Hill Cipher

Chelsea Beaton

April 2022

Abstract

The Hill Cipher is a polygraphic substitution cipher that employs some elementary linear algebra. Invented in 1929 by Lester Hill, the Hill Cipher is a relatively fast and simple method of encryption which involves multiplying blocks of letters by a key matrix to obtain an encrypted ciphertext message. This ciphertext message can then be decrypted by multiplying blocks of letters by the inverse of the key matrix modulo 27. Although this method of encryption is acceptable to use in certain scenarios, there are some major weaknesses associated with it that makes it not the most secure method to choose.

1 Introduction

Cryptography is 'a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.' [3] Encrypting a message usually follows this process: convert a readable (plaintext) message into an unreadable (ciphertext) message, send the ciphertext to someone else, and then when the ciphertext is received, convert the ciphertext back into plaintext so that it is readable once again. The process of transforming information so only certain people can read it is an old one. The first recorded evidence of cryptography was found in an inscription carved around 1900 BC in a tomb in Egypt. [4] Although it is not believed that this inscription was meant to be a secret message, it incorporated a transformation of original text, and it was the first known text to do so. Although the act of hiding secret messages has been around for thousands of years, systematic study of cryptography as a science just started around 100 years ago. [4] Since then, there have been many algorithms created to encrypt secret messages, and some are more successful than others.

There are many algorithms one can use to convert a readable plaintext message into an unreadable ciphertext message, and vice versa. These algorithms, called cryptographic algorithms, are typically sorted into two categories: symmetric key cryptography and asymmetric key cryptography. Symmetric key cryptography involves encrypting and decrypting the message with the same key and asymmetric key cryptography involves encrypting the message with one key, and decrypting it with a different one. Within these two categories, there are many different algorithms such as Advanced Encryption Standard (AES), Data

Encryption Standard (DES), Elliptic-Curve Cryptography (ECC), and Hill Cipher. In this paper, we will be analyzing the method of decryption using the Hill Cipher algorithm.

Hill Cipher is a 'polygraphic substitution cipher based on linear algebra.' [1] Polygraphic substitution means that a uniform substitution is performed on blocks of letters. Each letter in the alphabet is represented by a number (in this paper, we use A=1, B=2,..., Z=26 and 0 represents a space). To encrypt a plaintext message, the message is split into blocks of n letters, and each block of letters are multiplied by an invertible n by n matrix, against modulus 27. The blocks of letters can be represented by a 1 by n vector, p, and the key matrix can be represented by K. This gives the formula,

$$c = p \cdot K \tag{1}$$

where c is a vector that represents the encrypted block of plaintext, and each entry of c has been reduced c modulo 27. To encrypt the ciphertext message, each block of n encrypted letters is multiplied by the inverse of the key matrix, modulo 27 to get

$$p = c \cdot K^{-1}. \tag{2}$$

2 Method

In this paper, we will be decrypting two ciphers. The first cipher has $n = 2$ and the second has $n = 3$. When decrypting a cipher using Hill Cipher, we need to multiply each block of encrypted letters by the inverse of the key matrix, however in this project, we do not know the key matrix. This means the first thing we need to do is find the key matrix. In order to do this, we can find the blocks of letters that show up most frequently in the ciphertext, and match them to the blocks of letters that show up most frequently in the English language. For the first cipher, the ciphertext is broken into blocks of 2 encrypted letters. This means we will start by analyzing the bigrams that show up most frequently in this cipher. According to one website, the most frequent bigrams in our ciphertext are PB and ZI. [2] Although the most common bigrams in English are TH and HE, if we match PB and ZI to TH and HE, our resulting plaintext won't have many spaces. Because of that, we can look at the most common single letters in English and add a space to the start or end of the block to create a bigram. The most common letters in English are E and T, so we can match these letters (with a space) to PB and ZI to create a plaintext and ciphertext matrix, which can then be used to find the key. Rearranging equation (1), we can obtain the key by calculating

$$K = c \cdot p^{-1}. \tag{3}$$

Filling in the letters for each matrix (0 represents a space), we obtain

$$K = \begin{bmatrix} P & Z \\ B & I \end{bmatrix} \begin{bmatrix} E & 0 \\ 0 & T \end{bmatrix}^{-1}.$$

When we represent our bigrams with numbers we obtain the matrices,

$$K = \begin{bmatrix} 16 & 26 \\ 2 & 9 \end{bmatrix} \begin{bmatrix} 5 & 0 \\ 0 & 20 \end{bmatrix}^{-1} \pmod{27}.$$

When calculating the inverse of a matrix, we need the determinant of said matrix, and the adjoint of the matrix. If we have a matrix, $m = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we can calculate the determinant as $\det(m) = \frac{1}{ad-cb}$ or $det(m) = (ad - cb)^{-1}$. To find the adjoint of the 2 by 2 matrix m, we switch a and d and take the negative of b and c, $\text{adjoint}(m) = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$. We multiply the inverse of the determinant by the adjoint, and in this case, take it modulo 27.

When calculating the determinant modulo 27 of p, we get $\det(p) = (20 \cdot 5 - 0 \cdot 0) \pmod{27} = 100 \pmod{27} = 19$. We need the inverse of the determinant, $(\det(p))^{-1} = (19)^{-1} = 10$.

$$K = \begin{bmatrix} 16 & 26 \\ 2 & 9 \end{bmatrix} \left(\det(p)^{-1} \begin{bmatrix} 20 & 0 \\ 0 & 5 \end{bmatrix} \right) \pmod{27}$$

$$K = \begin{bmatrix} 16 & 26 \\ 2 & 9 \end{bmatrix} \left(10 \begin{bmatrix} 20 & 0 \\ 0 & 5 \end{bmatrix} \right) \pmod{27}$$

$$K = \begin{bmatrix} 16 & 26 \\ 2 & 9 \end{bmatrix} \begin{bmatrix} 11 & 0 \\ 0 & 23 \end{bmatrix} \pmod{27}.$$

Multiplying the matrices modulo 27, we get

$$K = \begin{bmatrix} 14 & 4 \\ 22 & 18 \end{bmatrix}.$$

Now that we have calculated our key matrix K, we can take the inverse of it (using the method described above) to get

$$K^{-1} = \begin{bmatrix} 19 & 25 \\ 16 & 7 \end{bmatrix}.$$

Now we can multiply each block of encrypted letters by K^{-1} to determine the plaintext message.

Determining the key matrix of the second cipher can be achieved using the same method as explained above. For the second cipher, the ciphertext is broken into blocks of 3 encrypted letters. This means we will start by analyzing the trigrams that show up most frequently

in this cipher. According to one website, the most frequent trigrams in our ciphertext are OQW, QDN and YIP. [2] Although the most common trigrams in English are THE, AND and ING, if we match OQW, QDN and YIP to these trigrams, our resulting plaintext won't have many spaces. In this case, we can't look at single letters because we don't use double spaces in English. Because of that, we look at the most common bigrams again, and add a space to the beginning or end of the bigram to create a trigram. The most common bigrams in English are TH, HE and IN. However, when looking at the frequencies of these bigrams and trigrams, TH has a frequency of 3.88%, HE has a frequency of 3.68%, IN has a frequency of 2.28% and THE has a frequency of 3.51%. We can see that THE shows up more frequently than IN, so we will use that instead. After some trial and error, we can match THE, (space)TH and HE(space) to OQW, QDN and YIP. In doing so, we get the ciphertext and plaintext matrices as

$$K = \begin{bmatrix} O & Q & Y \\ Q & D & I \\ W & N & P \end{bmatrix} \begin{bmatrix} T & 0 & H \\ H & T & E \\ E & H & 0 \end{bmatrix}^{-1} .$$

Representing these trigrams with their corresponding numbers we get,

$$K = \begin{bmatrix} 15 & 17 & 25 \\ 17 & 4 & 9 \\ 23 & 14 & 16 \end{bmatrix} \begin{bmatrix} 20 & 0 & 8 \\ 8 & 20 & 5 \\ 5 & 8 & 0 \end{bmatrix}^{-1} \pmod{27}.$$

To calculate the inverse of the plaintext matrix, we can compute the determinant modulo 27, $\det(p) = 20[(20\cdot 0)-(8\cdot 5)]-0[(8\cdot 0)-(5\cdot 5)]+8[(8\cdot 8)-(5\cdot 20)] = -1088 \pmod{27} = 19$. The inverse of the determinant modulo 27 is equal to 10. The adjoint of the matrix modulo 27 is equal to

$$adj = \begin{bmatrix} 14 & 10 & 2 \\ 25 & 14 & 18 \\ 18 & 2 & 22 \end{bmatrix}$$

and if we multiply it by the inverse of the determinant modulo 27, we obtain

$$p^{-1} = \begin{bmatrix} 5 & 19 & 20 \\ 7 & 5 & 18 \\ 18 & 20 & 4 \end{bmatrix} .$$

Now we can calculate $K = c \cdot p^{-1}$,

$$K = \begin{bmatrix} 15 & 17 & 25 \\ 17 & 4 & 9 \\ 23 & 14 & 16 \end{bmatrix} \begin{bmatrix} 5 & 19 & 20 \\ 7 & 5 & 18 \\ 18 & 20 & 4 \end{bmatrix} \pmod{27}.$$

$$K = \begin{bmatrix} 23 & 6 & 4 \\ 5 & 10 & 16 \\ 15 & 17 & 20 \end{bmatrix}$$

Now that we have calculated our key matrix K, we can take the inverse of it (using the method described above) to get

$$K^{-1} = \begin{bmatrix} 9 & 14 & 14 \\ 8 & 19 & 21 \\ 4 & 26 & 23 \end{bmatrix}.$$

Now we can multiply each block of encrypted letters by K^{-1} to determine the plaintext message.

3 Results

To obtain the decrypted plaintext for the first cipher (where $n = 2$), we can start by multiplying the first block of 2 letters, $c = XG$, representing it with the corresponding numbers, $c = [24, 7]$ and multiplying it by the inverse of the key matrix modulo 27,

$$p = \begin{bmatrix} 19 & 25 \\ 16 & 7 \end{bmatrix} \begin{bmatrix} 24 \\ 7 \end{bmatrix} \pmod{27} = \begin{bmatrix} 13 \\ 1 \end{bmatrix}.$$

When we convert these numbers back into letters we get our first block of plaintext, $p =$ MA. If we continue this process for more blocks of encrypted ciphertext, we get the plaintext message to be, "MARLEY WAS DEAD TO BEGIN WITH THERE IS NO DOUBT WHATEVER ABOUT THAT THE REGISTER OF HIS BURIAL WAS SIGNED BY THE CLERGYMAN..."

To obtain the decrypted plaintext for the second cipher (where $n = 3$), we can start by multiplying the first block of 3 letters, $c = OQW$, representing it with the corresponding numbers, $c = [15, 17, 23]$ and multiplying it by the inverse of the key matrix modulo 27,

$$p = \begin{bmatrix} 9 & 14 & 14 \\ 8 & 19 & 21 \\ 4 & 26 & 23 \end{bmatrix} \begin{bmatrix} 15 \\ 17 \\ 23 \end{bmatrix} \pmod{27} = \begin{bmatrix} 20 \\ 8 \\ 5 \end{bmatrix}.$$

When we convert these numbers back into letters we get our first block of plaintext, $p =$ THE. If we continue this process for more blocks of encrypted ciphertext, we get the plaintext message to be, "THE WONDERFUL WIZARD OF OZ THE CYCLONE DOROTHY LIVED IN THE MIDST OF THE GREAT KANSAS PRAIRIES..."

4 Analysis

4.1 Strengths of Hill Cipher

There are a lot of different algorithms that work well for encryption and decryption. When deciding which one is right to use in a particular instance, it is helpful to look at the strengths and weaknesses of each. One strength of the Hill Cipher method is that it is relatively simple to execute. Anyone with basic knowledge of linear algebra (matrix multiplication and taking the inverse of a matrix), can use the Hill Cipher to encrypt and decrypt messages. Another strength of the Hill Cipher is that it is relatively fast, and has high throughput. The Hill Cipher is one example of a symmetric encryption algorithm. Because the same key is used to encrypt and decrypt, symmetric encryption algorithms tend to be faster and take less computation power than asymmetric encryption algorithms.

4.2 Weaknesses of Hill Cipher

Although the Hill Cipher offers a relatively easy and fast method of encryption, there are also some drawbacks of choosing this method. One weakness of the Hill Cipher is if the key matrix is going to be shared with someone who is going to decrypt a ciphertext message, there needs to be a secure method of communication between the sender and the receiver. If a third party happens to intercept this method of communication, then they will be able to decipher the ciphertext message with ease. Setting up a secure method of communication between two people can be a challenge, especially if they happen to live far away from each other. Another weakness of the Hill Cipher is even if the key matrix is not sent with the ciphertext, the ciphertext can be broken relatively easily. As we have shown in this report, frequency analysis is a very effective way to decrypt a ciphertext. Unless the plaintext message exhibits significant deviations from standard linguistic patterns, it is quite simple to match the n-blocks of letters to the most common n-blocks in the English language, and set up a system of equations to figure out the key. One way to overcome this problem is to use bigger blocks of letters, and therefore have a bigger key matrix. As shown in this report, when we use frequency analysis to try to decrypt a ciphertext where $n = 3$, we have to examine the most common bigrams and trigrams in the English language. This is because we can add spaces to the bigrams to make them trigrams. As we increase the size of the text blocks, there will be more things to examine. For example, if $n = 4$, we would need to examine the most common bigrams, trigrams and quadrigrams. Another way to overcome this problem is to make it so the most common bigrams, trigrams, etc, in our plaintext message do not coincide with the most common ones in English. This will make it much more difficult for someone to guess which letters in the ciphertext correspond with certain letters in the plaintext. One more weakness of the Hill Cipher is in order to decrypt

a ciphertext message, the key matrix has to be invertible modulo 27. When inverting a matrix, we need to divide the transpose of the matrix by its determinant (this is the same as multiplying the transpose of the matrix by the inverse of its determinant). Since we are dealing with matrices modulo 27, we will not be able to find the inverse of the determinant modulo 27 of every matrix.

For example, if we had the matrix $m = \left(\begin{smallmatrix} 9 & 17 \\ 3 & 6 \end{smallmatrix}\right)$, $\det(m) = (9 \cdot 6) - (3 \cdot 17) = 144 - 57 = 93 \pmod{27} = 12$. When we try to find the multiplicative inverse of 12 mod 27, we find that there isn't one. This means that we would have to choose a new key matrix because this one can not be used to decrypt ciphertext messages.

5 Conclusion

The Hill Cipher provides a relatively simple method of encryption/decryption. Anyone with a basic understanding of linear algebra can use this method to encrypt plaintext and decrypt ciphertext. Although using the Hill Cipher has its advantages, it is not the most secure method of encryption, because it is very vulnerable to known plaintext attacks.[5] Also, there are a limited number of possible key matrices because the key matrix has to be invertible modulo 27. There have been many attempts at securing the Hill Cipher, but it is still not as secure as other methods of encryption. Even with these weaknesses, the Hill Cipher is still being studied today due to its simplicity and because it offers a very large throughput when compared to other methods.

References

[1] GeeksforGeeks. *Hill Cipher*. https://www.geeksforgeeks.org/hill-cipher/. accessed: April 3, 2022.

[2] Charles F. Rocca Jr. *Decrypting Hill's Cipher*. https://sites.wcsu.edu/mbxml/html/hill$_d$*ecrypt*$_s$*ection.h* accessed: April 4, 2022.

[3] Kathleen Richards. *Cryptography*. https://www.techtarget.com/searchsecurity/definition/cryptograph accessed: April 2, 2022.

[4] Huzaifa Sidhpurwala. *A Brief History of Cryptography*. https://www.redhat.com/en/blog/brief-history-cryptography. accessed: April 2, 2022.

[5] SecGroup Unive. *Known Plaintext Attacks*. https://secgroup.dais.unive.it/teaching/cryptography/know plaintext-attacks/. accessed: April 7, 2022.