Ingeniería en Computación e Informática
Asignatura: *Seguridad Informática*
Docente*: Mg. Miguel Trigo Zapata*
Ingeniero Informático, postítulo en Seguridad de la Información & Ciberseguridad

Unidad III

Seguridad Informática
Departamento de Ingeniería en Computación e Informática
2023

Temas:

- Cifrador de PlayFair
- Cifrador de Hill
- Cifradores por transposición
- Transposición por grupos
- Transposición por series
- Transposición por columnas
- Transposición por filas
- Transposición por series
- Transposición por columnas
- Transposición por filas

Ingeniería en Computación e Informática
Asignatura: *Seguridad Informática*
Docente*: Mg. Miguel Trigo Zapata*
Ingeniero Informático, postítulo en Seguridad de la Información & Ciberseguridad

Cifrador de PlayFair

El cifrado de Playfair es un cifrado de sustitución polialfabético que utiliza una matriz de clave para cifrar pares de letras en un texto claro.

P L A Y F
I R B C D
E G H K M
N O Q S T
U V W X Z

En el esquema simple, se considera un cifrado básico del proceso de cifrado de Playfair, este comienza con una clave, por ejemplo, "PLAYFAIR". Elimina las letras duplicadas y luego completa la matriz (generalmente 5x5) con el alfabeto restante, excluyendo las letras de la clave, de esta manera la clave se utiliza para rellenar la matriz de izquierda a derecha y de arriba a abajo.

Aunque el cifrado de Playfair fue diseñado originalmente para el cifrado manual de mensajes, su uso en la seguridad informática es limitado, por su vulnerabilidad frente a métodos más avanzados. Sin embargo, aún se puede utilizar en ciertos contextos donde la seguridad no es una preocupación muy crítica, algunos ejemplos de su utilización podrían ser las siguientes:

Uso de claves básicas:
Al igual que en el cifrado de Playfair, en la seguridad informática, es crucial utilizar claves robustas y seguras. Las claves fuertes ayudan a aumentar la resistencia del sistema contra ataques.

Matrices y Transformaciones:
El concepto de utilizar matrices y transformaciones para cifrar datos puede inspirar métodos más avanzados en seguridad informática. Por ejemplo, las transformaciones lineales en matrices son fundamentales en algoritmos modernos de cifrado, como AES (Advanced Encryption Standard).

Protección contra Ataques de Frecuencia:
Aunque el cifrado de Playfair no es inmune a todos los tipos de ataques, su capacidad para dificultar los ataques de frecuencia puede recordarnos la importancia de diversificar los métodos de cifrado para evitar patrones predecibles.

Sustitución Polialfabética:
La idea de utilizar sustituciones polialfabéticas (cifrados que utilizan múltiples alfabetos) es esencial en la criptografía moderna. Algoritmos como el cifrado de Vigenère y otros cifrados de flujo aprovechan esta técnica.

Ejemplo, se trabajará con la palabra MTRIGO:

M T R I
G O A B
C D E F
H K L N

Agruparemos las letras en pares, aplicando reglas para manejar letras duplicadas o palabras con letras repetidas, en este caso, agregamos una letra ficticia ('X') entre las letras repetidas:

MTRIGO -> MT RX IG OX

Cifrado en pares de letras, aplicando las reglas de cifrado para cada par de letras.

MT -> FG
RX -> LO
IG -> EH
OX -> UN

Resultado obtenido, como la palabra "MTRIGO" fue escogida en esta ocasión al utilizar el método de cifrado de Playfair, la matriz de clave proporcionada sería: "FGLOEHUN".

La expresión sería *C=Cifrar(P, Matriz de Clave)*

$$K = \begin{bmatrix} M & T & R & I \\ G & O & A & B \\ C & D & E & F \\ H & K & L & N \end{bmatrix}$$

$$P = \begin{bmatrix} M & T \\ R & I \\ G & O \end{bmatrix}$$

Aunque el cifrado de Playfair fue innovador en su época, la seguridad informática ha avanzado significativamente. Hoy en día, se prefieren algoritmos criptográficos más robustos y seguros, como AES, RSA, y ECC (Elliptic Curve Cryptography), que ofrecen una mayor resistencia a diversos ataques.

Cifrador de Hill

Este opera sobre bloques de texto plano representados como vectores y utiliza una matriz cuadrada como clave de cifrado, la clave determina la transformación lineal aplicada al bloque de texto. La fortaleza del cifrado radica en la dificultad de invertir la transformación sin conocer la matriz clave. El texto claro se divide en bloques, cada uno representado como un vector. Se elige una matriz cuadrada como clave de cifrado. La dimensión de la matriz debe ser compatible con el tamaño de los bloques.

Cada bloque se multiplica por la matriz clave utilizando aritmética modular para evitar desbordamientos (Operación Matricial). El resultado de la operación matricial constituye el bloque cifrado y para descifrar, se debe calcular la inversa de la matriz clave.

Cifrado:

Divide el texto claro en bloques de tamaño $\boldsymbol{n}$ (la dimensión de la matriz clave).

$$P = \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix}$$

Matriz Clave:

Elige una matriz cuadrada clave $\boldsymbol{K}$ de tamaño $\boldsymbol{n \times n}$.

$$K = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n2} & \dots & k_{nn} \end{bmatrix}$$

Operación de Cifrado:

Calcular el bloque cifrado $\boldsymbol{C}$ utilizando la multiplicación matricial:

$$\boldsymbol{C = K \cdot P}$$

Descifrado:

Inversa de la Matriz Clave:

$$\boldsymbol{k^{-1}}$$

Entonces se comprende, de esta manera:

Cifrado:

Representación del Texto Claro: P = [9, 7]
Matriz Clave: K = [[6, 24], [13, 16]]
Operación de Cifrado: C = K * P = [258, 233]

Descifrado:

Inversa de la Matriz Clave: K^-1 = (1/144)[[16, -24], [-13, 6]]
Operación de Descifrado: P' = K^-1 * C = [9, 7]

Comprendiendo lo anterior realizaremos la encriptación con la palabra **MTRIGO**

Matriz Clave:

$$K = \begin{bmatrix} 6 & 24 \\ 13 & 16 \end{bmatrix}$$

Texto Claro:

$$P = \begin{bmatrix} 12 \\ 19 \end{bmatrix}$$ (Correspondiente a las letras "MTRIGO" en el alfabeto, A=0, B=1, ..., Z=25)

Operación de Cifrado:

$$C = K \cdot P$$

$$C = \begin{bmatrix} 6 & 24 \\ 13 & 16 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 19 \end{bmatrix} = \begin{bmatrix} 258 \\ 233 \end{bmatrix}$$

Resultado del cifrado, que en la palabra "**MTRIGO**" cifrada con el Cifrador de Hill es "**FGLOEHUN**", que coincide con el resultado del cifrado de Playfair en nuestro ejercicio anterior, dando como presentación que este es un ejemplo de cómo se vería el mismo texto claro cifrado utilizando el Cifrador de Hill donde ambos cifradores utilizan principios matriciales, pero sus enfoques y operaciones específicas difieren.

En los algoritmos de cifras conocidos como "monoalfabéticas" se cambian las letras del mensaje usando un único alfabeto de cifrado y sí, se usan dos o más alfabetos, hablaríamos de algoritmos que se usan "polialfabética". Es relevante señalar que el alfabeto de cifrado, no puede o no albergar los mismos elementos que el alfabeto del texto.

Una alternativa adicional de esta modalidad de operaciones es la utilización de operaciones "monográmicas", específicamente, el mensaje mediante un grupo de letras del mismo, los algoritmos de sustitución "monoalfabética" son más conocidos como algoritmo del César, el cifrado de Playfair y las matrices de Hill por lo general, son los algoritmos clásicos de cifrado y se utilizaban el mismo alfabeto del texto.

El método que se seguía era el de asignar a cada letra del alfabeto un número (A → 0, B → 1, C → 2…), dando además, no se solía tener en cuenta el carácter del espacio en blanco, ya que esto entregaría una información muy valiosa a cualquier criptoanalista que intente romper el sistema de cifrado. Todo esto, sin duda, solo tiene sentido en los sistemas de cifra clásicos, ya que el cifrado moderno se basa en los bits y, por consiguiente, en ese caso sí se cifran todos los caracteres, incluidos los espacios en blanco y todos los caracteres no imprimibles de un documento.

Podemos utilizar Python con la librería de NumPy para operaciones matriciales y álgebra lineal. Por ejemplo, para el cifrado de Hill

```
import numpy as np

# Definir la matriz clave y el vector de texto claro
K = np.array([[6, 24], [13, 16]])
P = np.array([12, 19])

# Operación de cifrado
C = np.dot(K, P)

# Resultado del cifrado
print(C)
```

Cifradores por transposición

Un cifrador por transposición es un tipo de cifrado que opera mediante la reorganización de los caracteres en el texto claro sin alterar los caracteres mismos en lugar de cambiar las letras, como en los cifradores de sustitución, los cifradores por transposición reorganizan la disposición de los caracteres para ocultar el mensaje original estos cifradores son especialmente efectivos cuando se utilizan junto con otros métodos de cifrado.

Ingeniería en Computación e Informática
Asignatura: *Seguridad Informática*
Docente*: Mg. Miguel Trigo Zapata*
Ingeniero Informático, postítulo en Seguridad de la Información & Ciberseguridad

Ejercicio Práctico
Taller – N.°1

Supongamos que eres el ingeniero de seguridad en una empresa de desarrollo de software que está implementando un sistema de comunicación segura para una red interna, en esta empresa se necesita transmitir información confidencial entre diferentes equipos de manera segura donde se han seleccionado dos cifradores para este propósito; El Cifrador de Playfair y el Cifrador de Hill, la empresa está en búsqueda de cumplir las normas dictadas por el gobierno de Chile, el cual es aplicar la **nueva política nacional de ciberseguridad** y quiere iniciar con el propósito de "no más papeles", en donde las firmas digitales es la prioridad y estas se deben cumplir requisitos básicos como:

Resguardar la integridad de la información, cumplir con protección autorizada, mantenerse siempre activa y chequear su integridad desde que el documento se realizó, mostrando siempre cada autor que modifico el documento y si esta sufrió alguna alteración/modificación.

Como tú conoces sobre estos tipos de cifrados, sugieres solo ocupar un modelo, ya sea el cifrado de Playfair o el cifrador de Hill, porque sabes que este modelo no cumplirá al 100% lo que se busca.

La contraseña seccionada es; "**Lo diré en clases**", se debe explicar cómo se puede encriptar por medio del uso de la matriz, también se deberá crear una guía simple de cómo es posible que este cifrado es vulnerable y como endurecer este cifrado.

Objetivo adicional:

- Proporciona el mensaje cifrado y comparte la matriz de clave con un compañero de otro grupo para el otro equipo puede descifrarlo y genere un reporte del método, tiempo y análisis que utilizaron para descifrarlo.
- Propone otro medio de encriptación que sea más moderno, incluyendo un framework que ayude a cumplir lo que la empresa desea.
- Crea de manera simple la importancia del framework seleccionado que ayudara a cumplir lo que busca esta empresa apegándose a los 5 objetivos estratégicos de ciberseguridad, ***Infraestructura resiliente, Derechos de las personas, Cultura de ciberseguridad, Coordinación nacional e internacional y Fomento a la industria y la investigación científica***

Elaboren un póster que permita comunicar de forma breve y precisa. Las Infografías / pósteres tienen la finalidad de comunicar algo en solo un par de minutos. Ustedes deberán hacer un póster con su idea y explicarlo. El póster / infografía debe tener, al menos, los siguientes elementos.

- Título y autores.
- Problema/oportunidad.
- Objetivo.
- Solución propuesta.
- Metodología propuesta.
- Referencias e impacto.

Entrega el 23 de noviembre – 2023, Nota pondera de un 50% En Taller N.°1

Referencia Bibliográficas

https://digital.gob.cl. (n.d.). Regulación. Regulación. Retrieved November 16, 2023, from https://digital.gob.cl/biblioteca/regulacion/ley-19799-sobre-documentos-electronicos-firma-electronica-y-servicios-de-certificacion-de-dicha-firma/

Nacional, B. del C. (n.d.). Biblioteca del Congreso Nacional | Ley Chile. Www.bcn.cl/Leychile. Retrieved November 16, 2023, from https://www.bcn.cl/leychile/navegar?idNorma=&idVersion=&idLey=&tipoVersion=&cve=&i=196640

(2023). Worldcat.org. https://tarapaca.on.worldcat.org/search/detail/8081159865?queryString=CRIPTOGRAF%C3%8DA%20SIM%C3%89TRICA%20Y%20ASIM%C3%89TRICA&stickyFacetsChecked=false&clusterResults=true&groupVariantRecords=false

Armando, C. (2007). Pki* y firmas digitales: aplicaciones reales, 2(3), 13–26. https://doi.org/10.26620/uniminuto.inventum.2.3.2007.13-26

Shab, E. N., Ali, A., Vanessa, M. N., & Miguel, J. H. B. (2022). Learning the basics of cryptography with practical examples, 11(24), 274–281. https://doi.org/10.30827/Digibug.74740