Cryptography

Rizmont Rion Angeles

Introduction

Cryptography is the study of the techniques of writing and decoding messages and code.

Cipher: a procedure to render messages Unintelligible except to the recipient

Plaintext: the message or information before the cipher is used

Ciphertext: the message or information after the cipher is used

Classical Methods

The Shift Cipher

Dating back to the time of Julius Caesar, it is one of the oldest ciphers. It is clearly bad In terms of its secrecy and security, but it is from it's failures, that derives examples of what not to do.

Encryption: each letter of the message is simply shifted forward a certain number of times

Decryption: each letter is shifted backwards The same specified number of times

"Treavor likes pie"
20,18,5,1,22,15,18 12,9,11,5,19 16,9,5

Would be shifted to by 1 to...

"usfbwps mjlft qjf"
21,19,6,2,23,16,19 13,10,12,6,20 17,10,6

Affine Cipher

A much more effective shift cipher due to its larger keysize

$$E_{a,b}(x) = (a * x + b) \bmod 26 \text{ for } a, b = 0 \ldots 25$$

$$D_{a,b} = E^{-1} a, b = E^{-1} a, -a^{-1} * b = (a * c) \bmod 26 = 1, -((a * c) \bmod 26 * b) \bmod 26$$

$$E_{3,11}(\text{hello how are you}) = GXSSB\ GBZ\ LKX\ FBT$$

The Known Plaintext Attack on the Affine Cipher

$$a = ((E_{a,b}(x) - E\, a, b(y))/(x - y)) \bmod 26$$

$$b = (E_{a,b}(x) - a * x) \bmod 26$$

Using Matrices

A Matrix can be used as a cipher assuming it has an inverse that can be used to decipher

$$Cipher = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 0 & 3 \\ 4 & -3 & 8 \end{bmatrix}$$

$$TREAVOR = 20, 18, 5, 1, 22, 15, 19$$

$$TREAVOR = \begin{bmatrix} 20 & 1 & 18 \\ 18 & 22 & 27 \\ 5 & 15 & 27 \end{bmatrix}$$

$$Cipher * Treavor = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 0 & 3 \\ 4 & -3 & 8 \end{bmatrix} * \begin{bmatrix} 20 & 1 & 18 \\ 18 & 22 & 27 \\ 5 & 15 & 27 \end{bmatrix} = \begin{bmatrix} 28 & 52 & 81 \\ 35 & 46 & 99 \\ 66 & 58 & 207 \end{bmatrix}$$

$$(Inverse\ Cipher) * (Cipher * TREAVOR) = \begin{bmatrix} -9/2 & 7 & -3/2 \\ -2 & 4 & -1 \\ 3/2 & -2 & 1/2 \end{bmatrix} * \begin{bmatrix} 28 & 52 & 81 \\ 35 & 46 & 99 \\ 66 & 58 & 207 \end{bmatrix} = \begin{bmatrix} 20 & 1 & 18 \\ 18 & 22 & 27 \\ 5 & 15 & 27 \end{bmatrix}$$

Results

Shift Cipher: simple in design but it's that simplicity that leads to it's weaknesses. The cipher is highly susceptible to brute force attacks, and once the cipher is discovered, it takes just as much time to decipher as it does to cipher.

Affine Cipher: much more difficult to decipher. still susceptible to brute force attacks although it will take much longer. Multiple repetitions of the cipher does not increase it's security.

Matrices: difficult to decipher if the original matrix is not known. Impossible to even encrypt, if the matrix is non invertible.

References

Garrett, P. (2001). Making, Breaking Codes. New Jersey: Prentice Hall, Inc.