Project 3 - Eleanor Miranda

Eleanor Miranda

November 26, 2024

1 Introduction

Cryptology is the study of creating and breaking ciphers for the purpose of secret communication. Cryptanalysis is the science of finding techniques to decrypt these codes. Cryptology has been around for centuries, dating back to the creation of written languages [1]. Mathematicians throughout history have created many different types of ciphers, which vary in security. When it comes to ciphers, there are plaintext messages and ciphertext messages. Plaintext refers to the message in its original form, while ciphertext refers to the message after it has been encrypted. In addition, a key acts as additional information that is used in the encryption and decryption of plaintext messages and is known by both the sender and the receiver of the code [2]. One well-known type of cipher is a substitution cipher. A substitution cipher is a type of cipher in which the plaintext message is substituted by the corresponding letters that create the ciphertext message [3]. Furthermore, a polygraphic substitution cipher is a cipher in which the plaintext is "divided into groups of adjacent letters of the same fixed length n, and then each such group is transformed into a different group of n letters" [4].

One particular polygraphic substitution cipher is the Hill cipher, created by Lester Hill in 1929 with the intention of making a more secure encryption system. The Hill cipher was created during a time when most other ciphers were only able to encrypt larger blocks of letters into ciphertext. Instead of the simpler methods of previous ciphers for encryption, the Hill cipher uses topics from linear algebra, including matrix transformations over finite fields, to encrypt the plaintext into ciphertext, with the key being an n x n invertible matrix [3]. During its time, the Hill cipher proved to be more useful than previous substitution ciphers because it was one of the "first systematic yet simple polygraphic ciphers using more than two letters per group" [4]. Due to it being a polygraphic substitution cipher, the Hill cipher shows resistance to frequency analysis attacks. Furthermore, it was one of the first general methods of encryption that uses linear algebra in a feasible way [4].

As newer encryption methods were created and mathematicians spent time trying to decrypt Hill ciphers, the Hill cipher suffered several weaknesses. One of the key weaknesses of this cipher is its vulnerability to known plaintext attacks. If the attacker knows some of the plaintext and its corresponding ciphertext, then it wouldn't be difficult to figure out the key using the information they already know [1]. In addition, the Hill cipher has a small key space, as there are a limited number of possible keys that can be used [5]. A third weakness is that the encrypted message may not be able to be decrypted if the key matrix

is not invertible, since the method of decryption is to apply the inverse of the key matrix to the ciphertext [6]. As discussed further below, many mathematicians have developed modifications that can be applied to the Hill cipher to provide more security.

2 Literature Review

Due to its vulnerability to known plaintext attacks, as well as the inability to be decrypted if the key matrix is not invertible, many mathematicians have come up with modifications that can help make the Hill cipher more secure [1]. In Sachin Jain and Khushboo Arya's article titled "A Neoteric Strategy of Hill Cipher for Analysis of Degenerate Matrices Key," a new approach to the encryption and decryption processes of the Hill cipher are introduced to combat the original cipher's weaknesses to zero vulnerability due to degenerate matrices, which are matrices with a determinant of zero. Jain and Arya propose a new algorithm in which the first step in encryption is to find the determinant of the key matrix. If the determinant is greater than or equal to zero, then the compensate value is set to equal one, whereas if the determinant is less than zero, then the value is set to equal negative one. This value is then applied to the key matrix, creating a modified key matrix. The modified key matrix is then multiplied to the plaintext mod 29, resulting in the ciphertext, like how the inverse of the key matrix is multiplied to the plaintext mod 26 in the original Hill cipher. The algorithm for decryption, however, is not as simple as performing the encryption steps in reverse, as the original Hill cipher does. The first step to decrypt the ciphertext using this modified system is to find the determinant of the modified key matrix mod 29. If the determinant is less than or equal to zero, then X is set to equal X + 29, whereas if the determinant is greater than zero, X is set to equal itself. Next, the value for i is found in the equation i * X mod 29 = 1 and set to equal Y. Then, the inverse of the modified key matrix is found by multiplying the modified key matrix by Y mod 29. This inverse matrix is then transposed, which means that the rows and columns are swapped. Finally, the plaintext is found by multiplying the ciphertext by the transposed inverse matrix mod 29 [1]. Altogether, this article provides a new method of encryption and decryption of the Hill cipher that accounts for some of its weaknesses, including zero vulnerability due to having a degenerate key matrix. However, while diagrams depicting the encryption and decryption processes were included, the authors do not provide examples to support their explanations, which makes it more difficult for the reader to understand.

While Jain and Arya proposed a modified Hill cipher that modifies the key matrix during encryption to resolve the degenerate key matrix issue, Acharya et al. approach the issue of generating a non-invertible key matrix a different way in their article titled "Image Encryption Using Advanced Hill Cipher Algorithm." Instead of modifying the key matrix, and then eventually having to find the inverse of said modified matrix, Acharya et al. incorporate an involuntary key matrix in their advanced algorithm. The article references previous research in which an involuntary key matrix is used for encryption. The algorithm is described in Figure 1 [6].

Acharya et al. discover that when the classic Hill cipher is used to encrypt images that consist of large areas of the same color, the cipher is not able to encrypt them correctly. So, they incorporate this algorithm into their own algorithm called AdvHill, which they use to

Algorithm:

1. Select any arbitrary $\frac{n}{2} \times \frac{n}{2}$ matrix A_{22}.
2. Obtain $A_{11} = -A_{22}$.
3. Take $A_{12} = k(I - A_{11})$ or $k\ (I + A_{11})$ where k is a scalar constant.
4. Then, $A_{21} = \frac{1}{k}(I + A_{11})$ or $\frac{1}{k}(I - A_{11})$.
5. Form the matrix completely.

Figure 1: Encryption Algorithm using Involuntary Key Matrix [6]

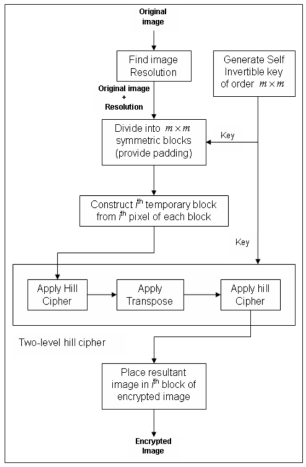

Figure 2: The block diagram for proposed AdvHill algorithm. [6]

encrypt images. The first step of their algorithm is to construct an involuntary key matrix of dimensions mxm. The next step is to divide the plain image into mxm symmetric blocks. Then, the i^{th} pixels of each block are brought together to form a temporary block, where the Hill cipher is applied first, then the matrix is transposed, and then the Hill cipher is applied again. Finally, the resulting matrix is placed into the i^{th} block of the encrypted image. This process can be seen in Figure 2. As a result, the images that the original Hill cipher was not able to encrypt properly can now be encrypted using this modified algorithm. This algorithm is also designed to be more secure against brute force and known plaintext attacks [6]. Overall, while there is not much background provided when it comes to image encryption, this article is effective in clearly explaining the mathematical background of the Hill cipher, as well as providing examples to assist in understanding.

In their article titled "A New Approach of Classical Hill Cipher in Public Key Cryptography," Hasoun et al. expand upon the idea of using an involuntary matrix for encryption rather than facing the problem of coming across a non-invertible key matrix. Instead of just implementing the involuntary key matrix, they approach encryption by first the Hill cipher, then the RSA algorithm. According to the article, the RSA algorithm is a public key system created by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1978 that uses

number theory for encryption and decryption. This algorithm consists of three steps, which are generation, encoding, and decoding. The steps to generate the public and private keys are shown in Figure 3 [5].

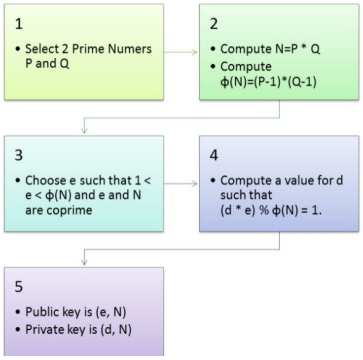

Figure 3: Generation Step of RSA [5]

After generating the public and private keys, the next step is to generate the involuntary key matrix, as Acharya et al. explained in their article on image encryption. Next, the Hill cipher is applied to encrypt the plaintext using the involuntary key matrix. Then, the RSA algorithm is used to encrypt the ciphertext given from the previous step using the public key, resulting in the final ciphertext. To decrypt the ciphertext, first the private key from the RSA algorithm is used. Then, the involuntary key matrix is used to decrypt the ciphertext from the previous step back into the plaintext. Combining these two encryption and decryption algorithms results in a more secure modification of the Hill cipher that removes the issue of the invertible key matrix [5]. Altogether, this article provides much detail in the step-by-step processes of encryption and decryption, and there are many examples and diagrams to support the explanations as well.

3 Theoretical Foundations

3.1 The Classic Hill Cipher

The Hill cipher encrypts plaintext into ciphertext using a combination of modular arithmetic and matrix multiplication, as described later. This cipher uses n x n square invertible matrices along with modulo 26 in order to encrypt plaintext messages [3]. The classic Hill cipher is encrypted and decrypted in mod 26 due to there being 26 letters of the English alphabet. To encrypt a message, the plaintext is converted into numbers, as shown in Table 1, divided into groups of length n, and are multiplied by the key matrix, where the resulting numbers are converted back into letters. To decrypt a message, the process is repeated in reverse. The ciphertext is converted into numbers, which are then divided into groups of length n, and then multiplied by the inverse of the key matrix, where the resulting numbers are converted back into the plaintext [4].

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

Table 1: The integers corresponding to the twenty-six letter alphabet [3].

3.2 Modular Arithmetic

One of the main mathematical concepts used in the Hill cipher is the topic of modular arithmetic. When given an integer $m > 1$, also known as the modulus, two integers a and b are congruent to each other modulo m if the difference $a - b$ is an integral multiple of m. This can be written as $a \equiv b \bmod m$. This means that for some integer k, a is congruent to b when $a = b + k \times m$ [4]. For example, $13 = 1 \bmod 4$, since $4 \times 3 = 12$, with 1 left over. In this case, $a = 13$, $b = 1$, $k = 3$, and $m = 4$. However, when there is no remainder, like for 12 mod 4, it ends up being equal to zero, since 4 divides evenly into 12. Furthermore, a set defined by $Z_m = \{0, 1, ..., m - 1\}$ in which addition and multiplication are closed is known as the "number system of the integers modulo m" [4]. There are several properties of this set, as detailed in Figure 4, that are useful when it comes to the Hill cipher. One property that is omitted from this figure states that "For each $a \in Z_m$ with $a \neq 0$, there is a unique $y \in Z_m$, called the multiplicative inverse or reciprocal of a, such that $a \times y = 1 = y \times a$." This is not true, since not every number has an inverse for each modulus m. For example, there is no number a, that when multiplied by 2 equals 1 mod 4. This is due to the fact that 2 divides evenly into 4, so 2 does not have a multiplicative inverse mod 4. However, if m is a prime number, then each integer in the set has a multiplicative inverse [4].

Proposition 1. *Let m be an integer with $m > 1$. Then in $\mathbb{Z}_m$:*

1. *For all $a, b, c \in \mathbb{Z}_m$, $(a + b) + c = a + (b + c)$.*
2. *For all $a, b \in \mathbb{Z}_m$, $a + b = b + a$.*
3. *For each $a \in \mathbb{Z}_m$, $a + 0 = a = 0 + a$.*
4. *For each $a \in \mathbb{Z}_m$, there is a unique $x \in \mathbb{Z}_m$, called the* additive inverse *of a, such that $a + x = 0 = x + a$.*
5. *For all $a, b, c \in \mathbb{Z}_m$, $(ab)c = a(bc)$.*
6. *For all $a, b \in \mathbb{Z}_m$, $ab = ba$.*
7. *For each $a \in \mathbb{Z}_m$, $1 \cdot a = a = a \cdot 1$.*
8. *(This property is intentionally omitted!)*
9. *For all $a, b, c \in \mathbb{Z}_m$, $a(b + c) = ab + ac$.*
10. *In $\mathbb{Z}_m$, $1 \neq 0$.*

Figure 4: Properties of Z_m [4]

3.3 Matrices

A matrix is an arrangement of numbers in rows and columns, where each number is a component of the matrix. In general, m represents the number of rows and n represents the number of columns, so that the matrix can be referred to as an $m \times n$ matrix. The structure of a matrix can be seen in Figure 5. In addition, vectors can also be written as column matrices with one column and m rows [7]. The classic Hill cipher uses vectors written as column matrices for the plaintext and ciphertext messages, and square matrices as the key matrices. A square matrix has n rows and n columns, and is referred to as an $n \times n$ square matrix. Three of the main properties of matrices that are used for the Hill cipher are matrix multiplication, the finding of the matrix's determinant, and the creation of an invertible matrix [3].

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

Figure 5: An $m \times n$ matrix [7]

3.3.1 Matrix Multiplication

To encrypt a message using the Hill cipher, the plaintext is converted into numbers which make up a column matrix, which is then multiplied by the key matrix. In order to multiply the two matrices, the number of columns in the key matrix must equal the number of rows in the column matrix. Thus, if the key matrix were a 2×2 matrix, then the column matrix must be a 2×1 matrix in order to be multiplied together. Since matrix multiplication is not commutative, it is important to note that the column matrix is to the left of the key matrix. To multiply the two matrices, as shown in Figure 6, each component in the column matrix is multiplied to the components in the first row of the key matrix and are added together to create the first entry of the new matrix. This step is repeated for each row of the key matrix. As a result, the product of these two matrices is a new 2×1 column matrix, which becomes the ciphertext in the encryption. An example of the multiplication of a 2×2 matrix by a 2×1 matrix is shown in Equation 1.

$$\mathbf{Ax} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{bmatrix}$$

Figure 6: Matrix-vector product [8]

$$Ax = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 6 \end{bmatrix} = \begin{bmatrix} (5 \cdot 1) + (6 \cdot 2) \\ (5 \cdot 3) + (6 \cdot 4) \end{bmatrix} = \begin{bmatrix} 17 \\ 39 \end{bmatrix} \tag{1}$$

3.3.2 Determinants

An important function used in linear algebra is finding the determinant of matrices. Finding the determinant is useful because it helps in finding the inverses of different matrices. Since the decryption of the Hill cipher relies on finding the inverse of the key matrix, the determinant is an essential part of the process. To find the determinant of a 2×2 matrix, as shown in Figure 7, the number on the top right, b, is multiplied by the number on the bottom left, c, and subtracted from the number on the top left, a, multiplied by the number on the bottom right, d [9].

$$\det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc.$$

Figure 7: Finding the determinant of a 2×2 matrix [9]

3.3.3 Invertible Key Matrices

In order to decrypt a message using the Hill cipher, the key matrix must be invertible. An invertible matrix, as described in Equation 2, is a matrix which produces the identity matrix, I, when multiplied by the original matrix.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \tag{2}$$

To find the inverse of a matrix, the multiplicative inverse of the determinant is multiplied by the matrix which is formed when the values along the main diagonal, a and d, are swapped, while the values along the other diagonal, b and c, become negative, as seen in Equation 3. When working with a modulus, it is essential that the determinant of the key matrix is relatively prime to the modulus m; otherwise, the key matrix is not invertible. In addition, the determinant cannot equal zero, since there is no number that can be multiplied by zero to get one. In other words, zero does not have a multiplicative inverse.

$$A^{-1} = [det(A)]^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \tag{3}$$

4 Application

4.1 Encryption

To encrypt a chosen plaintext message using the Hill cipher, the first thing that must be done is to choose the value of n for the n x n square invertible key matrix. To make

things simple, a 2 x 2 matrix will be used in explaining the encryption and decryption using the Hill cipher. Next, the plaintext letters are broken into pairs and converted into integers using Table 1. If the chosen plaintext message is not long enough to create a set of pairs, a random letter can be chosen and added on to the end of the message [3]. Then, the integer pairs formed by the plaintext message are converted into column matrices, which are then multiplied by the key matrix mod 26. The resulting column matrices are then changed back into a string of integers, which are then converted back into letters using Table 1. The result is the letters that make up the ciphertext [4]. This can be seen in Equation 4, where the first matrix represents the key matrix, P represents the integers converted from the plaintext, and C represents the ciphertext [3].

3	5	7	17	19	25
9	21	15	23	11	25

Table 2: The multiplicative inverses mod 26.

$$\begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} \bmod 26 \tag{4}$$

An important thing to note is that when creating the key matrix, it is essential for decryption that the matrix is invertible. Thus, a key matrix must be chosen in which the determinant is relatively prime to the modulus, which in this case is modulo 26. If the key matrix is not invertible, then the ciphertext cannot be decrypted [3].

4.2 Decryption

To decrypt a ciphertext message using the Hill cipher, the reverse of the encryption process is done. The first step is to divide the letters up into pairs and convert them into the corresponding integers, as shown in Table 1. Next, the pairs of integers are converted into column vectors, which are then multiplied by the inverse of the key matrix [4]. To find the inverse of the key matrix, as shown in Equation 5, the multiplicative inverse of the determinant of the key matrix is multiplied by the matrix which is formed when the values along the main diagonal are swapped, while the values along the other diagonal become negative. Table 2 can be used to find the multiplicative inverse of the determinant mod 26. The integers in the resulting matrix are then reduced mod 26. If the determinant of the key matrix is not relatively prime to mod 26, then it does not have a multiplicative inverse mod 26. This means that the ciphertext cannot be decrypted because without the multiplicative inverse of the determinant of the key matrix mod 26, the inverse of the key matrix cannot be found, and therefore cannot be used to decrypt the ciphertext message [3].

$$A^{-1} = \begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix}^{-1} = [det(A)]^{-1} \begin{bmatrix} K_4 & -K_2 \\ -K_3 & K_1 \end{bmatrix} \bmod 26 \tag{5}$$

After finding the inverse of the key matrix, it is then multiplied by the column matrices composed of the integers that correspond to the ciphertext, as shown in Equation 6. The resulting column matrices are then broken up into a string of integers, which can be converted

back into letters using Table 1 [4]. After converting the integers back into the letters, the result is the original plaintext message.

$$\begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix} \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \bmod 26 \tag{6}$$

4.3 Example

4.3.1 Encryption

For this example, the message that is going to be encrypted is "HI". The letters H and I correspond to the numbers 7 and 8, respectively, as seen in Table 1 earlier. Thus, they form a the column matrix that is $\begin{bmatrix} 7 \\ 8 \end{bmatrix}$. The next step is to find an invertible key matrix. In order for the matrix to be invertible, the determinant of the matrix must have a multiplicative inverse mod 26. In this example, A is the invertible key matrix, as seen in Equation 7.

$$A = \begin{bmatrix} 9 & 4 \\ 6 & 5 \end{bmatrix} \tag{7}$$

The next step of the encryption process is to multiply the column matrix by the key matrix and then reduce the result mod 26, as shown in equation 8.

$$\begin{bmatrix} 9 & 4 \\ 6 & 5 \end{bmatrix} \cdot \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} (9 \cdot 7) + (4 \cdot 8) \\ (6 \cdot 7) + (5 \cdot 8) \end{bmatrix} = \begin{bmatrix} 95 \\ 82 \end{bmatrix} = \begin{bmatrix} 17 \\ 4 \end{bmatrix} (mod 26) \tag{8}$$

The resulting column matrix, $\begin{bmatrix} 17 \\ 4 \end{bmatrix}$, consists of the numbers that make up the ciphertext message. These numbers are then translated back into letters using Table 1. So, in this case, the ciphertext message is "RE".

4.3.2 Decryption

Now that we have the ciphertext message, "RE", we can decrypt it in order to get the plaintext back. The first step for decryption would be to find the inverse of the key matrix A, as seen in Equation 9. To do so, the multiplicative inverse of the determinant is multiplied by the matrix which is formed when the values along the main diagonal, 9 and 5, are swapped, while the values along the other diagonal, 4 and 6, become negative. The inverse of the determinant can be found in Table 2, which states every multiplicative inverse in mod 26.

$$A^{-1} = \begin{bmatrix} 9 & 4 \\ 6 & 5 \end{bmatrix}^{-1} = \frac{1}{(9 \cdot 5) - (4 \cdot 6)} \cdot \begin{bmatrix} 5 & -4 \\ -6 & 9 \end{bmatrix} = \frac{1}{21} \cdot \begin{bmatrix} 5 & -4 \\ -6 & 9 \end{bmatrix} = \tag{9}$$

$$= 5 \cdot \begin{bmatrix} 5 & -4 \\ -6 & 9 \end{bmatrix} (mod 26) = \begin{bmatrix} 25 & -20 \\ -30 & 45 \end{bmatrix} = \begin{bmatrix} 25 & 6 \\ 22 & 19 \end{bmatrix} (mod 26)$$

The next step is to multiply this inverse matrix by the column matrix containing the ciphertext message and then reduce the result mod 26, as seen in Equation 10.

$$\begin{bmatrix} 25 & 6 \\ 22 & 19 \end{bmatrix} \cdot \begin{bmatrix} 17 \\ 4 \end{bmatrix} = \begin{bmatrix} (25 \cdot 17) + (6 \cdot 4) \\ (22 \cdot 17) + (19 \cdot 4) \end{bmatrix} = \begin{bmatrix} 449 \\ 450 \end{bmatrix} = \begin{bmatrix} 7 \\ 8 \end{bmatrix} (mod 26) \tag{10}$$

The final step of the decryption process is to translate the numbers from the column matrix, 7 and 8, back into letters using Table 1. The letters that are returned are H and I, thus we get back our original plaintext message of "Hi".

5 Conclusion

Overall, the creation of Lester Hill's Hill cipher is introduced, along with its main encryption and decryption methods. With the advancement of the cryptological field comes more secure algorithms, while the older ciphers become more susceptible to various attacks. Thus, the Hill cipher is explained to have several weaknesses, which include its vulnerability to the known plaintext attack, as well as the issue of having to generate an invertible key matrix, otherwise the ciphertext cannot be decrypted. Because the Hill cipher suffers from these weaknesses, mathematicians have proposed modifications to the original algorithm in order to enhance the security of the cipher. Three specific modifications are compared, as well as the results. Altogether, the three approaches share mainly the same results, which are stronger resistance to the known plaintext attack, as well as the removal or replacement of the invertible key matrix to prevent the possibility of failed encryption due to a non-invertible key matrix being generated. Future works may include studies of how well these modified algorithms work. In addition, further modifications can be done on the classic Hill cipher with the ever-growing algorithms in the field of cryptology.

References

1. Jain, S. & Arya, M. K. A Neoteric Strategy of Hill Cipher for Analysis of Degenerate Matrices Key. *Journal of Algebraic Statistics* **13,** 194–198 (2022).
2. Poritz, J. A. Some Speculative History. `https://math.libretexts.org/@go/page/77011` (2021).
3. Mokhtari, M. & Naraghi, H. Analysis and design of affine and hill cipher. *Journal of Mathematics Research* **4,** 67 (2012).
4. Eisenberg, M. Hill ciphers and modular linear algebra. *Mimeographed notes* **165,** 1–19 (1999).
5. Hasoun, R. K., Khlebus, S. F. & Tayyeh, H. K. A new approach of classical Hill Cipher in public key cryptography. *International Journal of Nonlinear Analysis and Applications* **12,** 1071–1082 (2021).
6. Acharya, B., Panigrahy, S. K., Patra, S. & Panda, G. Image Encryption Using Advanced Hill Cipher Algorithm. *International Journal of Recent Trends in Engineering* **1** (Apr. 2009).
7. Nykamp, D. Q. Introduction to matrices. `https://mathinsight.org/matrix_introduction`.

8. Nykamp, D. Q. Multiplying matrices and vectors. https://mathinsight.org/matrix_vector_multiplication.
9. The determinant of a matrix. http://mathinsight.org/determinant_matrix.