How to Keep Classified Information Classified

Lindsey Skelton

CSULB

Math247

Dr. Jen Mei Chang

Introduction

The type of ciphers used in this presentation are Hill ciphers, named after Lester S. Hill, which were invented in 1929. The message that has yet to be encrypted is called plain text, the message afterwards is called ciphertext. The process of changing plaintext to ciphertext is called encryption, the reverse process is called deciphering.

The process of cryptography has been around for thousands of years, and has been revolutionized in the 20th century due to our complex machines and more complex and efficient ways of encryption. Society as a whole is getting more secretive, which creates an exponential demand for being able to keep secrets. One of the more notable uses of cryptography was the US's interception of the Zimmerman telegram which eventually led to the U.S.'s involvement in WWI.

Enciphering

$$A = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$$

The invertible enciphering matrix

$$P = \begin{bmatrix} 20 & 18 & 9 & 1 & 15 & 5 & 19 & 13 & 19 & 18 \\ 5 & 13 & 14 & 13 & 19 & 12 & 5 & 5 & 20 & 5 \end{bmatrix}$$

We assign values to each letter of the alphabet, a-1, b-2,…z-26. Spelling out our plain text phrase "Terminamos el semestre" and putting them into matrix P

Now We Multiply AP

$$AP = \begin{bmatrix} 130 & 168 & 129 & 83 & 189 & 97 & 125 & 95 & 215 & 120 \\ 55 & 75 & 60 & 41 & 87 & 46 & 53 & 41 & 98 & 51 \end{bmatrix}$$

Since there are no letters corresponding to these numbers, we simplify them modulo 26

$$AP \equiv \begin{bmatrix} 26 & 12 & 25 & 5 & 7 & 19 & 21 & 17 & 7 & 10 \\ 3 & 23 & 8 & 15 & 9 & 20 & 1 & 15 & 20 & 25 \end{bmatrix}$$

We have now successfully encrypted our message

Deciphering

Now to completely decipher our ciphertext, we multiply A inverse by AP to get our original P

$$A^{-1}AP = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \begin{bmatrix} 26 & 12 & 25 & 5 & 7 & 19 & 21 & 17 & 7 & 10 \\ 3 & 23 & 8 & 15 & 9 & 20 & 1 & 15 & 20 & 25 \end{bmatrix}$$

$$= \begin{bmatrix} 98 & 564 & 217 & 365 & 223 & 499 & 45 & 377 & 487 & 610 \\ 265 & 533 & 352 & 325 & 227 & 532 & 187 & 421 & 436 & 555 \end{bmatrix} \equiv$$

$$\begin{bmatrix} 20 & 18 & 9 & 1 & 15 & 5 & 19 & 13 & 19 & 18 \\ 5 & 13 & 14 & 13 & 19 & 12 & 5 & 5 & 20 & 5 \end{bmatrix} (\mathrm{mod}\, 26)$$

Deciphering

In order to decipher our ciphertext, we need to find the inverse of our key matrix A.

$$A^{-1} = \det^{-1} \begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} = 3^{-1} = 9 (\mathrm{mod}\, 26)$$

$$A^{-1} = 9 \begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} = \begin{bmatrix} 27 & -54 \\ -18 & 45 \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} (\mathrm{mod}\, 26)$$

Sweet Success

Translating each number back into letters using our system, we have: Terminamos El Semestre, which translated from Spanish means "We Finished The Semester". Thus we have successfully encrypted our plain text as well as deciphered our ciphertext, and can now enjoy summer vacation.

References

Paal Schiefloe Cryptography Project (accessed May 3-May13 2009) http://www.math.washington.edu/~king/coursedir/m308a01/Projects/Cryptography.htm