INFORME DE QUIZ 1

Criptosustitución

García Grimaldos, Alberto Manuel; Álvarez Caballero, Hernán David
alberto.garcia.2016@upb.edu.co; hernan.alvarez.2014@upb.edu.co
Universidad Pontificia Bolivariana
Seccional Bucaramanga
Octubre 6 de 2019

I. OBJETIVOS DE DESARROLLO

Objetivo General

– *Identificar y comprender los procedimientos criptográficos antiguos por sustitución y transposición, mediante la práctica de ejercicios manuales y algorítmicos, con el fin de sentar una base teórico-práctica para el entendimiento de los procedimientos criptográficos modernos.*

II. INTRODUCCIÓN

Los algoritmos de criptosustitucón, son la base de la criptografía clásica, por lo que comprenderlos bien, puede ayudar a traer claridad acerca del funcionamiento del cifrado en la criptografía moderna. Dada la antigüedad de estos métodos, existe la facilidad de utilizarlos y comprobarlos a mano, sin la necesidad de un computador para ello, por lo que pueden ser una excelente oportunidad para aprender de criptografía practicando con ejercicios manuales.

III. PROCEDIMIENTO

Teniendo **a=2** y **b=49**, se realiza la decimación en factor dos y la rotación en 49%26, pero, teniendo en cuenta las reglas del cifrado, sabemos que **a** no puede ser par, ni estar dentro del conjunto de divisores de **n** (26), por lo que, al intentar descifrar, obtendremos un error.

```
Enter the 'a' value: 2
Enter the 'b' value: 49
Enter the text to be encrypted: es hora de ganar
Affine encryption result: FHLZFXDFJXXXF
```

Descifrando el criptograma "JTTCQTGXZYAFNIC" con **a=37** y **b=125,** podemos percatarnos de que **a** cumple con todas las reglas del cifrado, por lo que no obtenemos un error al descifrar, como en el punto anterior. El mensaje en claro es "**GOODJOBMYFRIEND**".

```
Enter the 'a' value: 37
Enter the 'b' value: 125
Enter the text to be decrypted: JTTCQTGXZYAFNIC
Affine decryption result: GOODJOBMYFRIEND
```

Para el tercer punto se utilizan las reglas inversas del cifrado de playfair para dar con el posible resultado.

CZ-> E?, OQ-> I/J T, EN-> OE, TN-> NE, IR-> ¿Q, VW-> ¿?, YE-> DZ, AD-> EC, WC-> ¿?, TD-> SE, AV-> BU, NT-> EN, PS-> ¿?, BC-> AB, BW-> ¿?, LZ-> ¿?

Para el punto cuatro, encontramos que no hay diferencia alguna en utilizar la clave "ARAR" o "AR", pues en este tipo de cifrado, la clave es cíclica

En el quinto punto se deben pasar por la compuerta XOR tanto criptograma como mensaje en claro, así se logrará la consecución de la cadena, pues este tipo de cifrado es simétrico, y la posible variación de bit a bit es del 50/50.