| Keyword | L | I | N | E | A | R | L | I |
|---|---|---|---|---|---|---|---|---|
| Message | I | L | O | V | E | Y | O | U |
| Cypher | T | T | B | Z | E | P | Z | C |

Before doing Hill cipher, we designed $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 5 \end{bmatrix}$ (3*3) as our key matrix and converted alphabets into numbers (0~25).

After encrypting by Hill cipher, the whole cipher text is as below.

19 57 5 25 12 75 25 6 -5

As for decryption, we found the inverse matrix of key first, which is $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1/3 & 0 \\ 0 & 0 & 1/5 \end{bmatrix}$, divided the numbers {19 57 5 25 12 75 25 6 -5} into 3 parts, and then multiply each vector with key inverse. Now we get {19 19 1 25 4 15 25 2 -1}.For the next step, we converted numbers into alphabets (we filled in -1 to represent the null factor in last vector because "I love you" contains only eight letters) and used our keyword "linear" with the table mentioned above to decrypt back. The result is definitely "I love you".

| Decryption | T | T | B | Z | E | P | Z | C |
|---|---|---|---|---|---|---|---|---|
| Keyword | L | I | N | E | A | R | L | I |
| Message | I | L | O | V | E | Y | O | U |

# Evaluation of Proposed Solution

## Pros:

Messages would be harder to understand and thus avoid any unnecessary discovery. Besides, you might be more impressive to the one who receives your mysterious love letter.

## Cons:

We can’t guarantee that whether the receiver can decrypt it or not. Moreover, the time interval of decryption would depends on the ability of the receiver, which limits the use of encryption in daily lives as well. For instance, if you desperately want someone to get your message, encryption might not be the best choice.

# Discussion and Conclusion

## Discussion:

There exists the possibility that messages be intercepted by anyone else. To prevent it from happening, you can send the keyword of Vigenere cipher and the key matrix of Hill cipher respectively, which greatly reduces the possibility that the message be decrypted. Also, if you care more about the intensity of the encryption, this will help increase the difficulty of decryption.

## Conclusion:

Though Hill cipher is a relatively basic cipher in cryptography, if we didn't learn how to find the inverse matrix in this course, we might not be capable of understanding the basis of Hill cipher. Indeed, there are many other ways to encrypt the message, so we are deeply convinced that there are more bridges other than the two ciphers we mentioned above to connect linear algebra with cryptography.