# Hill Cipher Algorithm

Nolan Winsman, Taylor Carney, Mark Mueller

November 2021

## 1 Encryption

### 1.1 Formula

The general formula for Encrypting text using the Hill Cipher Algorithm is $\boldsymbol{K} \times \boldsymbol{P} \mod \mathbf{26}$. Where **K** is our $n \times n$ Matrix that serves as the Key. The determinant of **K** must be relatively prime with **26**. **P** is our text we want to encrypt in the form of an $n \times 1$ Matrix.

### 1.2 Modulus

For this example, we are modding the matrix by 26 since we will be using the 26 letters of the alphabet. Technically you mod the matrix by the length of potential values. For instance if you were using ASCII characters, it would be $\boldsymbol{K} \times \boldsymbol{P} \mod \mathbf{256}$ for the 256 possible ASCII characters.

### 1.3 Example Key and Text

For this example we will be using a $2 \times 2$ Matrix for our key, therefore our text matrices will be several $2 \times 1$ matrices.

$\mathbf{K} = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

**P** = ”LinearMath”

### 1.4 Validating K

As mentioned above, the determinant of **K** must be relatively prime with **26**. This is easy to check. We calculate the determinant of **K** which is 9 in our example above. Then we calculate the greatest common divisor between 9 and 26 or GCD(9, 26). If GCD(9, 26) is equal to 1 then **K** is a valid Key. If GCD(9,26) is not equal to 1, then **K** is an invalid Key and we cannot use it.

### 1.5 Convert P to Matrices

"LinearMath" converts to matrices → $\begin{bmatrix} L \\ I \end{bmatrix} \begin{bmatrix} N \\ E \end{bmatrix} \begin{bmatrix} A \\ R \end{bmatrix} \begin{bmatrix} M \\ A \end{bmatrix} \begin{bmatrix} T \\ H \end{bmatrix}$

Now that we have our text in several 2 × 1 matrices, we want to convert the characters to numbers corresponding to their letter in the alphabet, so 'A' will be 1 and 'Z' will be 26

"LinearMath" converts to matrices → $\begin{bmatrix} 12 \\ 9 \end{bmatrix} \begin{bmatrix} 14 \\ 5 \end{bmatrix} \begin{bmatrix} 1 \\ 18 \end{bmatrix} \begin{bmatrix} 13 \\ 1 \end{bmatrix} \begin{bmatrix} 20 \\ 8 \end{bmatrix}$

### 1.6 Encrypting the Text

The process to encrpyt our text now is quite simple. Simply multiply each $2 \times 1$ matrix, or vector of dimension 2, to our $2 \times 2$ key matrix.

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 12 \\ 9 \end{bmatrix} \mod 26 = \begin{bmatrix} 63 \\ 69 \end{bmatrix} \mod 26 = \begin{bmatrix} 11 \\ 17 \end{bmatrix}$$

Continue this process until all of your vectors are converted

"LinearMath" encrypts to matrices → $\begin{bmatrix} 11 \\ 17 \end{bmatrix} \begin{bmatrix} 5 \\ 1 \end{bmatrix} \begin{bmatrix} 5 \\ 14 \end{bmatrix} \begin{bmatrix} 16 \\ 5 \end{bmatrix} \begin{bmatrix} 6 \\ 2 \end{bmatrix}$

If we convert these numbers back to characters we get

"LinearMath" encrypts to matrices → $\begin{bmatrix} K \\ Q \end{bmatrix} \begin{bmatrix} E \\ A \end{bmatrix} \begin{bmatrix} E \\ N \end{bmatrix} \begin{bmatrix} P \\ E \end{bmatrix} \begin{bmatrix} F \\ B \end{bmatrix}$

Encrypted Text = "KQEAENPEFB"

## 2 Decryption

### 2.1 Formula

The formula for decrypting text is $\boldsymbol{K^{-1}} \times \boldsymbol{P} \mod \mathbf{26}$. Where $\boldsymbol{K^{-1}}$ is our $n \times n$ Matrix that is the inverse of our key, **K**. The letter **P** is our text we want to decrypt in the form of, typically multiple, $n \times 1$ matrices.

### 2.2 Calculating $\boldsymbol{K^{-1}}$

Decrypting text using the Hill Cipher Algorithm is almost identical to encrypting the text. The only difference is we use the multiplicative inverse of **K** as the key. Remember we can only do this if the determinant of **K** and **26** are coprimes. The first part of this process is evidently calculating the multiplicative inverse of **K**. To do this we first calculate the inverse of **K**. The inverse of a 2 × 2 matrix is quite easy so we get.

$$\boldsymbol{K^{-1}} = \frac{1}{9}\begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \rightarrow \begin{bmatrix} 5/9 & -3/9 \\ -2/9 & 3/9 \end{bmatrix}$$

This will potentially leave us with decimals which can mess up our decryption, so we calculate the inverse of each value in the $2 \times 2$ matrix. To fix this, we calculate the multiplicative inverse of our scalar. $\frac{1}{9}^{-1} \mod 26$ To solve the multiplicative inverse in this example it is →

$9 \times x \equiv 1 \mod 26$ Where the inverse of $\frac{1}{9}$ is 9

In this formula our **x** is equal to **3** since $9 \times 3 \equiv 1 \mod 26$

With this we can rewrite our key as

$$\boldsymbol{K^{-1}} = 3\begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$$

This formula is almost complete, but we cannot have negative numbers inside the matrix so we $\mod$ all the values inside the matrix by 26

$$\boldsymbol{K^{-1}} = 3\begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix} \rightarrow \begin{bmatrix} 15 & 69 \\ 72 & 9 \end{bmatrix}$$

Lastly, we have to mod the entire matrix by 26 again to deal with the values larger than 26.

$$\boldsymbol{K^{-1}} = \begin{bmatrix} 15 & 69 \\ 72 & 9 \end{bmatrix} \mod 26 \rightarrow \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

### 2.3 Decrpytion Key and Text

$$\boldsymbol{K^{-1}} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

**P** = ”KQEAENPEFB”

### 2.4 Convert P to Matrices

With the text we previously encrypted ”KQEAENPEFB” we convert it into several 2 × 1 matrices

$$\text{"KQEAENPEFB" converts to matrices} \rightarrow \begin{bmatrix} K \\ Q \end{bmatrix} \begin{bmatrix} E \\ A \end{bmatrix} \begin{bmatrix} E \\ N \end{bmatrix} \begin{bmatrix} P \\ E \end{bmatrix} \begin{bmatrix} F \\ B \end{bmatrix}$$

Then we convert all the letters into numbers just like the encryption.

$$\text{"KQEAENPEFB" encrypts to matrices} \rightarrow \begin{bmatrix} 11 \\ 17 \end{bmatrix} \begin{bmatrix} 5 \\ 1 \end{bmatrix} \begin{bmatrix} 5 \\ 14 \end{bmatrix} \begin{bmatrix} 16 \\ 5 \end{bmatrix} \begin{bmatrix} 6 \\ 2 \end{bmatrix}$$

### 2.5 Decypting the Text

The process to encrpyt our text now is quite simple. Simply multiply each 2 × 1 matrix, or vector of dimension 2, to our 2 × 2 key matrix.

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 11 \\ 17 \end{bmatrix} \mod 26 = \begin{bmatrix} 454 \\ 373 \end{bmatrix} \mod 26 = \begin{bmatrix} 12 \\ 9 \end{bmatrix}$$

Continue this process until all of your vectors are converted

$$\text{"KQEAENPEFB" decrypts to} \rightarrow \begin{bmatrix} 12 \\ 9 \end{bmatrix} \begin{bmatrix} 14 \\ 5 \end{bmatrix} \begin{bmatrix} 1 \\ 18 \end{bmatrix} \begin{bmatrix} 13 \\ 1 \end{bmatrix} \begin{bmatrix} 20 \\ 8 \end{bmatrix}$$

If we convert these numbers back to characters we get

$$\text{"KQEAENPEFB" decrypts to} \rightarrow \begin{bmatrix} L \\ I \end{bmatrix} \begin{bmatrix} N \\ E \end{bmatrix} \begin{bmatrix} A \\ R \end{bmatrix} \begin{bmatrix} M \\ A \end{bmatrix} \begin{bmatrix} T \\ H \end{bmatrix}$$

Encrypted Text = ”KQEAENPEFB” Decrypts to ”LINEARMATH”

## 3 Honor Code

We have acted with honesty and integrity in producing this work and are unaware of anyone who has not