UNIVERSIDAD CENTRAL DEL ECUADOR

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

CRIPTOGRAFIA Y CIBERSEGURIDAD

Integrantes: Espinosa Joel
Soria Nelson
Toscano Juan

Curso: C8 – 001

Fecha: 05/11/2024

Algoritmos de Cifrado

Cifrado de transposición

Un cifrado de transposición reorganiza el orden de las letras o símbolos en el texto plano, de acuerdo con una regla o clave fija. Por ejemplo, el cifrado de la cerca del riel divide el texto sin formato en filas y luego las lee en diagonal.

La escítala espartana es un ejemplo de transposición (las letras simplemente se cambian de sitio o se transponen, por tanto las letras son las mismas en el mensaje original y en el cifrado. En términos de pasatiempos se dice que las letras se trasponen o se anagraman). [1]

Cifrado de sustitución (Cesar)

Un cifrado de sustitución reemplaza cada letra o símbolo en el texto plano con otro, de acuerdo con una regla o clave fija. Por ejemplo, el cifrado César desplaza cada letra en un cierto número de posiciones en el alfabeto. [2]

El procedimiento que empleaba Julio César para enviar mensajes secretos a sus legiones, es uno de los algoritmos criptográficos más simples. [1]

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

En la mayoría de los casos la criptografía, en esta época, se refería exclusivamente a cifrarlos mono alfabéticos. En ellos la sustitución clave, una vez elegida, no se modifica a lo largo de toda la operación de cifrado. [1]

Cifrado de Sustitución Poli alfabético.

El cifrado Vigenère es un cifrado basado en diferentes series de caracteres o letras del cifrado César formando estos caracteres una tabla, llamada tabla de Vigenère, que se usa como clave. El cifrado de Vigenère es un cifrado poli alfabético y de sustitución. [3]

Consiste en una disposición de letras que contiene en orden los 26 alfabetos de César. Además, para proteger más el cifrado suele introducirse una palabra clave, que consiste en una palabra o texto que se repite a largo de todo el mensaje a cifrar. [1]

En términos matemáticos, puede expresarse la función de cifrado como:

$$E(X_i) = (X_i + K_i) mod\ L$$

Donde (X_i) es la letra en la posición i del texto a cifrar, (K_i) es el carácter de la clave correspondiente a (X_i) , pues se encuentran en la misma posición, y

L es el tamaño del alfabeto. En este caso L=27. [3]

Matrices Alfabéticas.

El proceso para descifrar un mensaje cifrado por sustitución mono alfabética se basa en el uso de la tabla de frecuencias correspondiente a cada idioma, combinado con el análisis de frecuencias del mensaje; sin embargo, en mensajes cortos las frecuencias pueden no corresponder a las previstas en la tabla de frecuencias, por tal razón se propone un método para descifrar mensajes en español, cifrados mediante sustitución mono alfabética, en el cual se diferencian los caracteres cifrados que corresponden a vocales y consonantes. [4]

La efectividad del análisis de frecuencias radica en que distintas letras no aparecen con la misma frecuencia en un mensaje, esto hace que algunas de ellas destaquen por su abundancia, por ejemplo las letras e, a, y otras por su escasez como es el caso de k y x; en el caso de un mensaje en español. [4]

Máquinas de Cifrado.

La máquina Enigma es uno de los ejemplos más célebres de cifrado poli alfabético. Diseñada por Arthur Scherbius, utilizaba rotores y un tablero de conexiones para cambiar las configuraciones de sustitución, haciendo que cada mensaje fuera único y difícil de descifrar sin conocer la configuración precisa de los rotores.

En la Segunda Guerra Mundial se construyó por parte alemana la famosa máquina Enigma, que se basaba en un perfeccionamiento del cilindro de Jefferson. La máquina británica Colossus diseñada por matemáticos ingleses, dirigidos por Alan Turing, logró desenmascarar las claves de Enigma. [1]

Enigma era muy similar a una máquina de escribir, salvo por que se alimentaba de una batería y no empleaba papel. Sus mensajes codificados se transmitían en código morse para ser descifrados por otra máquina Enigma al otro extremo de la línea. La máquina estaba formada por varias partes; un teclado de 26 caracteres, un clavijero interno o panel Stecker

con 6 pares de conexiones cableadas que podían conmutarse, un panel luminoso con 26 caracteres, varios rotores o modificadores (dependiendo de la versión de la Enigma), cada uno de los cuales contenía 26 muescas perimetrales con las 26 letras de alfabeto, y el reflector que devolvía el impulso eléctrico hacia los rotores una vez la señal había sido codificada. [5]

Bibliografía

[1] S. Fernández, “LA CRIPTOGRAFÍA CLÁSICA”, *Cloudfront.net*. [En línea]. Disponible en: https://d1wqtxts1xzle7.cloudfront.net/38520592/9_Criptografia_clasica-libre.pdf?1440040591=&response-content-disposition=inline%3B+filename%3DLA_CRIPTOGRAFIA_CLASICA.pdf&Expires=1730827466&Signature=ELCdcZ~hEGUBw22x-fnHNroCaQZLhw2RQZko5YwP9DnscXjSaXy3o-~KkbqbdqDlZb606B6-2qtwOCAwOd1wVeWfy0fhfW9dTsG8IP8CQczJ4dnUWdQizELPlwSo2hytyux3uErlXO-4dJGTeVG-oamqmL2TNuQw8Q-RXbfdkagg4s803Lub-W4V1lGsMB32GArtk1B6xRxNxm17lwhT7SdOZDCYZrcQW7iU5A0GMOfPqiMSvtAyJi0xy-syk4EP0jIyYJYRot2GaJkVJ1UX3Z~pUKuTiMMu7zYPS4EfNeUL882wEwycaajIWKlEpNoz2lGRPtaEK6Hvfh9vHZUbcA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. [Consultado: 05-nov-2024].

[2] COMSEC, “¿Cómo se prueba la fuerza y seguridad de un cifrado de sustitución o transposición?”, Linkedin.com, 09-mar-2023. [En línea]. Disponible en: https://www.linkedin.com/advice/1/how-do-you-test-strength-security-substitution-transposition?lang=es&originalSubdomain=es. [Consultado: 05-nov-2024].

[3] “El cifrado de Vigenère”, Ugr.es. [En línea]. Disponible en: https://www.ugr.es/~anillos/textos/pdf/2011/EXPO-1.Criptografia/02a11.htm.

[4] [Consultado: 05-nov-2024].

[5] J. G. Triana Laverde y J. M. Ruiz Vera. “Ataque matricial a cifrados de sustituci´on monoalfab´etica”. Accedido el 5 de noviembre de 2024. [En línea]. Disponible: https://www.researchgate.net/profile/Juan-Triana-6/publication/296063959_Ataque_matricial_a_cifrados_de_sustitucion_monoalfabetica/links/56d2428e08ae059e375fa033/Ataque-matricial-a-cifrados-de-sustitucion-monoalfabetica.pdf

J. M. Sánchez Muñoz, *Descifrando Enigma. La Epopeya polaca, vol. 34, Lecturas Matamaticas*. Madrid: Univ. Politec. Madr., 2013.