Ryan Doyle

Hill's Cipher: Linear Algebra in Cryptography

Introduction:

Since the beginning of written language, humans have wanted to share information secretly. The information could be orders from a general in times of war, a message between secret admirers, or information regarding some of the world's most villainous crimes. It is this need for secrecy and its wide applications that gave rise to cryptography and have made it an area of study for thousands of years. In this paper, I will introduce the study of cryptography and some of the weaknesses of classical ciphers by looking at the Caesar cipher. Moving on from this introduction, I will focus on a linear algebra based cipher, the Hill cipher, which fixed the main problems associated with ciphers like the Caesar cipher. I will also analyze the shortcomings of the Hill cipher and introduce a method to improve the linear algebra behind it in order to make it more secure.

Caesar Cipher:

Until recently, encrypting secret messages was performed by hand using relatively trivial mechanisms to disguise information. One of the most well-known ciphers was named after Julius Caesar, namely, the Caesar cipher. The Caesar cipher is an example of a substitution cipher. Each letter of a given plaintext, the information to be encrypted, is substituted with another letter some given number of positions from it in the alphabet. For example, if we had an alphabet comprised of the standard 26 letters in the English alphabet and swapped each letter with the letter three places after it in the alphabet, we would have the following Caesar cipher (Luciano and Prichett, 3):

Plaintext:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Cipher text:

D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Using this cipher, the text "TOP SECRET MESSAGE" would encode to "WRS VHFUHW PHVVDJH."

One of the main problems with the Caesar cipher is that if an individual intercepts the cipher text and guesses that the Caesar cipher was used for the encryption, he or she could easily go through the 25 shift values until they come upon a shift that decodes the cipher text into a meaningful plaintext. On a broader scale, simple substitution ciphers all fall victim to simple analysis. Given any particular alphabetic language, certain letters are used more or less frequently than other letters. In a simple substitution cipher, these frequencies with which each letter occurs in an average sentence or paragraph are maintained. For example, if a substitution cipher encoded "e" to "w," "w" would occur in the cipher text with the same frequency as "e" in the original language, allowing for a relatively simple analysis to break the substitution cipher (Luciano and Prichett, 6).

Hill Cipher:

As time progressed, the study of cryptography continued to mature and, more recently, began to involve higher level mathematics. With this more advanced math came more advanced ciphers based

on the idea of encryption and decryption keys. Encryption keys are a special value or set of values used in an encryption algorithm to convert a plaintext into a cipher text. A decryption key is the opposite. Decryption keys are used as part of a decryption algorithm to convert the cipher text back into the original plaintext. One such example of an encryption scheme that utilizes more advanced mathematics, as well as encryption and decryption keys is a cipher from 1929 called the Hill cipher. The Hill cipher is based on linear algebra and overcomes the frequency distribution problem of the Caesar cipher that was previously discussed. The rest of this paper will be devoted to an explanation of the Hill cipher, its shortcomings, and one way to secure the cipher further.

For both encryption and decryption, the Hill cipher assigns numerical values to each letter of an alphabet. Throughout this paper, we will use the standard 26 character English alphabet and define the following associations between letters in our alphabet and numbers.

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

The computation used in the Hill cipher is based on linear algebra techniques. Before explaining the encryption and decryption procedures, it is important to recognize that the above alphabet is a linear space. Note the following (Hill 306-307):

1. The alphabet has a zero element. In this case, the zero element is "A." The numerical value of any letter $\alpha + A = \alpha$, just as any number added to 0 equals itself.
2. The alphabet is closed under modulo addition. The addition operator "+" is defined as modulo addition for use within this alphabet such that for the numerical values of two letters α and β, $\alpha + \beta = \gamma$ where γ is the remainder from dividing the sum of α and β by the size of the alphabet (26 in our case).
3. The alphabet is closed under modulo scalar multiplication. Scalar multiplication is defined for use within this alphabet such that for all numerical values of two letters α and β, $\alpha\beta = \gamma$ where γ is the remainder of the product of α and β divided by the size of the alphabet.

Encryption with the Hill Cipher:

Now that we know this alphabet is a linear space, we can perform linear transformations on it. Encrypting text using the Hill cipher is accomplished by breaking a given plaintext into blocks of size *n* (where *n* is an integer), writing these blocks as column vectors, and multiplying these column vectors by any invertible *n*x*n* matrix. The encryption matrix must be invertible because its inverse will be used to decrypt the cipher texts created with the Hill cipher and this encryption matrix. The invertibility of the encryption matrix allows us to say that its determinant must not be 0. The determinant of the encryption matrix must also be relatively prime to the size of the alphabet. In our case, any encryption matrix we choose must have a determinant that is relatively prime to 26 (Hill, 307-309). This condition allows for a randomized distribution of letters in the cipher text.

As an example, to encrypt the plaintext "TOP SECRET MESSAGE" with *n*=2, the process is as follows (University of Florida, 7 – 12):

1. Choose a 2x2 encryption matrix. For this example, we will use the matrix $\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix}$. This matrix has the determinant (3*7) – (2*5) = 21 – 10 = 11. Since 11 is ≠ 0, this matrix is invertible. 11 is also relatively prime to 26. These two qualities satisfy the requirements listed previously, making this encryption matrix a valid choice for use in the Hill cipher.
2. Split the plaintext into blocks of size 2 (ignoring spaces), determine the letters' numerical values, and align these as column vectors. If the length of the plaintext is not evenly divisible by 2, add a previously decided character to the end of the string until the plaintext is evenly divisible by 2.

$$\begin{vmatrix} T \\ O \end{vmatrix} = \begin{vmatrix} 19 \\ 14 \end{vmatrix} \quad \begin{vmatrix} P \\ S \end{vmatrix} = \begin{vmatrix} 15 \\ 18 \end{vmatrix} \quad \begin{vmatrix} E \\ C \end{vmatrix} = \begin{vmatrix} 4 \\ 2 \end{vmatrix} \quad \begin{vmatrix} R \\ E \end{vmatrix} = \begin{vmatrix} 17 \\ 4 \end{vmatrix} \quad \begin{vmatrix} T \\ M \end{vmatrix} = \begin{vmatrix} 19 \\ 12 \end{vmatrix}$$

$$\begin{vmatrix} E \\ S \end{vmatrix} = \begin{vmatrix} 4 \\ 18 \end{vmatrix} \quad \begin{vmatrix} S \\ A \end{vmatrix} = \begin{vmatrix} 18 \\ 0 \end{vmatrix} \quad \begin{vmatrix} G \\ E \end{vmatrix} = \begin{vmatrix} 6 \\ 4 \end{vmatrix}$$

3. Multiply each of these column vectors by the encryption matrix and take modulo 26 of the result.

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 19 \\ 14 \end{vmatrix} = \begin{vmatrix} (3*19)+(2*14) \\ (5*19)+(7*14) \end{vmatrix} = \begin{vmatrix} 85 \\ 193 \end{vmatrix} = \begin{vmatrix} 7 \\ 11 \end{vmatrix} \text{ (modulo 26)}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 15 \\ 18 \end{vmatrix} = \begin{vmatrix} (3*15)+(2*18) \\ (5*15)+(7*18) \end{vmatrix} = \begin{vmatrix} 81 \\ 201 \end{vmatrix} = \begin{vmatrix} 3 \\ 19 \end{vmatrix} \text{ (modulo 26)}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 4 \\ 2 \end{vmatrix} = \begin{vmatrix} (3*4)+(2*2) \\ (5*4)+(7*2) \end{vmatrix} = \begin{vmatrix} 16 \\ 34 \end{vmatrix} = \begin{vmatrix} 16 \\ 8 \end{vmatrix} \text{ (modulo 26)}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 17 \\ 4 \end{vmatrix} = \begin{vmatrix} (3*17)+(2*4) \\ (5*17)+(7*4) \end{vmatrix} = \begin{vmatrix} 59 \\ 113 \end{vmatrix} = \begin{vmatrix} 7 \\ 9 \end{vmatrix} \text{ (modulo 26)}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 19 \\ 12 \end{vmatrix} = \begin{vmatrix} (3*19)+(2*12) \\ (5*19)+(7*12) \end{vmatrix} = \begin{vmatrix} 81 \\ 179 \end{vmatrix} = \begin{vmatrix} 3 \\ 23 \end{vmatrix} \text{ (modulo 26)}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 4 \\ 18 \end{vmatrix} = \begin{vmatrix} (3*4)+(2*18) \\ (5*4)+(7*18) \end{vmatrix} = \begin{vmatrix} 48 \\ 146 \end{vmatrix} = \begin{vmatrix} 22 \\ 16 \end{vmatrix} \text{ (modulo 26)}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 18 \\ 0 \end{vmatrix} = \begin{vmatrix} (3*18)+(2*0) \\ (5*18)+(7*0) \end{vmatrix} = \begin{vmatrix} 54 \\ 90 \end{vmatrix} = \begin{vmatrix} 2 \\ 12 \end{vmatrix} \text{ (modulo 26)}$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix} \begin{vmatrix} 6 \\ 4 \end{vmatrix} = \begin{vmatrix} (3*6)+(2*4) \\ (5*6)+(7*4) \end{vmatrix} = \begin{vmatrix} 26 \\ 58 \end{vmatrix} = \begin{vmatrix} 0 \\ 6 \end{vmatrix} \text{ (modulo 26)}$$

4. Convert each of the matrices obtained in step 3 to their alphabetical vectors and combine them to produce the cipher text.

$$\begin{vmatrix} 7 \\ 11 \end{vmatrix} = \begin{vmatrix} H \\ L \end{vmatrix} \quad \begin{vmatrix} 3 \\ 19 \end{vmatrix} = \begin{vmatrix} D \\ T \end{vmatrix} \quad \begin{vmatrix} 16 \\ 8 \end{vmatrix} = \begin{vmatrix} Q \\ I \end{vmatrix} \quad \begin{vmatrix} 7 \\ 9 \end{vmatrix} = \begin{vmatrix} H \\ J \end{vmatrix} \quad \begin{vmatrix} 3 \\ 23 \end{vmatrix} = \begin{vmatrix} D \\ X \end{vmatrix}$$

$$\begin{vmatrix} 22 \\ 16 \end{vmatrix} = \begin{vmatrix} W \\ Q \end{vmatrix} \quad \begin{vmatrix} 2 \\ 12 \end{vmatrix} = \begin{vmatrix} C \\ M \end{vmatrix} \quad \begin{vmatrix} 0 \\ 6 \end{vmatrix} = \begin{vmatrix} A \\ G \end{vmatrix}$$ Cipher text: HLDTQIHJDXWQCMAG

This completes the process of the Hill cipher's encryption by matrix multiplication. We can see that the plaintext "TOP SECRET MESSAGE" encodes to "HLDTQIHJDXWQCMAG." It is important to note

that the Hill cipher overcomes the frequency distribution problem associated with simple substitution ciphers, such as the Caesar cipher. Since the encryption is not simply based on replacing certain characters with others but, instead, on linear transformations of blocks of characters, the frequencies of each letters' appearance in the language have been masked. In fact, the cipher text in the above case makes this even easier to see because it has more characters in it than the original plaintext.

Decryption with the Hill Cipher:

From here, we are interested in how the party receiving a secret message encoded by the Hill cipher can decode it into the original plaintext. As previously described, the Hill cipher is based on matrix multiplication and any encryption matrix used in the Hill cipher must be invertible. For three *n*x*n* matrices A, B, and C where AB = C and A is invertible, we know that $B = A^{-1}C$. Using this, we know we can decrypt an encoded message by multiplying it by the inverse of the encryption matrix. Due to the modulo arithmetic involved in this cipher, we need to find A^{-1} such that $AA^{-1} = I_n$ mod 26. From here, the cipher text is split into blocks of size *n* and multiplied by the inverse matrix. The process is the same as encryption, but with the inverse matrix instead of the original encryption matrix. Decryption of the cipher text "HLDTQIHJDXWQCMAG" with the 2x2 encryption matrix previously defined would go as follows:

1. Find A^{-1}

   $\det(\begin{vmatrix} 3 & 2 \\ 5 & 7 \end{vmatrix})$ = (3*7) – (2*10) = 11 $\quad$ 11^{-1} modulo 26 = 19

   $$19 \begin{vmatrix} 7 & -2 \\ -5 & 3 \end{vmatrix} = \begin{vmatrix} 133 & -38 \\ -95 & 57 \end{vmatrix} = \begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \text{ (modulo 26)}$$

2. Split the cipher text into blocks of 2, determine the letters' numerical values, and align these as column vectors.

   $$\begin{vmatrix} H \\ L \end{vmatrix} = \begin{vmatrix} 7 \\ 11 \end{vmatrix} \quad \begin{vmatrix} D \\ T \end{vmatrix} = \begin{vmatrix} 3 \\ 19 \end{vmatrix} \quad \begin{vmatrix} Q \\ I \end{vmatrix} = \begin{vmatrix} 16 \\ 8 \end{vmatrix} \quad \begin{vmatrix} H \\ J \end{vmatrix} = \begin{vmatrix} 7 \\ 9 \end{vmatrix} \quad \begin{vmatrix} D \\ X \end{vmatrix} = \begin{vmatrix} 3 \\ 23 \end{vmatrix}$$

   $$\begin{vmatrix} W \\ Q \end{vmatrix} = \begin{vmatrix} 22 \\ 16 \end{vmatrix} \quad \begin{vmatrix} C \\ M \end{vmatrix} = \begin{vmatrix} 2 \\ 12 \end{vmatrix} \quad \begin{vmatrix} A \\ G \end{vmatrix} = \begin{vmatrix} 0 \\ 6 \end{vmatrix}$$

3. Multiply each of these column vectors by the decryption matrix calculated in step 1 and take modulo 26 of the result.

   $$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 7 \\ 11 \end{vmatrix} = \begin{vmatrix} (3*7)+(14*11) \\ (9*7)+(5*11) \end{vmatrix} = \begin{vmatrix} 175 \\ 118 \end{vmatrix} = \begin{vmatrix} 19 \\ 14 \end{vmatrix} \text{ modulo 26}$$

   $$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 3 \\ 19 \end{vmatrix} = \begin{vmatrix} (3*3)+(14*19) \\ (9*3)+(5*19) \end{vmatrix} = \begin{vmatrix} 275 \\ 122 \end{vmatrix} = \begin{vmatrix} 15 \\ 18 \end{vmatrix} \text{ modulo 26}$$

   $$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 16 \\ 8 \end{vmatrix} = \begin{vmatrix} (3*16)+(14*8) \\ (9*16)+(5*8) \end{vmatrix} = \begin{vmatrix} 160 \\ 184 \end{vmatrix} = \begin{vmatrix} 4 \\ 2 \end{vmatrix} \text{ modulo 26}$$

   $$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 7 \\ 9 \end{vmatrix} = \begin{vmatrix} (3*7)+(14*9) \\ (9*7)+(5*9) \end{vmatrix} = \begin{vmatrix} 147 \\ 108 \end{vmatrix} = \begin{vmatrix} 17 \\ 4 \end{vmatrix} \text{ modulo 26}$$

   $$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 3 \\ 23 \end{vmatrix} = \begin{vmatrix} (3*3)+(14*23) \\ (9*3)+(5*23) \end{vmatrix} = \begin{vmatrix} 331 \\ 142 \end{vmatrix} = \begin{vmatrix} 19 \\ 12 \end{vmatrix} \text{ modulo 26}$$

$$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 22 \\ 16 \end{vmatrix} = \begin{vmatrix} (3*22)+(14*16) \\ (9*22)+(5*16) \end{vmatrix} = \begin{vmatrix} 290 \\ 278 \end{vmatrix} = \begin{vmatrix} 4 \\ 18 \end{vmatrix} \text{ modulo 26}$$

$$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 2 \\ 12 \end{vmatrix} = \begin{vmatrix} (3*2)+(14*12) \\ (9*2)+(5*12) \end{vmatrix} = \begin{vmatrix} 174 \\ 78 \end{vmatrix} = \begin{vmatrix} 18 \\ 0 \end{vmatrix} \text{ modulo 26}$$

$$\begin{vmatrix} 3 & 14 \\ 9 & 5 \end{vmatrix} \begin{vmatrix} 0 \\ 6 \end{vmatrix} = \begin{vmatrix} (3*0)+(14*6) \\ (9*0)+(5*6) \end{vmatrix} = \begin{vmatrix} 84 \\ 30 \end{vmatrix} = \begin{vmatrix} 6 \\ 4 \end{vmatrix} \text{ modulo 26}$$

4. Convert each of the matrices obtained in step 3 to their alphabetic vectors and combine them to produce the original plaintext.

$$\begin{vmatrix} 19 \\ 14 \end{vmatrix} = \begin{vmatrix} T \\ O \end{vmatrix} \quad \begin{vmatrix} 15 \\ 18 \end{vmatrix} = \begin{vmatrix} P \\ S \end{vmatrix} \quad \begin{vmatrix} 4 \\ 2 \end{vmatrix} = \begin{vmatrix} E \\ C \end{vmatrix} \quad \begin{vmatrix} 17 \\ 4 \end{vmatrix} = \begin{vmatrix} R \\ E \end{vmatrix} \quad \begin{vmatrix} 19 \\ 12 \end{vmatrix} = \begin{vmatrix} T \\ M \end{vmatrix}$$

$$\begin{vmatrix} 4 \\ 18 \end{vmatrix} = \begin{vmatrix} E \\ S \end{vmatrix} \quad \begin{vmatrix} 18 \\ 0 \end{vmatrix} = \begin{vmatrix} S \\ A \end{vmatrix} \quad \begin{vmatrix} 6 \\ 4 \end{vmatrix} = \begin{vmatrix} G \\ E \end{vmatrix}$$ Original plaintext: TOPSECRETMESSAGE

At this point, the cipher text has been decrypted into the original plaintext, minus the original spaces. Spaces can either be added by the recipient or an alphabet could be devised that would include a space character. For example, the character "_" could be added to our alphabet as having the numerical value 26 and all of our modulo functions would change to modulo 27 to adjust for the fact there would now be 27 characters in the alphabet. This modified alphabet would allow for encryption of the space character within messages.

Analysis of the Hill Cipher:

Since the Hill cipher is strictly based on matrix multiplication and inverses, it is quickly and easily computed and it overcomes the frequency distribution problem of earlier algorithms. This linearity, however, is still subject to simple attacks. If an attacker intercepted enough plaintext and cipher text pairs, a linear system could be set up to calculate the encryption matrix (Ismail et. al, 2023). That is, with encryption matrix A, given enough plaintext and cipher text pairs B and C, an attacker could solve $AB = C$ for A by manipulating the equation to $A = CB^{-1}$. Since this is simply solving a linear system, it is a relatively easy task. After an attacker computes A, he or she could easily compute A^{-1}, the decryption matrix, and the entire encryption scheme would be compromised for that particular encryption matrix A. In order to continue using the Hill cipher, the communicating parties would need to meet up and mutually agree upon a new encryption matrix A that could, again, be easily computed by an attacker with enough plaintext and cipher text pairs.

Another problem related to the Hill cipher's strict linearity is that the Hill cipher encodes every identical matrix B to the same matrix C. For example, in our previous encryption, the block $\begin{vmatrix} T \\ O \end{vmatrix}$ encrypted to $\begin{vmatrix} H \\ L \end{vmatrix}$. For every block $\begin{vmatrix} T \\ O \end{vmatrix}$ in a plaintext, that block will always be encoded to $\begin{vmatrix} H \\ L \end{vmatrix}$ when the encryption matrix from our example is used.

The problems that arise from this scenario are more easily demonstrated with images. Suppose that instead of text being encrypted, images were being encrypted. If an image was made of predominantly white pixels with an object in the center, the Hill cipher would encrypt all of the blocks of white pixels to the same values, in the same way it encrypted all blocks of $\begin{vmatrix} T \\ O \end{vmatrix}$ to $\begin{vmatrix} H \\ L \end{vmatrix}$ using the encryption matrix from our example. Since all of the blocks of white pixels are encrypted to the same

cipher text blocks, the general shape of the object in the center of the image is preserved. The following images illustrate this point (Ismail et. al, 2026). It is easy to see that encrypting this image with the Hill Cipher did nothing to prevent unwanted eyes from understanding the transmitted data. That is, the Nike symbol is still clearly visible, even if it is slightly distorted.

Nike

Original Hill

These images illustrate how the Hill cipher does very little to hide the data in a plaintext with many identical blocks. Note that all of the white pixels encrypted to the same pattern, leaving the Nike symbol identifiable. Source: Ismail et. al, 2026

Securing the Hill Cipher:

Several solutions for these problems have been proposed as means of securing the Hill cipher. One such solution, named HillMRIV by its authors, is to systematically alter the encryption matrix for every block being encrypted. Suppose we were working with our previously defined 26 character alphabet and were encrypting text using the following 3x3 encryption matrix: $\begin{vmatrix} 3 & 11 & 9 \\ 13 & 8 & 21 \\ 3 & 19 & 16 \end{vmatrix}$ Note that the determinant of this matrix is -401, meaning that this matrix is invertible. Normally, for use in the Hill cipher, a matrix has to be both invertible and have a determinant that is relatively prime to the number of letters in the alphabet. This modified Hill cipher algorithm does not require this feature of the matrix for reasons that will become evident later.

Instead of the communicating parties sharing just this encryption matrix, they can also share a random vector with the same length as the rows of the encryption matrix. For example, the vector v = $|7 \quad 2 \quad 15|$ satisfies this requirement for the 3x3 matrix above. For each block of information to be encrypted by this modified Hill cipher, the encryption matrix is adjusted by multiplying one of its rows by v and taking the product modulo 26, in sequential order. For example:

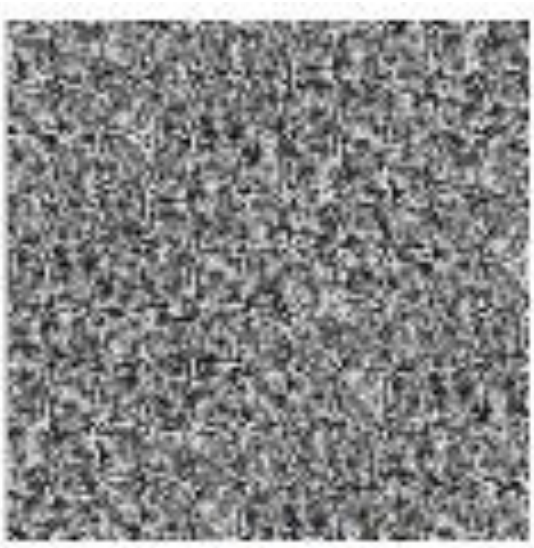
$$\begin{vmatrix} 7*3 & 2*11 & 15*9 \\ 13 & 8 & 21 \\ 3 & 19 & 16 \end{vmatrix} = \begin{vmatrix} 21 & 22 & 135 \\ 13 & 8 & 21 \\ 3 & 19 & 16 \end{vmatrix} = \begin{vmatrix} 21 & 22 & 5 \\ 13 & 8 & 21 \\ 3 & 19 & 16 \end{vmatrix} \text{ modulo 26,}$$

$$\begin{vmatrix} 21 & 22 & 5 \\ 7*13 & 2*8 & 15*21 \\ 3 & 19 & 16 \end{vmatrix} = \begin{vmatrix} 21 & 22 & 5 \\ 91 & 16 & 315 \\ 3 & 19 & 16 \end{vmatrix} = \begin{vmatrix} 21 & 22 & 5 \\ 13 & 16 & 3 \\ 3 & 19 & 16 \end{vmatrix}$$ modulo 26, and

$$\begin{vmatrix} 21 & 22 & 5 \\ 91 & 16 & 315 \\ 7*3 & 2*19 & 15*16 \end{vmatrix} = \begin{vmatrix} 21 & 22 & 5 \\ 13 & 16 & 3 \\ 21 & 38 & 240 \end{vmatrix} = \begin{vmatrix} 21 & 22 & 5 \\ 13 & 16 & 3 \\ 21 & 12 & 6 \end{vmatrix}$$ modulo 26 would be used to encrypt the first, second, and third blocks, respectively, of a plaintext. For each of the remaining blocks of plaintext, the process would continue, starting once again by multiplying the first row of $\begin{vmatrix} 21 & 22 & 5 \\ 13 & 16 & 3 \\ 21 & 12 & 6 \end{vmatrix}$ by v (Ismail et. al, 2023-2024). Besides this modification of the encryption matrix, the process of encryption using this modified Hill cipher is identical to that of the original Hill cipher. Decryption is also similar to the original Hill cipher, with the difference being that the decryption matrix for each block must be computed separately to correspond with the varying encryption matrices.

Performing the encryption with this variation adds a layer of complexity that is much harder to crack without knowledge of both the original encryption matrix and the vector v, while maintaining the properties of the Hill cipher that overcome the frequency distribution problem previously discussed. This system is harder to crack because for any given number of blocks, the blocks will all be encoded with a different encryption matrix, preventing this cipher from being broken by solving a simple linear system, as was possible with the original Hill cipher. It should also be noted that since each block is encrypted with a different encryption matrix, this modified Hill cipher properly encrypts plaintexts with duplicate blocks. A comparison of results from the original Hill cipher and this modified cipher, HillMRIV, are shown below.

Original Hill



HillMRIV

These images show the results of the HillMRIV cipher compared to the results of the original Hill cipher when encrypting an image of the Nike logo on a white background. Source: Ismail et. al, 2026

Conclusions:

In this paper, I have demonstrated the importance of linear algebra in cryptography by introducing one of the most well-known ciphers, Caesar's cipher, and demonstrating how its major flaw was overcome by Lester. S. Hill's Hill cipher in 1929. I then demonstrated a major security flaw in the Hill cipher and showed how further linear-algebra based computation can be used to better secure the cipher. All of this shows that cryptography is among the wide range of uses for linear algebra in everyday life. While there are many cryptographic schemes and ciphers currently in production environments and being researched around the world, this paper shows that linear algebra has a place in cryptography, serving purposes from securing instant messages to protecting email accounts to simply hiding a journal from the rest of the world.

Works Cited

Hill, Lester S. "Cryptography in an Algebraic Alphabet." *The American Mathematical Monthly* 36.6 (1929): 306-12. *JSTOR*. Web. 8 Mar. 2013. <http://www.jstor.org/stable/2298294>.

Ismail, I. A., Mohammed Amin, and Hossam Diab. "How to Repair the Hill Cipher." *Journal of Zhejiang University SCIENCE A* 7.12 (2006): 2022-030. *Springer Link*. Web. 8 Mar. 2013. <http://link.springer.com/article/10.1631%2Fjzus.2006.A2022#>.

Luciano, Dennis, and Gordon Prichett. "Cryptology: From Caesar Ciphers to Public-key Cryptosystems." *The College Mathematics Journal* 18.1 (1987): 2-17. *JSTOR*. Mathematical Association of America. Web. <http://www.jstor.org/stable/2686311>.

University of Florida, “How to Encipher and Decipher Codes using the Hill 2-Cipher,” Web. 8 Apr. 2013. <http://courses.writing.ufl.edu/3254/Examples%20and%20Readings/InstructionManualExample.doc>.