Expository Paper: The Hill Cipher

Until the early 20\textsuperscript{th} century, cryptography was still largely grounded in linguistics. Most ciphers were still vulnerable to some form of frequency analysis or plaintext attack, and the true potency of merging abstract mathematics with cryptography was not yet fully realized. In 1929, an assistant professor of mathematics by the name of Lester Hill published a paper concerning the synthesis of linear algebra and cryptography. He essentially proposed a polygraphic encryption method, an encryption technique in which blocks of plaintext letters are substituted, that would completely nullify any decryption attempts using frequency analysis (Kahn).

While the Hill Cipher, as his cryptographic method became known, was not the first polygraphic substitution cipher to be proposed, it was arguably the first time that multiple letter substitution became theoretically practical for daily use. Large quantities of cipher text could now be encrypted and decrypted using matrices, but this efficiency came with a price. The mathematical relationships involved in matrix multiplication permit the cryptanalyst to exploit these patterns given either the exact location of known plaintext within the cipher text or identical plaintexts encrypted with different keys. Furthermore, the nature of the cipher required laborious calculations for those using it to encipher and decipher text. Hill tried to simplify such calculations by introducing a machine capable of automatically performing
encryptions, but the device suffered from a relatively low fixed amount of keys and became too complicated for daily use as the key grew larger. As such, the cipher was not widely used by the military or government and was only employed to encrypt broadcasting stations’ identities, which were three-letter character codes (Kahn).

Whereas the Vigenère cipher and older monoalphabetic substitution ciphers were enciphered geometrically, the Hill cipher was grounded in linear algebra. In order to understand the inner-workings of the cipher, one must first grasp the fundamentals of modular arithmetic (a subset of linear algebra) and matrix multiplication. At its most basic level, modular arithmetic deals with remainders. In the equation \( a = b \pmod{m} \), \( m \) is called the modulus, and it is verbalized as “\( a \) and \( b \) are congruent modulo \( m \)” if the difference \( b - a \) is evenly divisible by \( m \) (Barr). For example, 11 and 43 are congruent modulo 26, as the difference 43 - 11 goes into 26 one time (an even number of times). An alternate definition gives another relationship between the components in the previous equation, and will be useful in the Hill cipher’s decryption. The equation \( b \mod{m} \) is equal to the remainder when \( b \) is divided by \( m \), and is also equal to the smallest nonnegative number \( a \) such that \( b = a \pmod{m} \) (Barr). For example, \(-54 \mod{26} \) is equal to 24, as \(-28\) is the remainder when \(-54\) is divided by 24, but 24 is the smallest nonnegative number such that the equation \(-54 = 24 \pmod{26}\).

Another way of thinking about this is displayed in the figure below (Figure 1).

![Figure 1](image-url)
While -28 is the remainder when 24 goes into -54, the number 26 must be added twice more to the initial value before the final value is nonnegative.

Matrix multiplication is the next element that is critical in encrypting and decrypting cipher text encoded with the Hill cipher. Simply defined, a matrix is an array (an arrangement) of numbers contained within a rectangular cell. Two matrices are only able to be multiplied by one another if the number of columns of the first matrix is the same as the number of rows in the second one, or vice versa (Barr). The following two examples demonstrate the multiplication of a 2 x 2 matrix with a 2 x 1 matrix, and the multiplication of two 2 x 2 matrices:

**Example 1:**
\[
\begin{bmatrix}
a & b \\
c & d \\
\end{bmatrix}
\begin{bmatrix}
e \\
f \\
\end{bmatrix}
= \begin{bmatrix}
ae + bf \\
ce + df \\
\end{bmatrix}
\]

**Example 2:**
\[
\begin{bmatrix}
a & b \\
c & d \\
\end{bmatrix}
\begin{bmatrix}
e & f \\
g & h \\
\end{bmatrix}
= \begin{bmatrix}
ae + bg & af + bh \\
ce + dg & cf + dh \\
\end{bmatrix}
\]

An important observation (and one that allows the Hill cipher to function) is the fact that the manner in which two matrices are multiplied determine the product. The product of the same two matrices in example 2, but now reversed, is the following:

\[
\begin{bmatrix}
e & f \\
g & h \\
\end{bmatrix}
\begin{bmatrix}
a & b \\
c & d \\
\end{bmatrix}
\neq \begin{bmatrix}
ae + bg & af + bh \\
ce + dg & cf + dh \\
\end{bmatrix}
\]

The product of the two reversed matrices is not equal to the product obtained in example 2. However, there are exceptional cases in which two matrices yield the same product regardless of the order in which they are multiplied. This idea gives rise to two more important concepts: the determinant and the inverse.
A cipher only works if both the intended recipient and the individual doing the encrypting possess the enciphering key. As the encryption in this particular cipher is performed using mathematical operations (specifically matrix multiplication and modular arithmetic), some inverse operations must be applied to reverse the encryption and recover the plaintext. A problem arises here, however, as not all matrices have an inverse. Therefore, it must be concluded that a given matrix is invertible (i.e. has an inverse) to make it eligible as a key to the Hill cipher. A matrix's determinant determines whether or not the matrix in question possesses an inverse. Given the matrix \[
\begin{bmatrix}
a & b \\
c & d
\end{bmatrix}
\], the determinant, \(\text{det}(A)\), equals \(ad - bc\). Furthermore, “the determinant of \(A\) modulo \(m\) is \(\text{det}(A)\) reduced modulo \(m\)” (Barr). \(\text{det}(A)\) reduced modulo \(m\) simply refers to the remainder when the value of \(\text{det}(A)\) is fully divided into \(m\). For example, given the matrix \[
\begin{bmatrix}
7 & 1 \\
20 & 4
\end{bmatrix}
\], \(\text{det}(A) = (7 \times 4) - (20 \times 1) = 8\), therefore \(\text{det}(A) = 8 \pmod{26}\), as \(8 - 8 = 0\), which is evenly divisible by 26. We can also check the answer by noting that \(8 \pmod{26} = 8\).

If \(\text{det}(A)\) is relatively prime to \(m\) (i.e. there are no other common factors other than 1), then the matrix \(A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\) is invertible modulo \(m\) (Barr). If this is the case, then the inverse of matrix \(A\) is the following:

\[
A^{-1} = \frac{1}{\text{det}(A)} \begin{bmatrix}
d & -b \\
-c & a
\end{bmatrix} \pmod{m}
\]

Now that all of the elements involved in the encryption and decryption of the Hill cipher have been covered, we can examine the inner-workings of the cipher itself. To encrypt plaintext using the Hill cipher, we must have two matrices – one containing the key, and one containing the plaintext. For a key matrix size of 2 x 2 and a plaintext matrix size of 2 x 1, the
equation \[
\begin{bmatrix}
y_1 \\
y_2
\end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_1 \\
x_2
\end{bmatrix} \pmod{26}
\] encrypts the plaintext (Barr). The matrix \[ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \] is the key, the matrix \[ \begin{bmatrix} x_1 \\
x_2
\end{bmatrix} \] is the plaintext, and the matrix \[ \begin{bmatrix} y_1 \\
y_2
\end{bmatrix} \] is the resulting cipher text. For example, to encrypt the letters O and K, we must first assign arbitrary numerical values for each of these letters. In this example, O will be represented by 12 and K represented by 21. The specific numbers representing each letter in the alphabet don’t matter as long as each letter is represented by a unique number (i.e. a numerical value doesn’t represent multiple letters in the alphabet) and the numbers range from 0 to 26. To encrypt the two letters at once, the following equation is set up:

\[
\begin{bmatrix}
y_1 \\
y_2
\end{bmatrix} = \begin{bmatrix} 3 & 7 \\ 9 & 10 \end{bmatrix} \begin{bmatrix} 12 \\
21
\end{bmatrix} \pmod{26}
\]

To calculate \( y_1 \) and \( y_2 \), we recall that 2 x 2 and 2 x 1 matrices are multiplied in the following manner: \[ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e \\
f
\end{bmatrix} = \begin{bmatrix} ae + bf \\
ce + df
\end{bmatrix} \]. The equation can be simplified to:

\[
\begin{bmatrix}
y_1 \\
y_2
\end{bmatrix} = \begin{bmatrix} 183 \\
318
\end{bmatrix} \pmod{26}
\]

To calculate \( y_1 \) we can evaluate the expression \( y_1 = 183 \pmod{26} \). 26 goes into 183 a total of 7 times with a remainder of 1, therefore \( y_1 = 1 \). To determine \( y_2 \) we evaluate the expression \( y_2 = 318 \pmod{26} \) and get \( y_2 = 6 \). If we had constructed the rest of the cipher alphabet, these two numbers, 1 and 6, would represent letters. If we had enciphered a larger plaintext message, we would likely notice that the Hill cipher does an excellent job of obfuscating repeated letters and that a cipher text letter can actually represent multiple plaintext characters (Barr).
To decrypt cipher text constructed using the Hill cipher with key \[
\begin{bmatrix}
    a & b \\
    c & d \\
\end{bmatrix}
\] the equation
\[
\begin{bmatrix}
    x_1 \\
    x_2 \\
\end{bmatrix} = \begin{bmatrix}
    a & b \\
    c & d \\
\end{bmatrix}^{-1} \begin{bmatrix}
    y_1 \\
    y_2 \\
\end{bmatrix} \mod 26
\] is employed (Barr). We recall that if the inverse of the matrix key exists, that is, if the determinant of \[
\begin{bmatrix}
    a & b \\
    c & d \\
\end{bmatrix}
\] is relatively prime to 26, the inverse of \[
\begin{bmatrix}
    a & b \\
    c & d \\
\end{bmatrix}
\] is equal to \[
\det(A)^{-1} \begin{bmatrix}
    d & -b \\
    -c & a \\
\end{bmatrix} \mod m
\]. To evaluate this expression, the modular multiplicative inverse must be used. This property states that \(a^{-1} = x \mod m\), which is equivalent to the expression \(ax = aa^{-1} = 1 \mod m\) (Wikipedia). To decrypt the plaintext encrypted in the earlier example, we must first calculate the inverse of the key matrix \[
\begin{bmatrix}
    3 & 7 \\
    9 & 10 \\
\end{bmatrix}
\]. The determinant is equal to \((3 \times 10) - (9 \times 7) = -33\), so the determinant A reduced modulo 26 is equal to \(-33 \mod 26\), or 19. The inverse of 19 can be found by solving the expression \(19x = 1 \mod 26\), which can be rewritten as \(19x \mod 26 = 1\). The smallest value of \(x\) that solves this congruence expression is 11, as the product of 19 and 11 divided by 26 yields a remainder of 1.

Substituting this value into \(\det(A)^{-1} \begin{bmatrix}
    d & -b \\
    -c & a \\
\end{bmatrix} \mod m\) gives the following:
\[
\begin{bmatrix}
    a & b \\
    c & d \\
\end{bmatrix}^{-1} = 11 \begin{bmatrix}
    10 & -7 \\
    -9 & 3 \\
\end{bmatrix} \mod 26 = 11 \begin{bmatrix}
    10 & 19 \\
    17 & 3 \\
\end{bmatrix} = \begin{bmatrix}
    110 & 209 \\
    187 & 33 \\
\end{bmatrix} = \begin{bmatrix}
    6 & 1 \\
    5 & 7 \\
\end{bmatrix} \mod 26
\]

Now that we have found the inverse of the matrix used to encipher, we have all the components necessary in deciphering the cipher text. Plugging the necessary parts into the equation used to decipher, we get:
\[
\begin{bmatrix}
    x_1 \\
    x_2 \\
\end{bmatrix} = \begin{bmatrix}
    3 & 7 \\
    9 & 10 \\
\end{bmatrix}^{-1} \begin{bmatrix}
    1 \\
    6 \\
\end{bmatrix} \mod 26 = \begin{bmatrix}
    6 & 1 \\
    5 & 7 \\
\end{bmatrix} \begin{bmatrix}
    1 \\
    6 \\
\end{bmatrix} \mod 26 = \begin{bmatrix}
    6 + 6 \\
    5 + 42 \\
\end{bmatrix} \mod 26
\]

\(x_1 = 12 \mod 26 = 12\)

\(x_2 = 47 \mod 26 = 21\)
If we recall that O and K were represented by 12 and 21 respectively, we can see that the decryption was successful in retrieving the initial plaintext.

While the Hill cipher is not susceptible to decryption attacks using frequency analysis, it can still be broken using either a brute force or known-plaintext attack. There are $26^n$ different matrices that have to be tried when attempting to brute force a Hill cipher, where $n$ is equal to the number of rows in the matrix multiplied by the number of columns (Barr). If the cryptanalyst knows the exact location of some known plaintext within the cipher text, however, he or she can exploit that fact by seeing whether the cipher text modulo 26 is relatively prime to 26. If the value is co-prime, the matrix containing the known cipher text is invertible, and the cryptanalyst can multiply both sides of the congruency expression relating the known plaintext to the cipher text by this inverse matrix to potentially yield the matrix used to encipher (Barr). Once the matrix used to encipher the plaintext is known, the matrix used to decipher – the inverse – can also be found using techniques discussed earlier.

The Hill Cipher was not ground-breaking for its time and played a relatively miniscule role in military and governmental affairs. However, the cipher served as an important stepping stone between the so-called “pencil and paper” ciphers of the 17th, 18th, and 19th centuries and today’s methods based on abstract mathematics (Kahn). While the Hill Cipher is regarded as being insecure today, some of its core principles are still in use. AES and Twofish, two ciphers currently in use, employ matrix multiplication as a method of diffusing encrypted information and making their algorithms more secure (Lyons).
Works Cited


