Group C

Project 3

[redacted]

September 2020

Introduction

This report presents an implementation of an algorithm using matrices for encryption and decryption of plaintext messages. Our algorithm is capable of encoding plaintext messages of any size and any character set into a ciphertext which can be typed on a standard keyboard.

The security of the algorithm we will present is based on cipher keys. Keys are simple to generate and are made up of a sequence of numbers and can vary in length and be as little as 4 numbers. For this report we will use a 3x3 matrix with 9 numbers, for increased security. Even with knowledge of the encryption algorithm, messages will remain secure as long as the key is not leaked. The key must be distributed to anyone who needs to encode or decode messages. As such, it is imperative that the key be safeguarded.

Explanation and Example

The algorithm uses the knowledge that $A^{-1}(AM) = M$ is true, with A and M being matrices. M is our message, put into a matrix, and A is the encryption key. In our example we will use a 3x3 matrix, but this could be changed to 2x2 if it needed to be simplified for any reason, or 4x4, or any bigger square matrix, to be even more secure. A 3x3 matrix, which can be represented with 9 numbers, is portable, easy to generate, and significantly less vulnerable to brute force attacks than a 2x2 matrix.

Encryption - Step 1

We start with a plaintext message. We will use the short phrase ”the quick onyx goblin jumps over the lazy dwarf” as an example. The plaintext message is translated to numbers using the scheme A=1, B=2, C=3... with the space character represented as the number 27. The resulting message after applying this translation is shown below.

20 8 5 27 17 21 9 3 11 27 15 14 25 24 27 7 15 2 12 9 14 27 10 21 13 16 19 27 15 22 5 18 27 20 8 5 27 12 1 26 25 27 4 23 1 18 6

The translation scheme we have presented above is a simple one representing all lower case letters of the alphabet and the space character which we believe is sufficient for sending basic encrypted messages. However, alternative schemes can be used that include other character sets if this is not sufficient. In order to add other characters, each new character must be assigned a unique number. For the purpose of sending readable messages, representing the alphabet and space character is sufficient.

Encryption - Step 2

The translated message is put into a matrix with three rows. Since the original message has 47 characters, the matrix will have 16 columns. Because 47 does not divide equally into 3, we will pad the final row with 0s so that each row has the same length.

$$M = \begin{bmatrix} 20 & 8 & 5 & 27 & 17 & 21 & 9 & 3 & 11 & 27 & 15 & 14 & 25 & 24 & 27 & 7 \\ 15 & 2 & 12 & 9 & 14 & 27 & 10 & 21 & 13 & 16 & 19 & 27 & 15 & 22 & 5 & 18 \\ 27 & 20 & 8 & 5 & 27 & 12 & 1 & 26 & 25 & 27 & 4 & 23 & 1 & 18 & 6 & 0 \end{bmatrix}$$

Encryption - Step 3

We will use the A as our encryption key matrix represented by a string of 9 numbers. The first 3 numbers of the key correspond to the first row of the matrix, the next 3 to the second row, and the last 3 to the final row. This could be any 3x3 matrix as long as it has an inverse, but the following will be used in our example as it has only integers in both the original matrix and its inverse.

$$A = \begin{bmatrix} -1 & 5 & -1 \\ -2 & 11 & 7 \\ 1 & -5 & 2 \end{bmatrix}$$

Encryption - Step 4

We then use the equation $AM = E$ Where E is the encoded matrix. Because of how matrix multiplication works, there is no single number that corresponds to every instance of that letter, and would be near impossible to decipher without the encryption key.

$$E = \begin{bmatrix} 28 & -18 & 47 & 13 & 26 & 102 & 40 & 76 & 29 & 26 & 76 & 98 & 49 & 68 & -8 & 83 \\ 314 & 146 & 178 & 80 & 309 & 339 & 99 & 407 & 296 & 311 & 207 & 430 & 122 & 320 & 43 & 184 \\ -1 & 38 & -39 & -8 & 1 & -90 & -39 & -50 & -4 & 1 & -72 & -75 & -48 & -50 & 14 & -83 \end{bmatrix}$$

Encryption - Step 5

This message is converted to a string of numbers, as shown below.

28 -18 47 13 26 102 40 76 29 26 76 98 49 68 -8 83 314 146 178 80 309 339 99 407 296 311 207 430 122 320 43 184 -1 38 -39 -8 1 -90 -39 -50 -4 1 -72 -75 -48 -50 14 -83

Encryption - Step 6

The next step is to convert the numbers into letters. This will create the ciphertext that is sent. We will use the following algorithm, which is a very similar scheme to the translation we did at the beginning that converted letters to numbers. The algorithm is shown below:

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=0 K=' ' L=-

The cipher text is now:

LADKHAKAAIKGAKLBIKLIKECKLBIKIJKHIKAIKLEKEIKADHKAHIKCBHKBJFKAIJKABJKBHFK AIJKBHAKCGFKBIDKGFKCAGKCCKLHJKLAABKLFFKEFKBDKLCEKEFKLHAKLGJKHKADKLCI

Decryption

Once received, the ciphertext is decoded by reversing step 6 of the encryption algorithm so that the ciphertext is back to a list of numbers with spaces in between. The list of numbers is converted back into a matrix by dividing it into 3 equal rows. In this case we know that the numbers will divide evenly because of the padding in step 2. This gives us the matrix E found in Step 4. After that we multiply the inverse, A^{-1} by the ciphertext matrix, E. The inverse of A is shown below:

$$A^{-1} = \begin{bmatrix} -57 & 5 & -46 \\ -11 & 1 & -9 \\ 1 & 0 & 1 \end{bmatrix}$$

Since $E = AM$, $A^{-1}(E) = A^{-1}(AM)$. We know from the start will simply give us M, the message matrix. From this, it is a simple process to pull out the string of numbers and replace them with the corresponding letter (or space). This gives the original message, known only to the sender and the recipient

Conclusion

The algorithm we have presented is ideal for encrypting messages of any using the standard alphabet. Messages encrypted using our algorithm are not vulnerable to others who may discover the algorithm. The cipher key is necessary to encrypt or decrypt messages and cannot be derived from knowledge of the algorithm or by analyzing the cipher text. The matrix encryption algorithm is a secure algorithm for encoding messages without requiring large resources or computation and results in a ciphertext of english characters. We think this method is an ideal solution for secure, fast messaging.