

**Trabajo de Investigación**

**Grupo 10:**

Hernández Vivanco, Carlos Alberto U19211936

Manrique Benites, Michael Francois U18100659

Ramos Verano, Wilmer Alexander U21222740

Sánchez Valderrama Jordy Anthony U19219159

Santivañez Guevara, Axel Samuel U20237224

**Universidad Tecnológica del Perú**

**35548:** Criptografía I

Carrasco García, Ricardo Jesús

11 de diciembre del 2023

**Índice de Contenido**

[Índice de Imágenes 3](#_Toc153176629)

[1. Introducción 4](#_Toc153176630)

[2. Historia 5](#_Toc153176631)

[3. Cifradores 6](#_Toc153176632)

[3.1. Cifrado Afin 6](#_Toc153176633)

[3.2. Cifrado Autoclave 7](#_Toc153176634)

[3.3. Cifrado Beaufort 8](#_Toc153176635)

[3.4. Cifrado Cesar 9](#_Toc153176636)

[3.5. Cifrado de Playfair 10](#_Toc153176637)

[3.6. Cifrado de Polybios 10](#_Toc153176638)

[3.7. Cifrado de Transposición Grupos 11](#_Toc153176639)

[3.8. Cifrado de Transposición Simple 11](#_Toc153176640)

[3.9. Cifrado de Vernam 12](#_Toc153176641)

[3.10. Cifrado Vigenere 13](#_Toc153176642)

[4. Conclusión 14](#_Toc153176643)

Índice de Imágenes

[Imagen 1 – Cifrado Afín 6](#_Toc153176648)

[Imagen 2 – Cifrado Beaufort 8](#_Toc153176649)

[Imagen 3 – Cifrado Cesar 9](#_Toc153176650)

[Imagen 4 – Cifrado Vigenere 13](#_Toc153176651)

1. Introducción

En la era moderna, donde la información fluye constantemente a través de redes digitales, la necesidad de proteger nuestra privacidad y asegurar la integridad de la información se ha vuelto más crucial que nunca. En este contexto, la criptografía emerge como una herramienta fundamental para salvaguardar la confidencialidad y la autenticidad de la información en el vasto y complejo mundo digital. Sin embargo, el alcance y la complejidad de la criptografía han evolucionado enormemente en la era digital. En la actualidad, abarca desde algoritmos matemáticos avanzados hasta protocolos de seguridad que son fundamentales para el funcionamiento de transacciones financieras, comunicaciones gubernamentales y la protección de datos personales.

La criptografía desempeña un papel vital en la seguridad digital al proporcionar mecanismos para garantizar la confidencialidad de la información. En su forma más básica, implica el uso de algoritmos y claves para cifrar datos, transformándolos en un formato ilegible para aquellos que no poseen la clave de descifrado correspondiente. A medida que la tecnología avanza, también lo hacen los desafíos para la criptografía. La llegada de computadoras cuánticas y la creciente sofisticación de los ciberataques plantean nuevas amenazas para los métodos criptográficos tradicionales. Es en este contexto que los criptógrafos y expertos en seguridad digital están trabajando arduamente para desarrollar soluciones innovadoras que puedan resistir los desafíos del futuro.

La criptografía cuántica, por ejemplo, se presenta como una posible respuesta a las amenazas que plantean las computadoras cuánticas. Estas máquinas tienen el potencial de desentrañar algoritmos criptográficos convencionales, pero la criptografía cuántica utiliza principios de la mecánica cuántica para ofrecer una seguridad aún más robusta.

1. Historia

Los primeros registros de la criptografía se remontan a la antigüedad, donde las civilizaciones egipcias y mesopotámicas ya utilizaban jeroglíficos y símbolos para transmitir mensajes secretos. Sin embargo, el primer sistema de cifrado documentado fue desarrollado por los antiguos espartanos alrededor del siglo V a.C. La "escítala espartana" consistía en un bastón alrededor del cual se enrollaba un pergamino con el mensaje. Solo aquellos que tenían un bastón de diámetro específico podían descifrar el mensaje correctamente al desenrollarlo. Este método temprano ilustra la premisa fundamental de la criptografía: la necesidad de una clave para entender el mensaje.

Durante la Roma antigua, Julio César se destacó por utilizar un cifrado simple pero efectivo conocido como el "Cifrado César". Este método consistía en desplazar cada letra del alfabeto por un número fijo, siendo el caso más conocido el desplazamiento de tres lugares. Este cifrado puede parecer rudimentario hoy en día, pero en su tiempo, proporcionaba cierta seguridad contra los enemigos que no conocían el desplazamiento. Siglos después, en el Renacimiento, Blaise de Vigenère desarrolló un cifrado más complejo conocido como el "Cifrado Vigenère". A diferencia del Cifrado César, el Vigenère utilizaba una clave que cambiaba a lo largo del mensaje, lo que lo hacía más resistente a los métodos de ataque de la época.

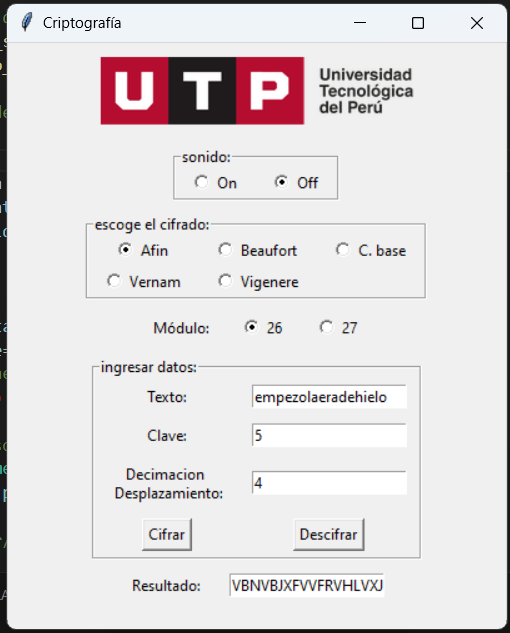
El siglo XX vio un salto significativo en la complejidad de la criptografía con la invención de la máquina Enigma por parte de los alemanes. Durante la Segunda Guerra Mundial, Enigma se convirtió en el símbolo de la criptografía militar y una herramienta formidable para los alemanes. Sin embargo, gracias a los esfuerzos de los criptoanalistas aliados, incluidos genios como Alan Turing, la Enigma fue finalmente descifrada. Este período marcó el comienzo de una nueva era en la criptografía, donde la tecnología y las habilidades matemáticas avanzadas desempeñaron un papel crucial en la guerra de la información.

Con el advenimiento de la computación en la segunda mitad del siglo XX, la criptografía dio un salto revolucionario. La criptografía de clave pública, propuesta por Whitfield Diffie y Martin Hellman en la década de 1970, permitió un intercambio seguro de claves a través de canales inseguros. Esto allanó el camino para la creación del algoritmo de cifrado RSA, que sigue siendo un pilar de la seguridad digital hoy en día.

La criptografía cuántica, una rama emergente, utiliza principios cuánticos para garantizar la seguridad en un mundo donde las computadoras cuánticas podrían amenazar los métodos convencionales.

1. Cifradores
   1. Cifrado Afín

El cifrado afín es un método de cifrado clásico que pertenece a la categoría de cifrados lineales. Se basa en una función matemática lineal de la forma E(x)=(ax+b)modm, donde a y b son enteros, m es el tamaño del alfabeto, y x representa el valor numérico asociado a una letra en el mensaje original. En el contexto del cifrado afín, el mensaje se divide en bloques, y cada bloque se cifra por separado aplicando la función lineal. En el caso de un alfabeto de m letras, cada letra del mensaje original es representada por un número entre 0 y m−1. La función de cifrado transforma este número según la ecuación mencionada anteriormente. El cifrado afín es una extensión del cifrado de César, donde a sería igual a 1 y b sería el desplazamiento. La ventaja del cifrado afín es que ofrece más posibilidades de combinaciones, ya que hay múltiples valores posibles para a y b. Sin embargo, también es vulnerable a ciertos tipos de ataques, como el análisis de frecuencia. Para que el cifrado afín sea seguro, es crucial elegir valores adecuados para a y b. Además, es importante que a sea coprimo con m para garantizar que la función de cifrado sea reversible.



1. Cifrado Afín
   1. Cifrado Autoclave

El cifrado autoclave es un método de cifrado que implica el uso de dos o más alfabetos diferentes para codificar un mensaje. Se utiliza un alfabeto principal y uno o varios alfabetos secundarios para realizar la sustitución de letras. La idea es alternar entre estos alfabetos secundarios de manera preestablecida para aumentar la complejidad y seguridad del cifrado.

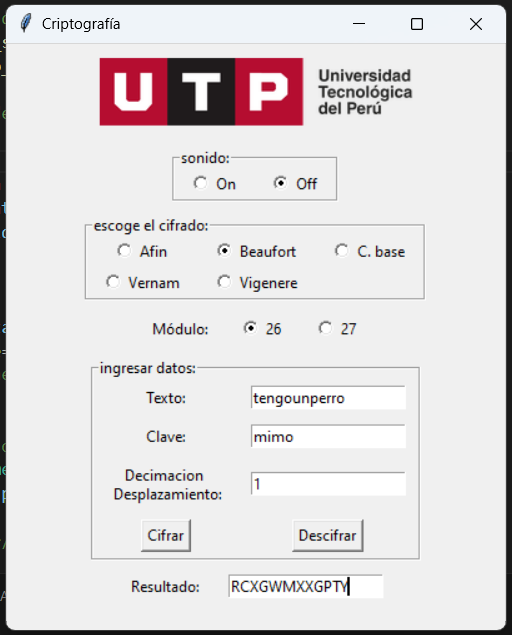
En este sistema, el mensaje original se divide en grupos de letras del mismo tamaño que la clave. Luego, se aplica la sustitución mediante la combinación de los alfabetos de acuerdo con la clave para codificar cada grupo de letras.

La clave en el autoclave determina el orden en el que se utilizan los diferentes alfabetos secundarios para cifrar el mensaje. Es esencial para el proceso de cifrado y descifrado, y si la clave no se conoce, descifrar el mensaje se vuelve considerablemente más difícil.

Una de las ventajas del cifrado autoclave es su capacidad para aumentar la seguridad del mensaje al utilizar múltiples alfabetos en lugar de uno solo, lo que hace que sea más complejo de descifrar. Sin embargo, la seguridad de este método depende en gran medida de la fortaleza y el secreto de la clave utilizada.

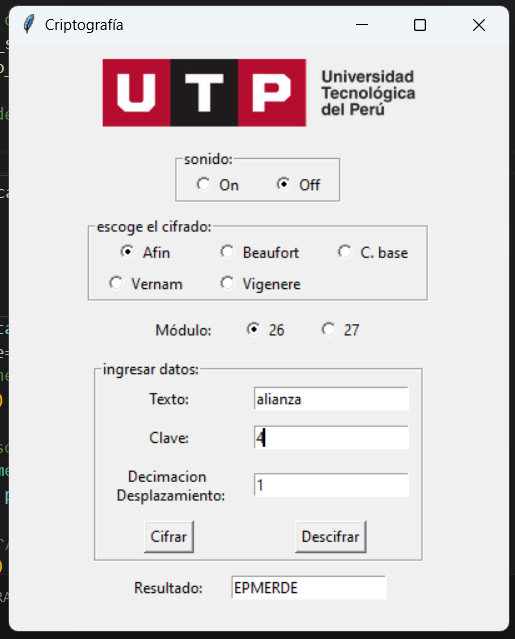
* 1. Cifrado Beaufort

El cifrado Beaufort, desarrollado por Sir Francis Beaufort alrededor de 1820, es un algoritmo criptográfico simétrico que, a diferencia del método Vigenère, emplea la resta en lugar de la suma. Al cifrar, se identifica la posición de las letras del mensaje y la clave en una tabla específica, y luego se resta la posición de la letra clave de la posición del texto plano para obtener la letra cifrada. Este método ofrece un nivel de seguridad relativo, dependiendo de la longitud y la complejidad de la clave utilizada, y se basa en operaciones de sustitución polialfabética para su funcionamiento.



1. Cifrado Beaufort
   1. Cifrado Cesar

El cifrado César es uno de los métodos de cifrado más simples y antiguos utilizados en la historia de la criptografía. Este sistema lleva el nombre de Julio César, quien se cree que lo utilizó para proteger comunicaciones militares durante sus campañas militares. La técnica del cifrado César implica desplazar cada letra de un mensaje por un número fijo de posiciones en el alfabeto. Por ejemplo, si se utiliza un desplazamiento de 3, la letra "A" se cifraría como "D", "B" como "E", y así sucesivamente. Este proceso se aplica de manera circular de modo que si el desplazamiento lleva más allá de la "Z", continúa desde la "A". Aunque el cifrado César fue eficaz en su tiempo y proporcionaba cierta seguridad contra lectores no autorizados, es extremadamente vulnerable a ataques de fuerza bruta y análisis de frecuencia. Dado que solo hay 25 posibles desplazamientos en el alfabeto latino estándar, un criptoanalista puede probar todas las combinaciones posibles para descifrar el mensaje.



1. Cifrado Cesar
   1. Cifrado de Playfair

El cifrado Playfair es un método de cifrado simétrico que utiliza una matriz de letras para cifrar pares de letras en un mensaje. Fue inventado por el criptógrafo británico Charles Wheatstone en 1854 y más tarde popularizado por su compatriota Lyon Playfair. La técnica del cifrado Playfair implica la creación de una matriz de 5x5, comúnmente llamada la "Tabla de Playfair". Esta tabla se llena con letras del alfabeto, excluyendo la letra "J" (se suele combinar con "I" en una única celda). La clave se utiliza para determinar la disposición específica de las letras en la tabla. Para cifrar un mensaje, este se divide en pares de letras. Si ambas letras de un par son iguales o están en la misma fila de la tabla, se aplican reglas específicas para modificar las letras y luego se cifran. Si las letras están en diferentes filas y columnas, se forman un rectángulo y se reemplazan por las esquinas opuestas de ese rectángulo. Aunque el cifrado Playfair fue considerado seguro en su época, hoy en día se considera relativamente débil y es vulnerable a métodos modernos de criptoanálisis.

* 1. Cifrado de Polybios

El cifrado Polybios es un método criptográfico antiguo y simple que se atribuye al historiador griego Polibio, de ahí su nombre. Este cifrado se basa en un cuadrado o rejilla conocido como la "Tabla de Polybios". La tabla tiene letras o símbolos dispuestos en filas y columnas, y se utiliza para cifrar mensajes mediante la asignación de coordenadas a cada letra. La tabla de Polybios comúnmente se organiza como un cuadrado de 5x5, utilizando el alfabeto latino. Las letras se distribuyen en el cuadrado, generalmente omitiendo la letra "J" para que haya espacio suficiente para las 26 letras del alfabeto. Las coordenadas de cada letra se determinan por la fila y la columna en la que se encuentra en la tabla. Para cifrar un mensaje, cada letra se reemplaza por sus coordenadas en la tabla. Por ejemplo, si la letra "H" está en la fila 2, columna 4, se cifra como "24". El mensaje cifrado consiste en una serie de números que representan las coordenadas de las letras en la tabla de Polybios. A pesar de su simplicidad, el cifrado Polybios no proporciona una seguridad significativa y es vulnerable a ataques de criptoanálisis, especialmente debido a su patrón predecible.

* 1. Cifrado de Transposición Grupos

El cifrado de transposición por grupos es un método criptográfico que reorganiza el orden de los caracteres del mensaje original en grupos específicos, y luego reordena estos grupos según una clave predefinida. En lugar de cambiar cada letra individualmente, este cifrado divide el mensaje en bloques o grupos de caracteres (a menudo del mismo tamaño) y luego altera el orden de estos grupos siguiendo las indicaciones de la clave. La clave puede ser un número que determine el patrón de reordenamiento de los grupos o incluso una palabra o frase que dictamine cómo se deben organizar los bloques de texto. Este método puede incrementar la seguridad del cifrado al hacer menos evidente la estructura del mensaje original y puede ser más resistente a ciertos tipos de ataques criptográficos que buscan patrones en la disposición de los caracteres. Sin embargo, su nivel de seguridad depende de la complejidad y la fortaleza de la clave utilizada, así como de la forma en que se implementa el proceso de reorganización de los grupos de caracteres.

* 1. Cifrado de Transposición Simple

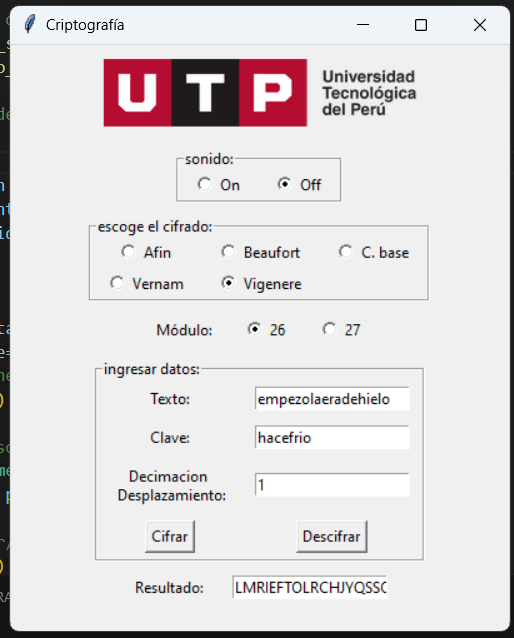
El cifrado de transposición simple es un método criptográfico que reorganiza el orden de los caracteres en un mensaje sin cambiarlos, utilizando una clave para determinar cómo se realiza esta reorganización. En lugar de sustituir caracteres como en los cifrados de sustitución, el cifrado de transposición reordena los caracteres del mensaje original. Por ejemplo, si la clave es un número, se pueden reorganizar las letras del mensaje moviéndolas un cierto número de posiciones hacia la izquierda o hacia la derecha, según la clave. Otra variante común es el uso de una palabra clave para reorganizar las letras del mensaje original basándose en el orden de las letras en la palabra clave. Aunque este tipo de cifrado puede parecer simple, su efectividad puede incrementarse mediante la repetición de la operación o mediante combinaciones con otros métodos criptográficos. Sin embargo, en su forma más básica, el cifrado de transposición simple puede ser vulnerable a análisis estadísticos o de patrones, y su seguridad depende en gran medida de la complejidad de la clave utilizada y de la implementación del método.

* 1. Cifrado de Vernam

El cifrado de Vernam, también conocido como cifrado de un solo uso o "cifrado perfecto", es un método de cifrado simétrico que se basa en el uso de una clave aleatoria del mismo tamaño que el mensaje. Desarrollado por Gilbert Vernam en 1917, este método combina cada letra del mensaje con una letra de la clave mediante una operación de suma modulo 26 (habitualmente, en el contexto del alfabeto inglés). Siendo una técnica de cifrado de flujo, cada bit o carácter del mensaje se combina con el bit correspondiente de la clave utilizando la operación XOR (o exclusiva). La clave utilizada es completamente aleatoria, y cada clave se usa solo una vez, lo que lo convierte en un sistema altamente seguro siempre que se mantenga la clave secreta. Este cifrado se considera invulnerable al análisis criptográfico, siempre y cuando se cumplan ciertas condiciones, como la generación verdaderamente aleatoria de la clave y que esta clave nunca se reutilice.

* 1. Cifrado Vigenere

El cifrado Playfair es un método de cifrado simétrico que utiliza una matriz de letras para cifrar pares de letras en un mensaje. Fue inventado por el criptógrafo británico Charles Wheatstone en 1854 y más tarde popularizado por su compatriota Lyon Playfair. La técnica del cifrado Playfair implica la creación de una matriz de 5x5, comúnmente llamada la "Tabla de Playfair". Esta tabla se llena con letras del alfabeto, excluyendo la letra "J" (se suele combinar con "I" en una única celda). La clave se utiliza para determinar la disposición específica de las letras en la tabla. Para cifrar un mensaje, este se divide en pares de letras. Si ambas letras de un par son iguales o están en la misma fila de la tabla, se aplican reglas específicas para modificar las letras y luego se cifran. Si las letras están en diferentes filas y columnas, se forman un rectángulo y se reemplazan por las esquinas opuestas de ese rectángulo. Aunque el cifrado Playfair fue considerado seguro en su época, hoy en día se considera relativamente débil y es vulnerable a métodos modernos de criptoanálisis.



1. Cifrado Vigenere
2. Conclusión

En el transcurso de este trabajo, hemos explorado la evolución de la criptografía desde sus raíces en civilizaciones antiguas hasta las complejidades de la era digital actual. La importancia de proteger la privacidad y garantizar la integridad de la información en un mundo interconectado ha llevado al desarrollo de diversas técnicas criptográficas a lo largo de la historia.

Desde los cifrados simples utilizados por Julio César hasta los algoritmos avanzados de la era digital, la criptografía ha enfrentado desafíos constantes y ha evolucionado para adaptarse a las amenazas emergentes. La introducción de la criptografía cuántica destaca la capacidad de la disciplina para innovar frente a la llegada de tecnologías disruptivas, como las computadoras cuánticas, que podrían comprometer métodos criptográficos tradicionales.

Es esencial reconocer que, si bien la criptografía desempeña un papel fundamental en la seguridad digital, no existe un enfoque único que sea invulnerable. La elección de un cifrador debe basarse en la evaluación de los requisitos de seguridad específicos y la comprensión de las vulnerabilidades potenciales.

En conclusión, la criptografía sigue siendo una herramienta esencial en la protección de la información en un mundo cada vez más digitalizado. Su continua evolución y adaptación son vitales para hacer frente a las amenazas en constante cambio, y la investigación en este campo seguirá siendo crucial para garantizar la seguridad de la información en el futuro.