Universidad Central del Ecuador

Informe Técnico sobre Técnicas de Cifrado

- **Hurtado Alexis**
- **Quinatoa John**
- **Rodríguez Gabriela**
- **Vergara Dario**

Ejercicio 1 - Generación de Anagramas (Permutaciones) en Criptografía

Concepto Base

La generación de anagramas implica calcular todas las permutaciones posibles de un conjunto de caracteres. Computacionalmente, esto se resuelve con algoritmos recursivos o heurísticas de back tracking [4]. Su complejidad factorial ($O(n!)$) lo hace útil en criptografía para espacios de claves pequeños [1].

Objetivo Criptográfico

Las permutaciones se aplican en:

1. **Cifrados por transposición**: Reordenamiento de bloques en sistemas como el *rail fence cipher* [2].
2. **Generación de claves combinatorias**: Uso en esquemas de autenticación de un solo uso (OTP) [3].
3. **Refuerzo de entropía**: Como etapa previa en funciones hash [1].

Fortalezas y Debilidades

Aspecto	Descripción	Referencia
Implementación	Eficiente para $n \leq 7$ con recursión.	[4]
Seguridad	Vulnerable a ataques de fuerza bruta si n es pequeño ($n < 8$).	[1], [3]
Uso en criptografía	Componente en sistemas híbridos (ej. cifrado Feistel con permutaciones).	[2]

Ejercicio 2 - Cifrado por Permutación de Filas

Concepto base:
El cifrado por permutación de filas es una técnica de transposición sencilla en la cual el texto plano (sin espacios) se escribe fila por fila en una matriz de tamaño n×n, y el texto cifrado se obtiene leyendo la matriz columna por columna. [5]

Objetivo criptográfico:
Ofrecer confidencialidad mediante la reordenación de posiciones de los caracteres, dificultando la reconstrucción directa del mensaje original. [5]

Fortalezas/debilidades:

- Fortaleza: Implementación simple y de bajo costo computacional.
- Debilidad: Susceptible a análisis de frecuencia y ataques de transposición si se conoce el tamaño de la matriz. [5]

Ejercicio 3 - Cifrado por Permutación de Columnas

Concepto base:
El cifrado por permutación de columnas es otra forma de transposición donde el texto plano (sin espacios) se coloca columna por columna en una matriz de tamaño n×n, y el texto cifrado se genera leyendo la matriz fila por fila. [6]

Objetivo criptográfico:
Garantizar la confidencialidad alterando el orden lineal del texto, distribuyendo los caracteres en una estructura matricial para ocultar el patrón original. [6]

Fortalezas/debilidades:

- Fortaleza: Aumenta la confusión al dispersar caracteres en columnas.
- Debilidad: De igual manera vulnerable a ataques de transposición y requiere gestión segura de la clave n. [6]

Ejercicio 4 – Cifrado de Cesar

Concepto Base

El cifrado César es una técnica criptográfica histórica y simple que pertenece a la familia de cifrados por sustitución monoalfabética. Consiste en desplazar cada letra del texto original (texto plano) un número fijo de posiciones en el alfabeto. Por ejemplo, con un desplazamiento de 3, la letra "A" se cifraría como "D", "B" como "E", y así sucesivamente. Su nombre honra a Julio César, quien lo utilizó para comunicaciones militares secretas en la antigua Roma [7].

Objetivo Criptográfico

Su propósito principal es garantizar la confidencialidad de un mensaje mediante la ocultación de su contenido legible. Al transformar el texto plano en un formato ininteligible sin conocer el desplazamiento aplicado, solo el receptor con la clave correcta (el número de desplazamiento) puede descifrarlo. Aunque rudimentario, fue diseñado para proteger información sensible en contextos de baja complejidad tecnológica [8].

Fortalezas y Debilidades

Fortalezas: Es fácil de implementar, requiere pocos recursos computacionales y es útil para introducir conceptos básicos de criptografía.

Debilidades: Extremadamente vulnerable a ataques de fuerza bruta (solo 25 combinaciones posibles en inglés) y al análisis de frecuencias debido a su estructura predecible [7][8].

Ejercicio 5 -Método de sustitución Poli alfabético de Vigenère

Concepto Base

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.

Objetivo Criptográfico

Este método nos sirve para cifrar y descifrar mensajes de texto utilizando una tabla de sustitución (tabla o la tabla de Vigenère) y una palabra clave.

Cuadrado o la tabla de Vigenère [10]

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

Fortalezas y Debilidades

Ventajas del cifrado Vigenère

El cifrado Vigenère es resistente al análisis de frecuencia, lo que lo hace más seguro que métodos simples como el cifrado César.
Utiliza múltiples alfabetos de sustitución, aumentando la complejidad y dificultando el descifrado sin la palabra clave. [9]

Vulnerabilidades del cifrado Vigenère

Su principal debilidad es la dependencia de una palabra clave, que, si se descubre, compromete todo el mensaje cifrado. Aunque resiste el análisis de frecuencia, técnicas como el método de Kasiski pueden romperlo al revelar patrones repetitivos. [9]

Ejercicio 6 – Cifrado de Polibio

Concepto Base

El cifrado de Polibio es uno de los métodos criptográficos más antiguos, desarrollado por el historiador griego Polibio en el siglo II a.C. Consiste en sustituir cada letra del alfabeto por un par de coordenadas (fila y columna) dentro de una matriz cuadrada de 5×5. Originalmente, se usó para transmitir mensajes mediante señales ópticas (antorchas) o acústicas (tambores), representando cada letra con dos símbolos. En alfabetos con más de 25 letras (como el español), se suelen fusionar caracteres (ejemplo: "I" y "J" comparten celda) para adaptarse al sistema [11][12].

Objetivo Criptográfico

Su finalidad principal era garantizar la confidencialidad en comunicaciones militares y secretas, permitiendo codificar mensajes en un formato no legible sin conocimiento de la matriz. Además, facilitaba la transmisión a distancia mediante códigos visuales o sonoros, donde cada par de coordenadas podía representarse con señales (ejemplo: dos antorchas para indicar "B3"). Históricamente, fue empleado por los nihilistas rusos en el siglo XIX para comunicaciones clandestinas [11].

Fortalezas y Debilidades

Fortalezas: Simpleza de implementación, útil para enseñar criptografía básica y adaptable a sistemas de señalización no textual.

Debilidades: Vulnerable al análisis de frecuencias (al ser una sustitución monoalfabética) y a ataques por fuerza bruta debido a su estructura predecible [12].

Bibliografía:

[1] A. Menezes et al., Handbook of Applied Cryptography. CRC Press, 1996. DOI: 10.1201/9781439821916 (Libro completo en Taylor & Francis).
[2] J. Pieprzyk et al., *Fundamentals of Computer Security*. Springer, 2003. DOI: 10.1007/978-3-662-07324-7.
[3] S. Even and O. Goldreich, "On the Power of Cascade Ciphers," *IEEE Trans. Inf. Theory*, vol. 29, no. 4, pp. 121–126, Jul. 1983. DOI: 10.1109/TIT.1983.1056719 *(Artículo en IEEE Xplore)*.
[4] R. Sedgewick and K. Wayne, *Algorithms, 4th Edition*. Addison-Wesley, 2011. Sitio oficial *(Incluye código y ejemplos)*.
[5] D. R. Stinson, *Cryptography: Theory and Practice*, 3rd ed., CRC Press, Boca Raton, FL, USA, 2006.
[6] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson Education, Boston, MA, USA, 2017.

[7] Ayuda Ley Protección Datos, "¿Qué es el cifrado César y cómo funciona?", 2020. [En línea]. Disponible: https://ayudaleyprotecciondatos.es/2020/06/10/cifrado-cesar/.

[8] Universidad de Granada, "El cifrado de César". [En línea]. Disponible: https://www.ugr.es/~anillos/textos/pdf/2010/EXPO-1.Criptografia/02a04.htm.

[9] Coded Insights, "Strengths and Weaknesses of the Vigenère Cipher," *Coded Insights*. [Enlace]. Disponible en: https://codedinsights.com/classical-cryptography/vigenere-cipher/#strengthsandweaknessesofthevigenrecipher.

[10] Universidad de Granada, "Criptografía clásica: El cifrado Vigenère," *Anillos*. [Enlace]. Disponible en: https://www.ugr.es/~anillos/textos/pdf/2011/EXPO-1.Criptografia/02a11.htm.

[11] Museo Inf. UPValencia, "Cifrado de Polibio", 2021. [En línea]. Disponible: https://museo.inf.upv.es/blog/2021/05/14/cifrado-de-polibio/.

[12] EncDesarrollo, "Cifrado de Polybios", 2012. [En línea]. Disponible: https://encdesarrollo.wordpress.com/2012/10/09/cifrado-de-polybios/.