MESSAGE ENCRYPTION USING HILL CYPHER ALGORITHM

Abstract

Cryptography is defined as “the enciphering and deciphering of messages in a secret code or cipher” [2]. There are many forms of this applied daily that uses simple to chaotic mathematic algorithms to secure transmitted information. The purpose of this paper is to illustrate a simple cypher using the application of linear algebra to encrypt and decrypt a message. The main algorithm applied is a version of Hill Cypher invented in 1929 by Lester S. Hill at Hunter College, New York [3]. The Hill Cypher involves the use of two matrices one used as a key to encode and an inversed version of the key to decode. This paper will further illustrate two applications of the Hill Cypher to encode and decode a message from the English alphabet using a 4 x 4 and 3 x 3 matrix. The method requires the matrices to be invertible, the characters of the alphabet assigned a numerical value, and a knowledge of modular arithmetic. Although the paper illustrates a surprisingly good encoding technique to send secret messages, the cypher is vulnerable to a “Known Plain-Text Attack” [4].

Keywords: Matrix, Inverse Matrix, Decrypt, Encrypt, Message, Modular Arithmetic.

John Wilson

jwils082@odu.edu

Computer Science Undergraduate

Dr. H. Kaneko MATH 316

I. INTRODUCTION

The practice of using confidential communications has been performed since humans have had a requirement to keep information confidential. Evidence of this can be witnessed as early as the ancient Greeks with their use of the Scytale; a strip of parchment with letters wrapped around a specific sized cylinder to show the message [5]. There are some that speculate to earlier civilizations than the ancient Greeks used a primitive form of secret writing for communication. Although, there is no definitive evidence to the actual origins of cryptography, the academic research of this technology began around the Renaissance Era, period between the 14th and 17th Century [9]. During this period, there is ample evidence of using methods like wax seals or rearranging of letters with a shared code key between the sender and recipient to keep messages confidential. Throughout the world, the dependence on cryptography to securely send and receive messages in today's electronics society is being seen more than it has been relied upon the past. When you look around society cryptography algorithms are used to protect both person and important business information of groups like: financial institutions, government's, communications, research and development, military movements and plans, health industry, there is even an algorithm that helps encrypt your home Wi-Fi. Linear Algebra's application in cryptography is used to conceal the contents of a message to keep them disclosed in privacy.

II. Matrix Multiplication

Matrix Multiplication is a system that produces a single matrix from two matrices through multiplication and the dot product. Matrix multiplication is the products of matrix A and matrix B where matrix AB = matrix C [8].

A. Properties of Matrix Multiplication [8]

Let A, B be $m\ x\ n$ matrices, C, D be $n\ x\ p$ matrices, and E be a $p\ x\ q$ matrix, and let r be a real number

1) If A is nonsingular, then so is A^{-1} and $(A^{-1})^{-1} = A$
2) $(AC)E = A(CE)$
3) $A(C + D) = AC + AD$
4) $(A + B)C = AC + BC$
5) $r(AC) = (rA)C = A(rC)$
6) $(AC)^T = C^T A^T$
7) $AI_n = I_m A = A$

III. Inverse Matrix [10]

An inverse matrix is defined as a square $n\ x\ n$ matrix A is called invertible, if there exists an $n\ x\ n$ square B matrix such the multiplication of both equals in a single identity matrix I; $i.e. AB = BA = I_n$. The result of I_n is the inverse of matrix A and is called the inverse noted as A^{-1}.

A. A formula to Find the Inverse of a Matrix

Let A be a matrix and I_2 be an identity matrix: $A * I_2 = A^{-1}$

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} and\ I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = AI_2 = \begin{bmatrix} 1 & 2 & 1 & 0 \\ 2 & 3 & 0 & 1 \end{bmatrix} \rightarrow$$

$$Perform\ r.r.e.f \rightarrow \begin{bmatrix} 1 & 0 & -3 & 2 \\ 0 & 1 & 2 & -1 \end{bmatrix} \rightarrow$$

$$Inverse\ of\ A = A^{-1} = \begin{bmatrix} -3 & 2 \\ 2 & -1 \end{bmatrix}$$

B. Properties of the Inverse Matrix [10]

1) If A is nonsingular, then so is A^{-1} and $(A^{-1})^{-1} = A$

2) If A and B are nonsingular matrices, then AB is nonsingular and $(AB)^{-1} = B^{-1} A^{-1}$
3) If A is nonsingular then $(AT)^{-1} = (A^{-1})^T$
4) If A and B are matrices with $AB = I_n$ then A and B are inverses of each other.

IV. Modular Arithmetic

Modular Arithmetic was invented by Carl Fredrich Gauss in 1801. The arithmetic is a system of integers that wrap around when reaching a certain value called a modulus.

A. Modular Arithmetic Example

An example of this is the 24-hour military time system. The standard clock is only 12-hours and cycles twice in a daily period. If you are charged with playing Taps on the base speaker system at preciously 2200 hours, how would you know what time to play it on a standard clock? The formula to figure this out is: $n = qm + r$. n represents the number you are trying to convert, q is the number you will multiply the modular value, m is the modular value, and r is the remainder. The remainder is the answer.

$$n = qm + r \rightarrow 22 = q * 12 + r \rightarrow$$

$$22 = 1 * 12 + r \rightarrow$$

$$22 = 1 * 12 + 10 \rightarrow$$

$$Answer = 10{:}00\ pm$$

B. Modular Congruence Operator Properties [7]

1) $a \equiv b \bmod p \; if \; n|(a - b)$
2) $(a \bmod p) = (b \bmod p) \Longrightarrow a \equiv b \bmod p$
3) $a \equiv b \bmod p \Longrightarrow b \equiv a \bmod p$
4) $a \equiv b \bmod p$ and $b \equiv a \bmod p \Longrightarrow a \equiv c \bmod p$

C. Modular Arithmetic Operations [7]

1) Addition: $(a + b) \bmod p = [(a \bmod p) + (b \bmod p)] \bmod p$
2) Negation: $-a \bmod p = p - (a \bmod p)$
3) Subtraction: $(a - b) \bmod p = [(a \bmod p) - (b \bmod p)] \bmod p$
4) Multiplication: $(a * b) \bmod p = [(a \bmod p) * (b \bmod p)] \bmod p$
5) Division: $\left(\frac{a}{b}\right) \bmod p = c \; when \; a = (b * c) \bmod p$

V. Hill Cypher

The Hill Cypher is an algorithm invented by the mathematician and educator Dr. Lester S. Hill in 1929. Dr. Hill worked with the US military during World War II sharing his work in linear and modular algebraic ciphers. He is notably one of the best-known contributors to cryptology with his famous Hill Cypher using manipulations of linear algebra through matrix multiplication, inverse matrix, and modular arithmetic to encode and decode messages. The cypher assigns numbers to individual letters on a key, like a=1, b=2, …, z=26 [3]. Once you have replaced the letters with numerical values, you would place the numerical values in a matrix and then multiply the matrix by a key matrix and then run through modular arithmetic to get the final result. A diagram of this process is illustrated in figure 1.

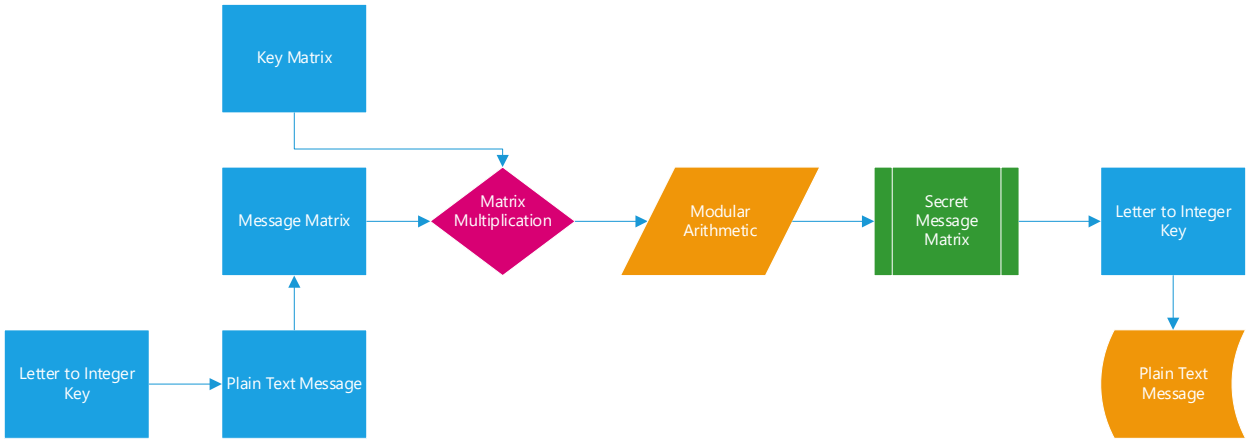

Figure 1: Matrix Encryption Process

The Decryption process is the same except completed in reverse. A diagram of this process is illustrated in figure 2.

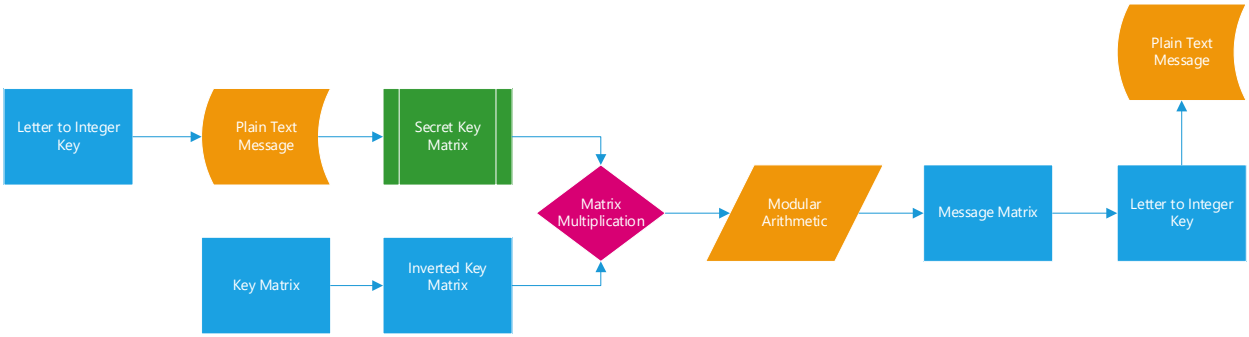

Figure 2: Matrix Decryption Process

A. Encryption Illustration 1

1) Create a $4\ x\ 4$ key matrix with integers

$$K = \begin{bmatrix} 1 & 2 & 3 & 2 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & -1 & -5 \\ 1 & 0 & 0 & 6 \end{bmatrix}$$

2) Using $table\ 1$, assign a numerical value to the letters in the message, I WILL BE ENCODED THEN I WILL BE DECODED and put into a $4\ x\ n$ matrix.

$$Plain\ Text = \begin{bmatrix} I & L & E & C & D & E & W & & D & D \\ & L & & O & & N & I & B & E & E \\ W & & E & D & T & & L & E & C & D \\ I & B & N & E & H & I & L & & O & \end{bmatrix}$$

$$M = \begin{bmatrix} 9 & 12 & 5 & 3 & 4 & 5 & 23 & 27 & 4 & 4 \\ 27 & 12 & 27 & 15 & 27 & 14 & 9 & 2 & 5 & 5 \\ 23 & 27 & 5 & 4 & 20 & 27 & 12 & 5 & 4 & 4 \\ 9 & 2 & 14 & 5 & 8 & 9 & 12 & 27 & 15 & 27 \end{bmatrix}$$

3) Multiply matrices $K\ x\ M\ =\ KM$

$$K = \begin{bmatrix} 1 & 2 & 3 & 2 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & -1 & -5 \\ 1 & 0 & 0 & 6 \end{bmatrix} M = \begin{bmatrix} 9 & 12 & 5 & 3 & 4 & 5 & 23 & 27 & 4 & 4 \\ 27 & 12 & 27 & 15 & 27 & 14 & 9 & 2 & 5 & 5 \\ 23 & 27 & 5 & 4 & 20 & 27 & 12 & 5 & 3 & 4 \\ 9 & 2 & 14 & 5 & 8 & 9 & 12 & 27 & 15 & 27 \end{bmatrix}$$

$$KM = \begin{bmatrix} 168 & 125 & 130 & 65 & 150 & 150 & 125 & 154 & 83 & 134 \\ 82 & 68 & 51 & 28 & 75 & 77 & 45 & 39 & 26 & 40 \\ -68 & -37 & -75 & -29 & -60 & -72 & -72 & -140 & -78 & -139 \\ 63 & 24 & 89 & 33 & 52 & 59 & 95 & 189 & 94 & 166 \end{bmatrix}$$

4) Take the KM matrix and perform modular arithmetic using mod 27 which will result in the matrix S

$$KM = \begin{bmatrix} 168 & 125 & 130 & 65 & 150 & 150 & 125 & 154 & 83 & 134 \\ 82 & 68 & 51 & 28 & 75 & 77 & 45 & 39 & 26 & 40 \\ -68 & -37 & -75 & -29 & -60 & -72 & -72 & -140 & -78 & -139 \\ 63 & 24 & 89 & 33 & 52 & 59 & 95 & 189 & 94 & 166 \end{bmatrix} (Mod\ 27)$$

$$S = \begin{bmatrix} 6 & 17 & 22 & 11 & 15 & 15 & 17 & 19 & 2 & 26 \\ 1 & 14 & 24 & 1 & 21 & 23 & 18 & 12 & 26 & 13 \\ 13 & 17 & 6 & 25 & 21 & 9 & 9 & 22 & 3 & 23 \\ 9 & 24 & 8 & 6 & 25 & 5 & 14 & 0 & 13 & 4 \end{bmatrix}$$

5) Using $table$ 1 as a key, replace the numerical values to the letters in the matrix S

$$S = \begin{bmatrix} 6 & 17 & 22 & 11 & 15 & 15 & 17 & 19 & 2 & 26 \\ 1 & 14 & 24 & 1 & 21 & 23 & 18 & 12 & 26 & 13 \\ 13 & 17 & 6 & 25 & 21 & 9 & 9 & 22 & 3 & 23 \\ 9 & 24 & 8 & 6 & 25 & 5 & 14 & 0 & 13 & 4 \end{bmatrix} \rightarrow \begin{bmatrix} F & Q & V & K & O & O & Q & S & B & Z \\ A & N & X & A & U & W & R & L & Z & M \\ M & Q & F & Y & U & I & I & V & C & W \\ I & X & H & F & Y & E & N & & M & D \end{bmatrix}$$

B. Decryption Illustration 1

1) Using $table$ 1, replace the letters with the numerical values in the matrix S

$$S = \begin{bmatrix} F & Q & V & K & O & O & Q & S & B & Z \\ A & N & X & A & U & W & R & L & Z & M \\ M & Q & F & Y & U & I & I & V & C & W \\ I & X & H & F & Y & E & N & & M & D \end{bmatrix} \rightarrow \begin{bmatrix} 6 & 17 & 22 & 11 & 15 & 15 & 17 & 19 & 2 & 26 \\ 1 & 14 & 24 & 1 & 21 & 23 & 18 & 12 & 26 & 13 \\ 13 & 17 & 6 & 25 & 21 & 9 & 9 & 22 & 3 & 23 \\ 9 & 24 & 8 & 6 & 25 & 5 & 14 & 27 & 13 & 4 \end{bmatrix}$$

2) Take K matrix and produce its inverse matrix K^{-1}

$$K = \begin{bmatrix} 7 & 20 & 3 & 8 \\ 13 & 4 & 15 & 2 \\ 6 & 19 & 17 & 10 \\ 11 & 12 & 9 & 24 \end{bmatrix} \rightarrow K^{-1} = \begin{bmatrix} -6 & 12 & 6 & 7 \\ 9 & -17 & -7 & -9 \\ -5 & 10 & 4 & 5 \\ 1 & -2 & -1 & -1 \end{bmatrix}$$

3) Multiply matrices $K^{-1}\ x\ S = K^{-1}S$

$$K^{-1} = \begin{bmatrix} -6 & 12 & 6 & 7 \\ 9 & -17 & -7 & -9 \\ -5 & 10 & 4 & 5 \\ 1 & -2 & -1 & -1 \end{bmatrix} S = \begin{bmatrix} 6 & 17 & 22 & 11 & 15 & 15 & 17 & 19 & 2 & 26 \\ 1 & 14 & 24 & 1 & 21 & 23 & 18 & 12 & 26 & 13 \\ 13 & 17 & 6 & 25 & 21 & 9 & 9 & 22 & 3 & 23 \\ 9 & 24 & 8 & 6 & 25 & 5 & 14 & 27 & 13 & 4 \end{bmatrix}$$

$$K^{-1}S = \begin{bmatrix} 117 & 276 & 248 & 72 & 463 & 275 & 266 & 351 & 409 & 166 \\ -135 & -330 & -324 & -48 & -594 & -364 & -342 & -430 & -562 & -184 \\ 77 & 193 & 194 & 30 & 344 & 216 & 201 & 248 & 327 & 112 \\ -18 & -42 & -40 & -11 & -73 & -45 & -42 & -54 & -66 & -27 \end{bmatrix}$$

4) Take the $K^{-1}S$ matrix and perform modular arithmetic using mod 27 which will result in the message matrix M

$$K^{-1}S = \begin{bmatrix} 117 & 336 & 248 & 138 & 463 & 275 & 266 & 351 & 409 & 166 \\ -135 & -420 & -324 & -147 & -594 & -364 & -342 & -430 & -562 & -184 \\ 77 & 243 & 194 & 85 & 344 & 216 & 201 & 248 & 327 & 112 \\ -18 & -52 & -40 & -22 & -73 & -45 & -42 & -54 & -66 & -27 \end{bmatrix} (mod\ 27)$$

$$M = \begin{bmatrix} 9 & 12 & 5 & 3 & 4 & 5 & 23 & 27 & 4 & 4 \\ 27 & 12 & 27 & 15 & 27 & 14 & 9 & 2 & 5 & 5 \\ 23 & 27 & 5 & 4 & 20 & 27 & 12 & 5 & 4 & 4 \\ 9 & 2 & 14 & 5 & 8 & 9 & 12 & 27 & 15 & 27 \end{bmatrix}$$

5) Using table 1, replace the numerical values with letters in matrix S.

$$M = \begin{bmatrix} 9 & 12 & 5 & 3 & 4 & 5 & 23 & 27 & 4 & 4 \\ 27 & 12 & 27 & 15 & 27 & 14 & 9 & 2 & 5 & 5 \\ 23 & 27 & 5 & 4 & 20 & 27 & 12 & 5 & 4 & 4 \\ 9 & 2 & 14 & 5 & 8 & 9 & 12 & 27 & 15 & 27 \end{bmatrix} \rightarrow$$

$$M = \begin{bmatrix} I & L & E & C & D & E & W & & D & D \\ & L & & O & & N & I & B & E & E \\ W & & E & D & T & & L & E & C & D \\ I & B & N & E & H & I & L & & O & \end{bmatrix}$$

6) To reveal the message, write the letters and blank spaces, beginning form the first column down.

$$Secret\ Message = \text{I WILL BE ENCODED THEN I WILL BE DECODED}$$

C. Encryption Illustration 2

To illustrate another option, we will use a 3 x 3 matrix for the message with a different letter to numerical value key ($table$ 2) and added some punctuation.

1) Create a 3 x 3 key matrix with integers

$$K = \begin{bmatrix} 15 & 4 & -5 \\ -12 & -3 & 4 \\ -4 & -1 & 1 \end{bmatrix}$$

2) Using $table$ 2, assign a numerical value to the letters in the message, A SENSITIVE MESSAGE. “MATH IS FUN” and put into a 3 x n matrix.

$$Plain\ Text = \begin{bmatrix} A & E & I & V & M & S & E & "M & T & I & F & . \\ & N & T & E & E & A & . & M & H & S & U & " \\ S & S & I & & S & G & & A & & & N & \end{bmatrix}$$

$$M = \begin{bmatrix} 28 & 1 & 12 & 6 & 19 & 5 & 1 & 2 & 27 & 1 & 14 & 15 \\ 23 & 11 & 27 & 1 & 1 & 28 & 15 & 19 & 3 & 5 & 24 & 2 \\ 5 & 5 & 12 & 23 & 5 & 10 & 23 & 28 & 23 & 23 & 11 & 23 \end{bmatrix}$$

3) Multiply matrices $K\ x\ M\ =\ KM$

$$K = \begin{bmatrix} 15 & 4 & -5 \\ -12 & -3 & 4 \\ -4 & -1 & 1 \end{bmatrix} M = \begin{bmatrix} 28 & 1 & 12 & 6 & 19 & 5 & 1 & 2 & 27 & 1 & 14 & 15 \\ 23 & 11 & 27 & 1 & 1 & 28 & 15 & 19 & 3 & 5 & 24 & 2 \\ 5 & 5 & 12 & 23 & 5 & 10 & 23 & 28 & 23 & 23 & 11 & 23 \end{bmatrix}$$

$$KM = \begin{bmatrix} 487 & 34 & 228 & -21 & 264 & 137 & -40 & -34 & 302 & -80 & 251 & 118 \\ -385 & -25 & -177 & 17 & -211 & -104 & 35 & 31 & -241 & 65 & -196 & -94 \\ -130 & -10 & -63 & -2 & -72 & -38 & 4 & 1 & -88 & 14 & -69 & -39 \end{bmatrix}$$

4) Take the KM matrix and implement modular arithmetic using $mod\ 29$ which will result in the matrix S.

$$KM \begin{bmatrix} 487 & 34 & 228 & -21 & 264 & 137 & -40 & -34 & 302 & -80 & 251 & 118 \\ -385 & -25 & -177 & 17 & -211 & -104 & 35 & 31 & -241 & 65 & -196 & -94 \\ -130 & -10 & -63 & -2 & -72 & -38 & 4 & 1 & -88 & 14 & -69 & -39 \end{bmatrix} (mod\ 29)$$

$$S = \begin{bmatrix} 23 & 5 & 25 & 8 & 3 & 21 & 18 & 24 & 12 & 7 & 19 & 2 \\ 21 & 4 & 26 & 17 & 21 & 12 & 6 & 2 & 20 & 7 & 7 & 22 \\ 15 & 19 & 24 & 27 & 15 & 20 & 4 & 1 & 28 & 14 & 18 & 19 \end{bmatrix}$$

5) Using $table\ 2$, replace the numerical values to the letters in the matrix S.

$$S = \begin{bmatrix} 23 & 5 & 25 & 8 & 3 & 21 & 18 & 24 & 12 & 7 & 19 & 2 \\ 21 & 4 & 26 & 17 & 21 & 12 & 6 & 2 & 20 & 7 & 7 & 22 \\ 15 & 19 & 24 & 27 & 15 & 20 & 4 & 1 & 28 & 14 & 18 & 19 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} & S & P & K & H & L & W & U & I & C & M & " \\ L & Y & A & O & L & I & V & " & B & C & C & D \\ . & M & U & T & . & B & Y & E & A & F & W & M \end{bmatrix}$$

D. Decryption Illustration 2

Now we decrypt the message.

1) Using $table\ 2$ as a key, replace the letters with the numerical values in the matrix S.

$$S = \begin{bmatrix} & S & P & K & H & L & W & U & I & C & M & " \\ L & Y & A & O & L & I & V & " & B & C & C & D \\ . & M & U & T & . & B & Y & E & A & F & W & M \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 23 & 5 & 25 & 8 & 3 & 21 & 18 & 24 & 12 & 7 & 19 & 2 \\ 21 & 4 & 26 & 17 & 21 & 12 & 6 & 2 & 20 & 7 & 7 & 22 \\ 15 & 19 & 24 & 27 & 15 & 20 & 4 & 1 & 28 & 14 & 18 & 19 \end{bmatrix}$$

2) Take K matrix and produce its inverse matrix K^{-1}.

$$K = \begin{bmatrix} 15 & 4 & -5 \\ -12 & -3 & 4 \\ -4 & -1 & 1 \end{bmatrix} \rightarrow K^{-1} = \begin{bmatrix} -1 & -1 & -1 \\ 4 & 5 & 0 \\ 0 & 1 & -3 \end{bmatrix}$$

3) Multiply matrices $K^{-1}\ x\ S = K^{-1}S$

$$K^{-1} = \begin{bmatrix} -1 & -1 & -1 \\ 4 & 5 & 0 \\ 0 & 1 & -3 \end{bmatrix} S = \begin{bmatrix} 23 & 5 & 25 & 8 & 3 & 21 & 18 & 24 & 12 & 7 & 19 & 2 \\ 21 & 4 & 26 & 17 & 21 & 12 & 6 & 2 & 20 & 7 & 7 & 22 \\ 15 & 19 & 24 & 27 & 15 & 20 & 4 & 1 & 28 & 14 & 18 & 19 \end{bmatrix}$$

$$K^{-1}S = \begin{bmatrix} -59 & -28 & -75 & -52 & -39 & -53 & -28 & -27 & -60 & -28 & -34 & -43 \\ 197 & 40 & 230 & 117 & 117 & 144 & 102 & 106 & 148 & 63 & 71 & 118 \\ -24 & -53 & -44 & -64 & -24 & -48 & -6 & -1 & -64 & -35 & -47 & -35 \end{bmatrix}$$

4) Take the $K^{-1}S$ matrix and perform modular arithmetic using $mod\ 29$ which will result in the message matrix M = Message Matrix

$$K^{-1}S = \begin{bmatrix} -30 & -28 & -75 & -52 & -39 & -53 & -28 & -27 & -60 & -28 & -34 & -43 \\ 119 & 40 & 230 & 117 & 117 & 144 & 102 & 106 & 148 & 63 & 71 & 118 \\ 5 & -53 & -46 & -64 & -24 & -48 & -6 & -1 & -64 & -35 & -47 & -35 \end{bmatrix} (mod\ 29)$$

$$M = \begin{bmatrix} 28 & 1 & 12 & 6 & 19 & 5 & 1 & 2 & 27 & 1 & 14 & 15 \\ 23 & 11 & 27 & 1 & 1 & 28 & 15 & 19 & 3 & 5 & 24 & 2 \\ 5 & 5 & 12 & 23 & 5 & 10 & 23 & 28 & 23 & 23 & 11 & 23 \end{bmatrix}$$

5) Using $table\ 2$, replace the numerical values with letters in the matrix M.

$$M = \begin{bmatrix} 28 & 1 & 12 & 6 & 19 & 5 & 1 & 2 & 27 & 1 & 14 & 15 \\ 23 & 11 & 27 & 1 & 1 & 28 & 15 & 19 & 3 & 5 & 24 & 2 \\ 5 & 5 & 12 & 23 & 5 & 10 & 23 & 28 & 23 & 23 & 11 & 23 \end{bmatrix} \rightarrow$$

$$Plain\ Text = \begin{bmatrix} A & E & I & V & M & S & E & "M & T & I & F & . \\ & N & T & E & E & A & . & M & H & S & U & " \\ S & S & I & & S & G & & A & & & N & \end{bmatrix}$$

6) To reveal the message, simply write the letters and blank spaces, beginning form the first column down.

$$Secret\ Message = \text{A SENSITIVE MESSAGE. “MATH IS FUN”}$$

VI. Project Problems

Some of the problems I had with this project:

1) When creating a $n\ x\ n$ matrix with random integers, I had difficulty getting similar inverse results. For the encryption to work, I needed to have the inverse results have only whole numbers in the matrix. Many of the matrices I tried would end up with fractions so when it came to performing the modular arithmetic it would end up with fraction or number I could not use. This problem took up a lot of time to fix and I am sure there is a better way of accomplishing that goal without getting fractions. Additionally, I am sure there is another option you could use to work with an inverse matrix that has fractions.
2) When performing the encryption procedures, I would write down the incorrect result in the matrix. This provided me with all kinds of problems down the road. Especially, when I would check the math to make sure it was correct. I had to go back and redo all the problems until I found the mistake and it was time consuming.

VII. Conclusion

In this project paper, I have illustrated a version of Dr. Hill’s Cypher process using linear algebra and modular arithmetic. The process uses matrix manipulation through matrix multiplication, by both the key matrix and its inverse, along with modular arithmetic to both encode and decode messages. Although this system is not the most secure way to hide information, it does illustrate that successful cryptography can be achieved using linear algebra as a base. This system has a lot of applications, for example, you could use this system to encode and decode images. Individual image pixels are represented as matrices of $n\ x\ n$ matrices of integers. Because of the system I have illustrated above you could easily transform the image into a secret message and decrypt it as well.

VIII. Tables

Numeric to Letter Assignment									
A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10
K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20
U	V	W	X	Y	Z				
21	22	23	24	25	26	27/0			

Table 1

Numeric to Letter Assignment									
E	"	H	Y	S	V	C	K	Q	G
1	2	3	4	5	6	7	8	9	10
N	I	X	F	.	J	O	W	M	B
11	12	13	14	15	16	17	18	19	20
L	D		U	P	Z	T	A	R	
21	22	23	24	25	26	27	28	29/0	

Table 2

IX. References

(1) A brief history of cryptography. (1997). Information Security Technical Report, 2(2), 14–17. https://doi.org/10.1016/s1363-4127(97)81323-4

(2) Cryptography. (n.d.). Retrieved November 02, 2020, from https://www.merriam-webster.com/dictionary/cryptography

(3) Hill, L. S. (1929). Cryptography in An Algebraic Alphabet. The American Mathematical Monthly, 36(6), 306–312. https://doi.org/10.1080/00029890.1929.11986963

(4) Ghen. (2019, January 2). *Break Hill Cipher with a Known Plaintext Attack*. Break Hill Cipher with a Known Plaintext Attackeldipa.Github.Io. https://eldipa.github.io/book-of-gehn/articles/2019/01/02/Break-Hill-Cipher-with-a-Known-Plaintext-Attack.html

(5) Kelly, T. (1998). THE MYTH OF THE SKYTALE. Cryptologia, 22(3), 244–260. https://doi.org/10.1080/0161-119891886902

(6) Axler, S. (2014). Linear Algebra Done Right (Undergraduate Texts in Mathematics) (3rd ed. 2015 ed.). Springer.

(7) Acharya, B., Rath,G.S., Patra, S. K., Panigrahy, S. K.. (2016) Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm. International Journal of Security, Vol 1: Issue (1). (PDF) Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm (researchgate.net)
(8) Bogack, P. (2019) Linear Algebra Concepts and Applications, Vol 47.
(9) Davies, D. (1997) A Brief History of Cryptography, Information Security Technical Report, Vol 2, Issue (2) (14-17). https://doi.org/10.1016/S1363-4127(97)81323-4.
(10) Properties of Inverse Matrices - Web Formulas. (n.d.). Web Formulas. Retrieved December 3, 2020, from https://www.web-formulas.com/Math_Formulas/Linear_Algebra_Properties_of_Inverse_Matrices.aspx