The Hill Cipher

Allison Liu, Taron Townsend, Priscila Trevino, Sarah Zendle

December 11 2019

1 Abstract

In this project, we study the Hill cipher and its applications. We begin with an introduction of how the Hill cipher works and give an example of encryption and decryption using the Hill cipher. We then analyze the cipher's weaknesses and demonstrate an effective attack on the cipher. Finally, we describe some recent modifications and applications of the cipher and conclude that the cipher, while not as effective as many modern-day cryptosystems, has many practical uses.

2 Introduction

Cryptography is the study of secure communication techniques. The most notable cryptographic method that utilizes linear algebra is the Hill cipher, an encryption method invented in 1929 by Lester S. Hill.Hill, "Cryptography in an Algebraic Alphabet" Lester was praised by the US government for his work in modular ciphers and codes during his lifetime. The Hill cipher is a technique that draws upon linear algebra, number theory, and modular arithmetic. It was the first polygraphic substitution cipher to allow for operations on groups of more than three plaintext characters at a time, as well as the first cipher based purely on mathematics. Since 1929, many modifications have been made to the Hill cipher in order to improve its security. In this project, we demonstrate how the Hill cipher works, implement a 3x3 version of the cipher in MATLAB, and analyze the cryptographic method.

3 Background

We use the term *plaintext* to refer to the phrase to be encoded and use the term *ciphertext* to refer to the encoded phrase. The *key* is the "password" required to decode the message and for the Hill cipher it will remain private or kept secret between the sender and the receiver. *Cracking the code* means successfully decoding the message without the key.

4 Methods

The Hill cipher demonstrates a practical application of linear algebra to ciphers. The cipher itself is a linear transformation represented by the key matrix with respect to the standard basis. The plaintext vectors form the domain, while the ciphertext vectors form the codomain. “Hill-Cipher”

4.1 Encryption

To encode a message, an n x n invertible matrix with respect to the chosen arithmetic modular alphabet size should be used as the key. The matrix key must be invertible in order to decode the cipher text.

To encrypt, we multiply the key matrix by the vectors of plaintext characters.

$$\vec{y} = K\vec{x} \mod p \tag{1}$$

where p is the number of characters in the chosen alphabet, K is an nxn invertible matrix modulo p, $\vec{x}$ is a vector of size nx1 of plaintext characters, and $\vec{y}$ is a vector of size nx1 representing the ciphertext characters. If the modern English alphabet is used, then computations will be done modulo 26, since there are 26 letters in the English alphabet.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 1: Numeric representation of English alphabet

We represent the each letter of the alphabet using the corresponding numbers above. Note: In practice, ASCII values are often used, but it is easier to work with the above numbers for the sake of modular arithmetic by hand.

For example, to encode the message ”BUFFS” using the key ”DGBF” we write the both the key and plaintext as a vector and convert both to numeric representations.

$$K = \begin{bmatrix} D & G \\ B & F \end{bmatrix} \to \begin{bmatrix} 3 & 6 \\ 1 & 5 \end{bmatrix}$$

$$\begin{bmatrix} B \\ U \end{bmatrix} \to \begin{bmatrix} 1 \\ 20 \end{bmatrix}$$

$$\begin{bmatrix} F \\ F \end{bmatrix} \to \begin{bmatrix} 5 \\ 5 \end{bmatrix}$$

$$\begin{bmatrix} S \\ Z \end{bmatrix} \to \begin{bmatrix} 18 \\ 25 \end{bmatrix}$$

We then multiply the plaintext vectors by K and obtain the following result.

$$\begin{bmatrix}3 & 6\\1 & 5\end{bmatrix}\begin{bmatrix}1\\20\end{bmatrix} = \begin{bmatrix}123\\101\end{bmatrix} \mod 26 = \begin{bmatrix}19\\23\end{bmatrix}$$

$$\begin{bmatrix}3 & 6\\1 & 5\end{bmatrix}\begin{bmatrix}5\\5\end{bmatrix} = \begin{bmatrix}45\\30\end{bmatrix} \mod 26 = \begin{bmatrix}19\\4\end{bmatrix}$$

$$\begin{bmatrix}3 & 6\\1 & 5\end{bmatrix}\begin{bmatrix}18\\25\end{bmatrix} = \begin{bmatrix}204\\143\end{bmatrix} \mod 26 = \begin{bmatrix}22\\13\end{bmatrix}$$

The encoded message is "TXTEWN".

4.2 Decryption

To decode a message, we multiply the column vectors of the ciphertext by the inverse of the key matrix.

$$K^{-1} = d^{-1} * adj(K) \tag{2}$$

$$dd^{-1} = 1 \mod 26 \tag{3}$$

where d is the determinant of K.

We notice that in order to decode, K must be invertible and there must exist a d^{-1} that makes Equation 3 equal to 1 mod 26. For these two conditions to be met, we are limited to using only numbers that are relatively prime to our chosen alphabet size of 26. The determinant of the key matrix must be a number that is relatively prime to 26 in order for it to have an inverse that satisfies Equation 3.Lyons

These equation restrictions can be guaranteed if we simply choose an alphabet whose size is a prime number, because all numbers will be relatively prime to it. In the English language, it can be helpful to add some characters to the numeric representation shown in Figure 1, making the size of the alphabet 29.

,	.	?
26	27	28

Figure 2: Additional characters

The adjugate of a square matrix is the transpose of its cofactor matrix. For a 2x2 matrix, the adjugate matrix is defined as

$$adj\left(\begin{bmatrix}a & b\\c & d\end{bmatrix}\right) = \begin{bmatrix}d & -b\\-c & a\end{bmatrix} \tag{4}$$

.

To decode the message "TXTEWN", we first find the inverse of the key.

$$adj\left(\begin{bmatrix}3 & 6\\ 1 & 5\end{bmatrix}\right) = \begin{bmatrix}5 & -6\\ -1 & 3\end{bmatrix} \tag{5}$$

$$d = \begin{vmatrix}3 & 6\\ 1 & 5\end{vmatrix} = 15 - 6 = 9 \tag{6}$$

$$d * d^{-1} = 9 * d^{-1} = 1 \mod 26 \Rightarrow d^{-1} = 3 \tag{7}$$

$$K^{-1} = d^{-1} * adj(K) = 3 * \begin{bmatrix}5 & -6\\ -1 & 3\end{bmatrix} = \begin{bmatrix}15 & -18\\ -3 & 9\end{bmatrix} \tag{8}$$

$$\begin{bmatrix}15 & -18\\ -3 & 9\end{bmatrix}\begin{bmatrix}19\\ 23\end{bmatrix} = \begin{bmatrix}-129\\ 150\end{bmatrix} \mod 26 = \begin{bmatrix}1\\ 20\end{bmatrix}$$

$$\begin{bmatrix}15 & -18\\ -3 & 9\end{bmatrix}\begin{bmatrix}19\\ 4\end{bmatrix} = \begin{bmatrix}213\\ -21\end{bmatrix} \mod 26 = \begin{bmatrix}5\\ 5\end{bmatrix}$$

$$\begin{bmatrix}15 & -18\\ -3 & 9\end{bmatrix}\begin{bmatrix}22\\ 13\end{bmatrix} = \begin{bmatrix}96\\ 51\end{bmatrix} \mod 26 = \begin{bmatrix}18\\ 25\end{bmatrix}$$

The decoded text is "BUFFSZ", our original encoded message!

5 Cracking the Hill Cipher

The Hill cipher can be cracked fairly easily, without complex code or machinery. Because it is completely linear, simple linear algebraic techniques can be used to decrypt the message fairly quickly with minimal information.

5.1 Crib Dragging

A rudimentary yet effective method for smaller messages is known as *crib dragging*. If we assume the size of the decoding and encoding matrices, nn, and make a guess at a string of size greater than $n^2(n-1)$ to serve as known plaintext, the process of finding the decryption matrix is simple. For example, if we have an encrypted message "DGPBGOQZAUJI" and we know the plaintext "MARKS" is contained somewhere within the decrypted message, then "MARKS" must be in one of the following positions for a 2x2 decryption matrix:

DG	**PB**	**GO**	**QZ**	**...**
MA	RK	S		...
M	AR	KS		...
	MA	RK	S	...
	M	AR	KS	...
		...	...	

Consider the first possible position: If this were the correct position, then "MA" maps to "DG" and "RK" maps to "PB":

$$D\begin{bmatrix}M\\A\end{bmatrix} = \begin{bmatrix}D\\G\end{bmatrix}, D\begin{bmatrix}R\\K\end{bmatrix} = \begin{bmatrix}P\\B\end{bmatrix}$$

Converting the above vectors in alphabetic form to their numerical representations, we get

$$D\begin{bmatrix}12\\0\end{bmatrix} = \begin{bmatrix}3\\6\end{bmatrix} \mod 26, D\begin{bmatrix}17\\10\end{bmatrix} = \begin{bmatrix}15\\1\end{bmatrix} \mod 26$$

$$\begin{bmatrix}12 & 17\\0 & 10\end{bmatrix} D = \begin{bmatrix}3 & 15\\6 & 1\end{bmatrix} \mod 26$$

$$D = \begin{bmatrix}5 & 7\\19 & 4\end{bmatrix}\begin{bmatrix}15 & 12\\2 & 19\end{bmatrix}^{-1} \mod 26$$

We can then use this possible decryption matrix to attempt to break the cipher - if the message is not decoded, we "drag" the crib onto the next possible position and repeat the process until we find a viable solution.

5.2 Limitations

This method relies on the ability to take the modular inverse of the matrix created from the crib; for an encryption done using a 2x2 matrix, the known plaintext must again produce two invertible matrices (with respect to the chosen modulo) to compare to the encrypted message: if these are not present, the process will find no possible solutions and a different crib must be chosen.

In addition, while relatively fast for low-rank matrices and shorter cipher text, the amount of time this method takes to crack the code increases exponentially with both of these parameters (Figure 4).

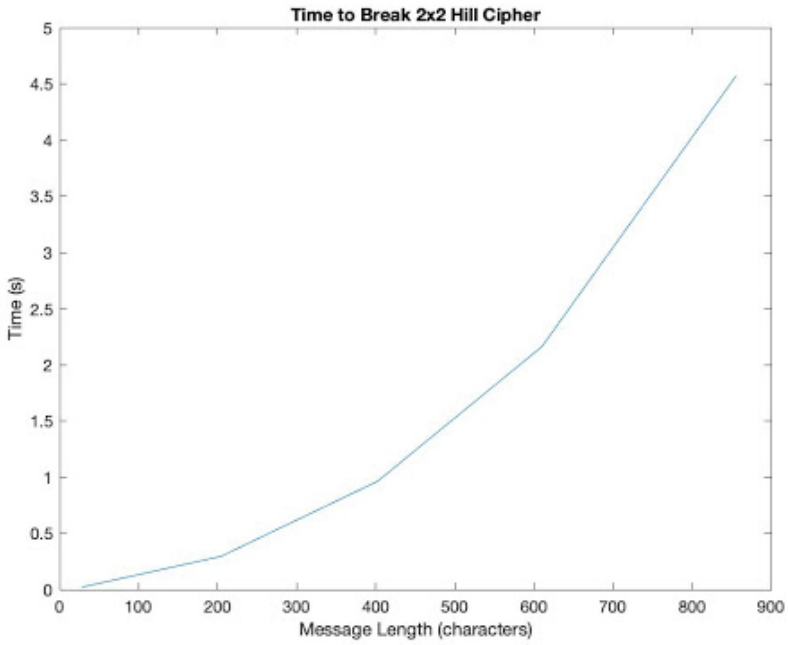

Figure 3: Graph of time vs. message length. The time to break the 2x2 Hill cipher increases exponentially with message length.

6 Extensions and Modifications

In 1949, Claude Shannon in describes two properties of a good cryptosystem—diffusion and confusion—that hinder attacks.Shannon Diffusion describes the distribution of frequency of characters. The Hill cipher diffuses well, because if a plaintext character is changed, multiple ciphertext characters will be altered, evening out the distribution of characters that appear; the same is true for the opposite scenario. This property can also be seen in matrix multiplication. Confusion refers to how the key is related to the ciphertext. Ideally, the key should change as the ciphertext changes, and the more the key changes, the better. The Hill cipher does not confuse well, because the key remains the same through all operations.Wade Trappe

Many modifications can be made to the Hill cipher in order to improve its security. The Hill cipher is vulnerable to attack because it is linear in nature. The first and most obvious is increasing the size of the key matrix, which will increase the computation time necessary to crack it. If the number of characters, p, in the chosen alphabet is a prime number, there will be p^{n*n} possible key matrices. The Hill cipher can also be trivially combined with shift ciphers such as the Caesar cipher, which shifts all characters of the alphabet by a certain

integer amount.

During his lifetime, Lester Hill himself suggested many improvements to the Hill cipher. Because it is not always trivial to determine the usability of a key matrix, Hill suggested using involutory (or self-invertible) matrices as keys in 1931.Hill, "Concerning Certain Linear Transformation Apparatus of Cryptography" This idea is used in many Hill cipher based encryption methods today. Additionally, Hill and Louis Weisner patented a physical "Message protector" in 1929 that used rotors to represent the matrices used to encrypt and decrypt.

Additionally, the Hill cipher can be combined with more modern-cryptographic techniques. One of these modifications involves changing the encryption key for each plaintext, thereby improving its "confusion" ability. In 2000, Saeedinia describes a modification to the Hill cipher by permuting the rows and columns of the key matrix after each operation.Saeedinia In 2009 and 2011, Toorani and Falahati use hash functions to change the encryption method for each operation.M. Toorani Both of these modifications, along with countless others have since been broken. Liam Keliher The Hill cipher is still being researched and improved upon today; Coggins and Glatzer presented an algorithm for combining the Hill cipher and an Enigma-based encoder in 2019 Porter E. Coggins IIIand Dawadeh et. al. published an image encryption technique by combining the Hill cipher with Elliptic Curve cryptography in 2018.Ziad E. Dawahdeh The applications of the Hill cipher are still relevant today.

7 Conclusion

The Hill cipher is a cipher that diffuses well, but due to its linearity can be cracked very easily. It is a cipher that can be extended in many interesting ways to improve its security, functionality, and practicality. We would like to further our understanding of the possible modifications of the Hill cipher, and its applications to other ideas, particularly image cryptography. Ultimately, however, due to the rapidly advancing field of cryptography, we conclude the Hill cipher will never be as effective or secure as modern-day cryptographic techniques, such as RSA cryptography and rising quantum cryptography methods.

8 References

Hill, Lester S. "Cryptography in an Algebraic Alphabet". *The American Mathematical Monthly* 36.6 (1929): 306–312. Print.

——."Concerning Certain Linear Transformation Apparatus of Cryptography". *The American Mathematical Monthly* 38.3 (1931): 135–154. Print.

Shannon, Claude. "Communication theory of secrecy systems". *Bell Systems Technical Journal* 28 (1949): 656–715. Print.

Saeedinia, S. "How to make the Hill Cipher secure". *Cryptologia* 24.4 (2000): 353–360. Print.

Wade Trappe, Lawrence Washington. *Introduction to Cryptography with Coding Theory*. Pearson, 2005. Print.

M. Toorani, A. Falahati. "A secure cryptosystem based on affine transformation". *Journal of Security and Communication Networks* 4.2 (2011): 207–215. Print.

Liam Keliher, Anthony Delaney. "Cryptanalysis of the Toorani-Falahati Hill Ciphers". *Proceedings - International Symposium on Computers and Communications* (2013). Print.

Ziad E. Dawahdeh, Shahrul N. Yaakob, Rozmie Razif bin Othman. "A new image encryption technique combinging Elliptic Curve Cryptosystem with Hill Cipher". *King Saud University* 30.3 (2018): 349–355. Print.

Porter E. Coggins III, Tim Glatzer. "An Algorithm for a Matrix-Based Enigma Encoder from a Variation of the Hill Cipher as an Application of 2 2 Matrices". *PRIMUS* 30.1 (2020): 1–18. Print.

"Hill-Cipher". (accessed: 12.09.2019). Web.

Lyons, James. "Practical Cryptography". (accessed: 12.09.2019). Web.

9 Attribution

Allison edited the report and wrote the introduction, background, and extensions and modifications sections. Taron wrote the program in MATLAB that implements the Hill cipher, as well as the MATLAB code summary in the appendix of the report. Priscila wrote the methods section of the report. Sarah wrote the cracking the Hill cipher section of the report, as well as the MATLAB code required to do the analysis. All members contributed to equally to this project.

10 Appendix

10.1 MATLAB code summary

The first part of the code identifies the phrase to be encrypted and the key by prompting the user to for inputs. The code then checks to ensure the key matrix will be invertible and that the determinant will not be a multiple of the modular base. The code then finds the length of the message that is going

to be scrambled. If the message is a length multiple of 3 then it breaks it into a matrix with 3 rows. This is so that the matrix will have the proper dimension to be multiplied with the key matrix. In cases where the encoded message is one or two letters short of being a perfect multiple of 3 then another element is added and then the code goes through the same steps to encode the message. The code then switches from letters to number through the ASCII values of the letters. It is at this step where the key and the message vectors are multiplied together. This creates another matrix containing the encoded message. This matrix is then reshaped to a row vector, and then switched back to the characters corresponding to their ASCII values.

The second section of the code decrypts encoded messages. It again begins by asking the user to enter the phrase that they want decrypted. This decryption also prompts the user for the length of the message that they are decrypting, because otherwise the code does not have enough information to determine which path to proceed on. The program then determines the inverse of the key and multiplies it by the numerical values corresponding to the ASCII encoded message. The final matrix is then resized to a row vector and transferred to character corresponding values.