Quentin Edfrennes
Kiersten Thorsen
Eric Roddom
Linear Algebra Project

Linear Algebra and Cracking the Code: An Introductory Report on Hill Ciphers

Hill Ciphers are considered archaic and among the most basic ways of coding messages, however they hold their place at the beginning of cryptography as one of the most heavily used and most unique. Relying heavily on linear algebra, Hill Cipher depend on a key matrix and involve basic and fundamental principles in order to encrypt messages. In cryptography, a cipher is an algorithm for performing encryption or decryption. While mostly used for encoding messages, they can also be recognized as converting information and programming data into a code, or cipher.

A cipher starts out originally as plaintext, which is written and then is converted into a ciphertext. An example of this can be the code itself written in ciphertext. When the ciphertext is received, it is unreadable without the proper key or cryptovariable. The information received is identical to the information sent, but will be seen as a random message to anyone without the key. Ciphers have been around for thousands of years, but Lester S. Hill invented this particular cipher itself in 1929. As one of many different types of ciphers, the hill cipher is based on linear algebra and has specific qualities, including the fact that it can operate more than three different symbols at once.

The operation of the cipher starts out with every letter being assigned as a number. One common assignment can be seen below:

A	B	C	D	E	F	G		I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
1	2	3	4	5	6	7		9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

For example, if someone types in HELPME as a password, the ciphertext will be seen as:

The key cipher we will use for our report is an invertible matrix, we'll now call matrix K and will be our cryptovariable used through converting our text

$$\begin{matrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{matrix}$$

The Process

Say the message "GUSTAFSON" were to be translated into a code word. GUSTAFSON would be first transferred into matrix form within a 3x3 matrix:

$$\begin{bmatrix} \mathrm{G} & \mathrm{U} & S \\ T & A & F \\ S & \mathrm{O} & N \end{bmatrix}$$

Translating it into numbers, again we use the key:

A	B	C	D	E	F	G	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
1	2	3	4	5	6	7	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

To turn the matrix into:

$$\begin{bmatrix} 7 & 21 & 19 \\ 20 & 1 & 6 \\ 19 & 15 & 14 \end{bmatrix}$$

which we'll call matrix A. Then using the invertible matrix K as our key matrix, the

matrix K is multiplied by A:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \cdot \begin{bmatrix} 7 & 21 & 19 \\ 20 & 1 & 6 \\ 19 & 15 & 14 \end{bmatrix}$$

And the resulting matrix is:

$$\begin{bmatrix} 541 & 165 & 272 \\ 601 & 439 & 483 \\ 765 & 662 & 692 \end{bmatrix}$$

At this point the resulting matrix is divided by 26, the number of the characters set, and the remainder matrix:

$$\begin{bmatrix} 21 & 9 & 12 \\ 3 & 23 & 15 \\ 11 & 12 & 16 \end{bmatrix} \text{mod } 26$$

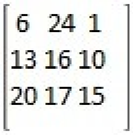
translates into the codeword:

$$\begin{bmatrix} \mathrm{U} & I & L \\ \mathrm{C} & \mathrm{W} & \mathrm{O} \\ K & L & P \end{bmatrix}$$

Therefore GUSTAFSON is translated into UILCWOKLP. If you know the matrix K you can translate this code back into GUSTAFSON.

Reversing the Process

Now, let’s say we’re given the code “UILCWOKLP” and we want to reverse the process in order to “break the code”. The important thing to remember is our key matrix.



$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

In order to begin solving the codeword we need to inverse our key matrix. Then once inverted we solve it for modulo 26. Our key matrix inverted and then plugging in the remainders once inverted is

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \bmod 26$$

Now we take our code and stick into a 3x3 matrix like we did before:

$$\begin{bmatrix} U & I & L \\ C & W & O \\ K & L & P \end{bmatrix} = \begin{bmatrix} 21 & 9 & 12 \\ 3 & 23 & 15 \\ 11 & 12 & 16 \end{bmatrix}$$

And we multiply it by our new inverted key matrix K^{-1}:

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 21 & 9 & 12 \\ 3 & 23 & 15 \\ 11 & 12 & 16 \end{bmatrix}$$

Which gives us the new matrix:

$$\begin{bmatrix} 293 & 307 & 331 \\ 696 & 625 & 708 \\ 565 & 561 & 560 \end{bmatrix}$$

When we cycle around 26 times and stick in the remainders again our final matrix looks like this:

$$\left. \begin{matrix} 293 & 307 & 331 \\ 696 & 625 & 708 \\ 565 & 561 & 560 \end{matrix} \right] \bmod 26 = \begin{bmatrix} 7 & 21 & 19 \\ 20 & 1 & 6 \\ 19 & 15 & 14 \end{bmatrix}$$

Which when we translate back into its letter form gives us:

$$\begin{bmatrix} 7 & 21 & 19 \\ 20 & 1 & 6 \\ 19 & 15 & 14 \end{bmatrix} = \begin{bmatrix} G & U & S \\ T & A & F \\ S & O & N \end{bmatrix}$$

In conclusion, Hill Ciphers have had a profound effect in the areas of Cryptography and Cryptanalysis and its foundation revolves around the elementary ideas found within Linear Algebra.