[redacted]

Group H

Math 485
Dr. Jenkins
September 10, 2020

Encryption Proposal

1 Introduction

Dear Mr. Andrews,

We are sorry to hear that your company has been struggling with security breaches. We are happy to offer our assistance, and we promise not to charge as much as Dr. Paul Jenkins.

Now, as we understand your problem, you need a system for encrypting text messages sent by your workers. It is imperative that the encryption system we provide can comfortably and securely encrypt a message of up to 160 characters while producing a cipher text no longer than 800 characters.

We propose a system based upon a known method- using an invertible matrix for the encoding key- with a slight twist. As we learn from Kerckhoff's principle, the power of a cipher cannot lie in the method alone, but must also lie in the key used. Our system would allow your company to choose from an infinite number of keys- making attack by brute force impossible- while using a simple computation to enact the key.

In this document we provide a detailed explanation of our method of encryption. We hope that you choose to work with us, and promise the results that you desire.

2 Encryption and Decryption

2.1 The Encryption Process

In order to increase the security of your messages, we propose the following system of encryption. For your convenience, a step by step sample of the encryption and decryption process is included below.

We will start by translating the characters of the message into their ASCII codes, which will instantly make them less available to any outsider. We will then add the number 1 twice between the digits, so that we end up with 4 digit numbers representing each character.

Each 4 digit number will then be converted to a 2x2 matrix by entering each digit into the matrix, from the top left to the top right, and then from the bottom left to the bottom right. After this process, we will have a matrix for each character in the message.

Now comes the part that makes the system truly secure. We use a different 2x2 matrix as the encryption key and multiply (using matrix multiplication) each character matrix by the encryption key matrix. This will produce new matrices from each of the original matrices. The reason this is so secure is because the encryption key could be any 2x2 matrix, and without the inverse of the matrix, we cannot convert back to the original matrices.

We then extract the matrix values from the matrices, and line them up without spaces between them. This creates a seemingly random string of a mixture of positive and negative integers, and that is what an attacker would see upon acquiring any messages sent by company employees.

Decryption, with the inverse of the encryption matrix is simple. We simply divide the digits into groups of 4 digits, put them back into matrix form (from the top left to the top right, and then from the bottom left to the bottom right), and multiply each matrix by the inverse of the encryption matrix (the decryption key). This will produce the original matrices. We then write them in groups of 4 numbers again, remove the 11 from between each group, and convert the ASCII codes back into characters.

Plaintext: To be, or not to be

Convert text to uppercase and remove punctuation: TO BE OR NOT TO BE

Translate to ASCII: 84 79 32 66 69 32 79 82 32 78 79 84 32 84 79

Insert extra ones between each character code: 8114 7119 3112 6116 6119 3112 7119 8112 3112 7118 7119 8114 3112 8114 7119

Convert to matrices: $\begin{bmatrix} 8 & 1 \\ 1 & 4 \end{bmatrix}, \begin{bmatrix} 7 & 1 \\ 1 & 9 \end{bmatrix}, \begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 6 & 1 \\ 1 & 6 \end{bmatrix}$, etc.

Right multiply by the 2x2 invertible matrix of your choice: $\begin{bmatrix} 8 & 1 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 7 & 1 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix},$ $\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 6 & 1 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$, etc.

Multiplication results: $\begin{bmatrix} 8 & -7 \\ 1 & 3 \end{bmatrix}, \begin{bmatrix} 7 & -6 \\ 1 & 8 \end{bmatrix}, \begin{bmatrix} 3 & -2 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 6 & -5 \\ 1 & 5 \end{bmatrix}$, etc.

Extract matrix values and piece back together: 8-7137-6183-2116-515...

Outcome: To be, or not to be $\Rightarrow 8 - 7137 - 6183 - 2116 - 5156 - 5183 - 2117 - 6188 - 7113 - 2117 - 6177 - 6188 - 7133 - 2118 - 7137 - 6183 - 2116 - 5156 - 518$

2.2 The Decryption Process

The decryption process is similar. We take the cipher text, rearrange it into matrices, decode it using the inverse of our encrypting matrix, and convert back into letters from the ASCII key characters.

Ciphertext: 8-7137-6183-2116-5156-5183-2117-6188-7113-2117-6177-6188-7133-2118-7137-6183-2116-5156-518

Rearrange as matrices: $\begin{bmatrix} 8 & -7 \\ 1 & 3 \end{bmatrix}, \begin{bmatrix} 7 & -6 \\ 1 & 8 \end{bmatrix}, \begin{bmatrix} 3 & -2 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 6 & -5 \\ 1 & 5 \end{bmatrix}$, etc.

Right multiply by the *inverse* of your encryption matrix: $\begin{bmatrix} 8 & -7 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 7 & -6 \\ 1 & 8 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 3 & -2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix},$ $\begin{bmatrix} 6 & -5 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$, etc.

Multiplication results: $\begin{bmatrix} 8 & 1 \\ 1 & 4 \end{bmatrix}, \begin{bmatrix} 7 & 1 \\ 1 & 9 \end{bmatrix}, \begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 6 & 1 \\ 1 & 6 \end{bmatrix}$, etc.

Take out of matrix form: 8114 7119 3112 6116 6119 3112 7119 8112 3112 7118 7119 8114 3112 8114 7119

Remove the extra ones: 84 79 32 66 69 32 79 82 32 78 79 84 32 84 79

Convert from ASCII to letters: TO BE OR NOT TO BE

From here, you can fix casing and replace punctuation however you please.

3 Conclusion

By implementing a method of encryption that requires a key that can be chosen from an infinite number of possibilities, we can guarantee that your messages will be kept private and secure. The system is multi-leveled, implementing the translation of letters to numbers, numbers to matrices, and matrices to different matrices. To the naked eye, the encryption will appear completely undecipherable. Even to the most skilled attacker who is aware of our method of encryption, the prospects of deciphering by brute force are impossible.

Again, we are sorry to hear that your company has been affected by breaches and attacks. Our system of encryption will provide security and peace of mind, so that you can continue to succeed and grow as an organization.

Sincerely,

[redacted]