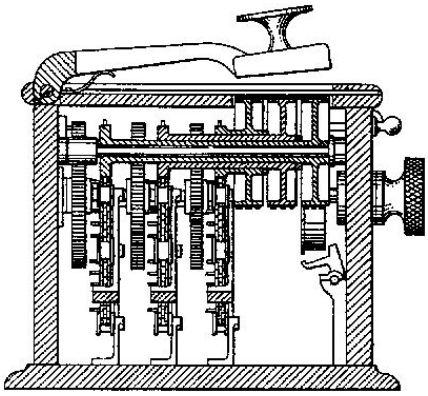
Instituto Politécnico Nacional

Escuela Superior de Cómputo

Cryptography

Práctica 3.2: Descifrado Hill cipher (equipos)
13/02/19



Nombres:

- Santuario Parra Luis Fernando
- Varela Cruz Cesar Alejandro

Grupo: 3CM6

Introducción

Como todo en la vida al existir secretos siempre habrá alguien que quiera obtener esa información para su propio uso y beneficio [1]. El principal problema que tienen y seguirán teniendo los criptologos es la posibilidad de que alguien usando mecanismos como el criptoanálisis quieran romper los métodos de cifrados vigentes para así poder obtener información [3].

Nosotros conocemos el método de cifrado llamado “Hill cipher” dicho método utiliza una matriz cuadrada de nxn para poder cifrar y descifrar un mensaje dado, sin embargo a pesar que por el procedimiento de cifrado y descifrado pudiera parecer seguro la realidad es que existe un método de criptoanálisis que permite romper dicha seguridad con un ataque conocido como “ Ataque por texto claro conocido”, que consiste en tener pares de texto en claro y texto conocido y utilizarlos para poder obtener la llave que se usó para cifrar el mensaje.[4]

Objetivo

Utilizar el criptoanálisis para realizar un ataque por texto claro conocido a un cifrado Hill. Siendo capaz de obtener la llave (la matriz) con la que fue encriptado un texto al ingresar un texto cifrado y el texto en claro correspondiente, y finalmente descifrar el texto completo una vez habiendo obtenido la llave, esto haciéndolo con el par de textos dados por otro equipo.

Desarrollo

El equipo con el que se trabajo nos dio varios pares de texto en claro y texto cifrado los cuales estaban en una sola línea, sin embargo estos textos tenían una serie de problemas entre los más destacables se encontraba que estaban usando un vector de símbolos de ascii “personalizado”, usando módulo 96 con diferente orden en la posición de los elementos además de haber añadido elementos del ascii extendido.

Una vez solucionados los problemas con el equipo contrario pudimos utilizar el programa que habíamos desarrollado para poder obtener la llave del texto.

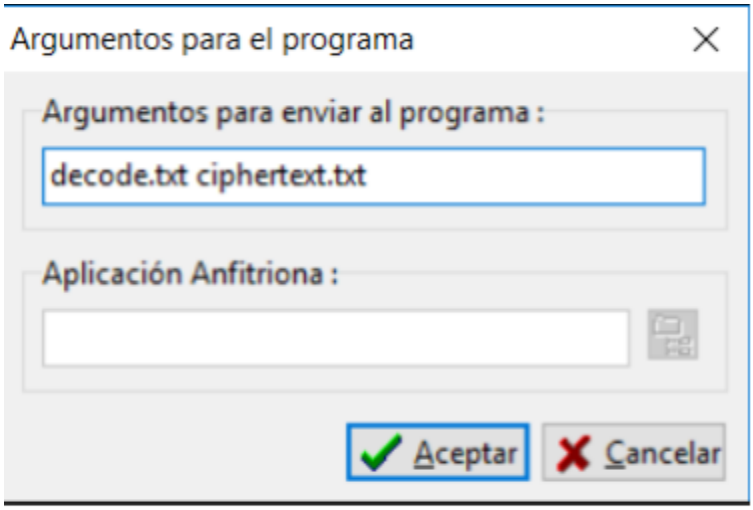


Figura 1. Paso de parámetros al programa (texto en claro y texto cifrado)

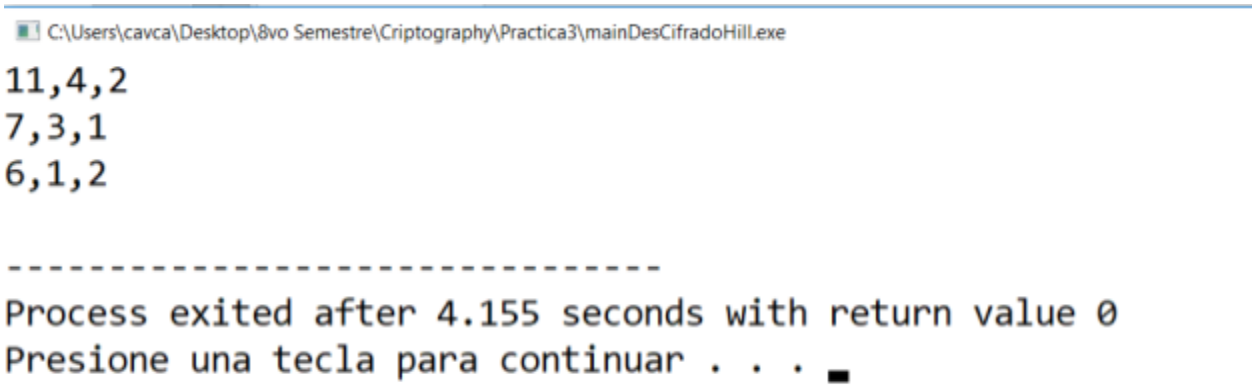


Figura 2. Llave obtenida de pasar el texto en claro y el texto cifrado por el programa

Ahora una vez que obtuvimos la llave procedimos a usar nuestro programa para verificar que está fuera útil para descifrar el texto.

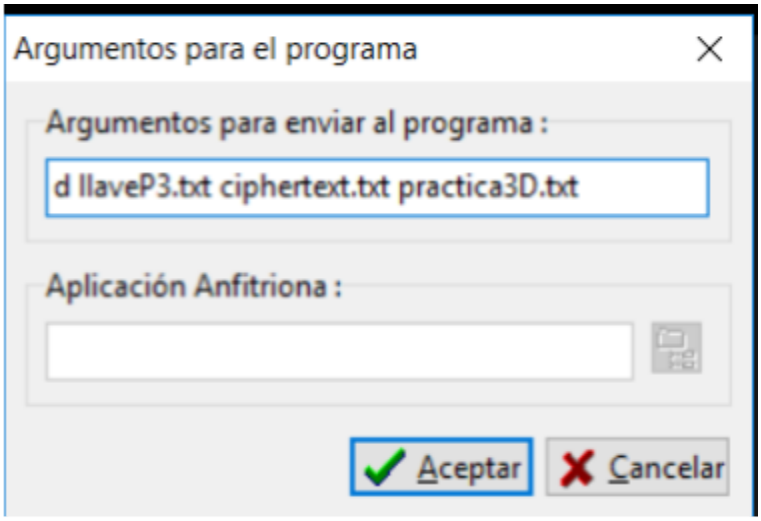


Figura 3. Paso de parámetros al programa para descifrar (Llave, texto cifrado y archivo de salida)

Al momento de correr el programa pudimos corroborar que el programa funciona y la llave obtenida por medio del criptoanálisis fue correcta.

Figura 4. Salida del programa de descifrado utilizando la llave que se obtuvo del criptoanálisis

Conclusión

Santuario Parra Luis Fernando

Durante el desarrollo de esta práctica se utilizó el programa de criptoanálisis de Hill cipher con pares de texto en claro y cifrado proporcionados por otro equipo con lo cual nos pudimos dar cuenta que aunque el concepto es el mismo si la implementación cambia como en el caso de nuestros compañeros que usaron su propio alfabeto y una longitud diferente a la del ascii imprimible, no siempre podrá ser posible descifrar la información a no ser que se conozcan detalles muy particulares de cómo se cifró la información, sin embargo con los arreglos correspondientes se pudo lograr descifrar la información y obtener la llave valida para ese texto cifrado.

César Alejandro Varela Cruz

Como resultado del criptoanálisis, pudimos desarrollar un programa que lograra encontrar la llave utilizada en el cifrado de un texto realizado por Hill Cipher.

Sin embargo pudimos observar algunos de los problemas a los que se enfrentan los criptoanalistas, ya que muchos de nosotros tuvimos que modificar nuestros programas, debido a que nuestros compañeros no habían realizado el mismo alfabeto, o habían realizado arreglos personalizados y nos tuvimos que adaptar los unos a los otros.

Es complicado realizar criptoanálisis, debido a que cada persona puede personalizar incluso los algoritmos preestablecidos.

Anexo (Texto claro y cifrado)

Texto Claro	Texto cifrado
Well, perhaps not, but I wanted to create one anyway for my own enjoyment and edification. And this one is neither too long and intimidating nor is it too skimpy and litee, but, as Goldilocks might have said, just right. Not too much in the way of fricativess and palatizationss and labialized velarss (this does not pretend to be a work of serious philology), but plenty of rollicking historical detail, action and intrigue.	HAQjZfeM1C}waBH90n@!PJ!^[L=je">j6Q'*s Dq{iQKW|muA$83sRDA|T\+Wb{9+#E5Z=,= #|902NDksfu"aQ5ny lls!>j6/:'qAOec"aBHr/#k-!<QV)0<WY"muAZ_ $i*j?qQ5nGWG7c7e4Sk5U<QVS7J,@!}7]g\|^ plZ3Qv{>XGG)T3\3yX7Px7C$d,}E6C#4&P}.3 qU4D!p:V;f7&JRH-or"x[CY<QV/1>RQ%G/IpJ H[q>6Y?KXHJ*N`x]gmETL+muAztJ%;!Q5nek EFK%t1]g|^plZ1]\w{f!g)lMD{1%t1]jjXdgI7.ga BHO$Vrg$yY1>j6K&(5[pQZY1sSKXH(Y7pR3 mDLc3wy[0Pz]Z4^3<bHU|&yJA9?.KT4I|("iG WG/:'y{C`x]6z&M=f{^Z+j+=f7:!$2NDcN0UV #|{o

Referencias

[1]*Egov.ufsc.br*, 2019. [Online]. Available: http://www.egov.ufsc.br/portal/sites/default/files/la_criptografia_desde_la_antigua_grecia_hasta_la_maquina_enigma1.pdf. [Accessed: 12- Feb- 2019].

[2]"Historia de la Criptografía | Seguridad en Cómputo", *Blogs.acatlan.unam.mx*, 2019. [Online]. Available: http://blogs.acatlan.unam.mx/lasc/2016/06/15/historia-de-la-criptografia/. [Accessed: 12- Feb- 2019].

[3]"Criptografía y criptoanálisis: la dialéctica de la seguridad | Revista .Seguridad", *Revista.seguridad.unam.mx*, 2019. [Online]. Available: https://revista.seguridad.unam.mx/numero-17/criptograf%C3%AD-y-criptoan%C3%A1lisis-la-dial%C3%A9ctica-de-la-seguridad. [Accessed: 27- Feb- 2019].

[4]"Practical Cryptography", *Practicalcryptography.com*, 2019. [Online]. Available: http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-hill-cipher/. [Accessed: 27- Feb- 2019].