UNIVERSIDAD AUTONOMA DE ZACATECAS

INGENIERÍA DE SOFTWARE

INVESTIGACIÓN: “EVOLUCIÓN HISTÓRICA DE LA CRIPTOGRAFÍA”

ALUMNO: JOSÉ LUIS REYES MAURICIO

MAESTRO: ANTONIO DE JESÚS GARCÍA DOMÍNGUEZ

MATERIA: CRIPTOGRAFÍA

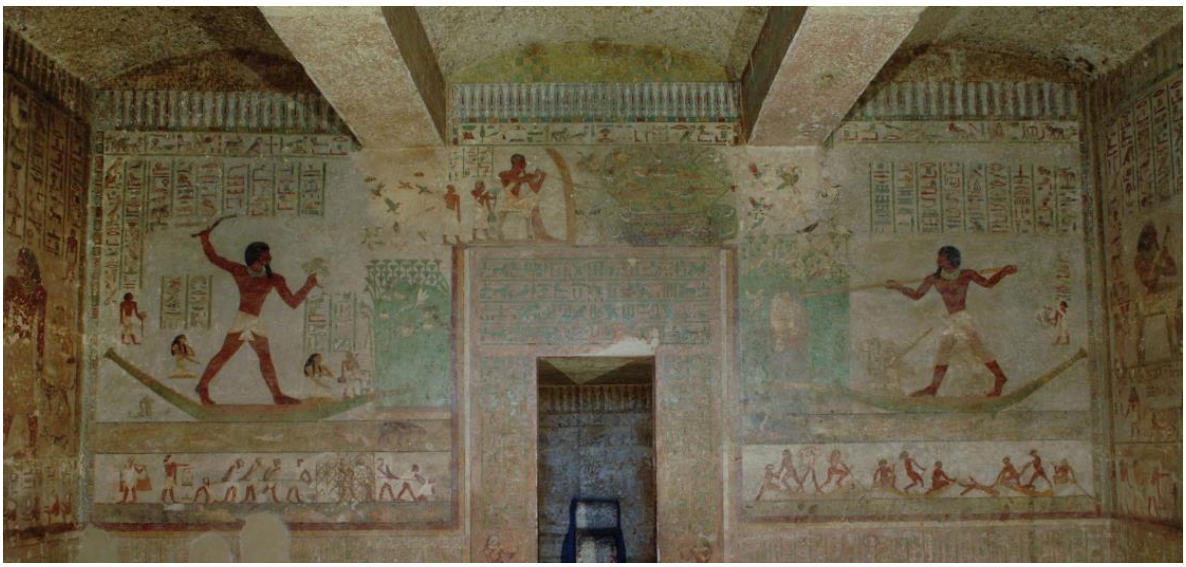
ZACATECAS, ZACATECAS

04/02/21

La criptografía es una palabra que viene del griego que significa el estudio de la ciencia que, mediante el tratamiento de la información, protege a la misma de utilización no autorizada, utilizando algoritmos matemáticos complejos para la transformación de la información en un extremo y la realización del proceso inverso en el otro.

A lo largo de la historia de la criptografía, se ha diferenciado entre: Precientífica(“Artística”), Científica (Shannon) y de clave pública (Diffie-Hellman).

El reemplazo de símbolos, la forma más básica de criptografía, se puede encontrar tanto en antiguas escrituras mesopotámicas como egipcias. El ejemplo más antiguo conocido de esta forma de criptografía se encontró en la tumba de un noble egipcio llamado Khnumhotep II, que vivió hace aproximadamente unos 3.900 años.



Tumba de Khnumhotep II

El propósito del reemplazo de símbolos en la inscripción de Knhumhotep no era ocultar información, sino incrementar su “atractivo lingüístico”. El caso más antiguo conocido de criptografía enfocada a proteger información sensible, es el de un escriba mesopotámico de hace 3.500 años que empleó la técnica para ocultar una fórmula para glaseado de cerámica en una tableta de arcilla.

En periodos posteriores de la antigüedad, la criptografía sería ampliamente utilizada para la protección de importantes informaciones militares, una función que aún hoy en día cumple. En la ciudad-estado

griega de Esparta, los mensajes se encriptaban al ser escritos en un pergamino colocado en un cilindro de una medida particular, lo que hacía que el mensaje fuera indescifrable hasta que el recipiente lo enrollaba en un cilindro similar. De forma parecida, se sabe que los espías de la antigua India empleaban mensajes codificados ya en el siglo II a.C

Escítala (Cilindro usado por los éforos espartanos)

Probablemente, la criptografía más avanzada del mundo antiguo fue la de los romanos. Un ejemplo destacado de criptografía romana, conocida como el cifrado del César.

En criptografía, el cifrado César, también conocido como cifrado por desplazamiento, código de César o desplazamiento de César, es una de las técnicas de cifrado más simples y más usadas. Es un tipo de cifrado por sustitución en el que una letra en el texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto. Por ejemplo, con un desplazamiento de 3, la A sería sustituida por la D (situada 3 lugares a la derecha de la A), la B sería reemplazada por la E, etc. Este método debe su nombre a Julio César, que lo usaba para comunicarse con sus generales.

La transformación se puede representar alineando dos alfabetos; el alfabeto cifrado es un alfabeto normal que está desplazado un número determinado de posiciones hacia la izquierda o la derecha. Por ejemplo, aquí el cifrado César está usando un desplazamiento de seis espacios hacia la derecha:

Texto original: ABCDEFGHIJKLMNÑOPQRSTUVWXYZ

Texto codificado: GHIJKLMNÑOPQRSTUVWXYZABCDEF

Para codificar un mensaje, simplemente se debe buscar cada letra de la línea del texto original y escribir la letra correspondiente en la línea codificada. Para decodificarlo se debe hacer lo contrario.

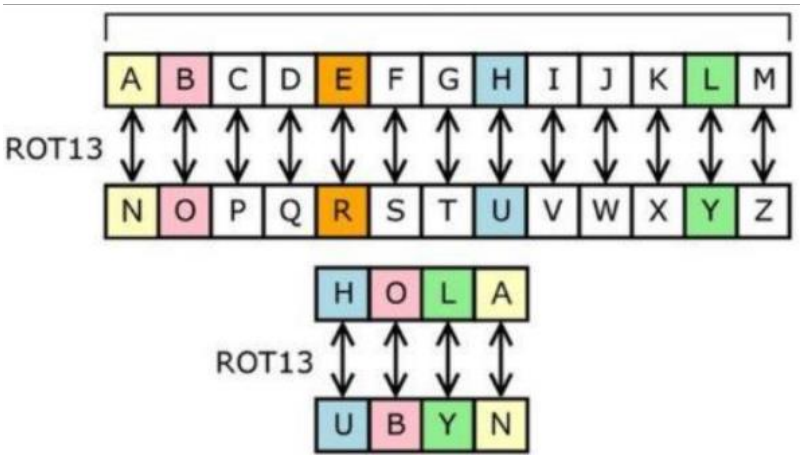
La codificación también se puede representar usando aritmética modular, transformando las letras en números, de acuerdo al esquema A = 0, B = 1,..., Z = 26.1 La codificación de la letra x con un desplazamiento n puede ser descrita matemáticamente como:

$$E_n(x) = x + n \mod 27.$$

La decodificación se hace de manera similar:

$$D_n(x) = x - n \mod 27.$$

La operación de sustitución se conserva siempre a lo largo de todo el mensaje, por lo que el cifrado se clasifica como un cifrado de tipo sustitución monoalfabética.



Al-Kindi, un célebre matemático árabe, desarrollaría en torno al 800 d.C. una técnica conocida como análisis de frecuencia, que dejaba en situación de vulnerabilidad a los cifrados por sustitución. Por primera vez, la gente que intentaba descifrar mensajes encriptados tenía a su disposición un método sistemático para lograrlo, lo que obligó a la criptografía a evolucionar para seguir siendo útil.

En 1465, Leone Alberti desarrolló el cifrado polialfabético, considerado la solución contra la técnica de análisis de frecuencia de Al-Kindi. En un cifrado polialfabético, el mensaje se codifica utilizando dos alfabetos distintos. Uno es el alfabeto en que el mensaje original se escribe, mientras el segundo es un alfabeto enteramente diferente, en el que el mensaje se muestra después de ser codificado. En combinación con los cifrados de sustitución tradicionales, los cifrados polialfabéticos incrementaban enormemente la seguridad de la información codificada. A no ser que el lector conociera el alfabeto en que el mensaje había sido originalmente escrito, el análisis de frecuencia resultaba inútil.

Nuevos métodos para codificar información serían también desarrollados durante el Renacimiento, incluyendo un temprano método popular de codificación binario inventado en 1623 por el célebre erudito Sir Francis Bacon.

Código Bacon o clave Baconiana

La ciencia criptográfica continuaría progresando en los siguientes siglos. Un notable avance en criptografía sería descrito, pero quizás nunca construido, por Thomas Jefferson en la década de 1790. Su invento, conocido como rueda de cifrado, consistía en 36 anillos de letras en ruedas móviles, que podían ser utilizados para lograr codificados complejos.

Discos de Jefferson

Este concepto era tan avanzado que serviría como base de la criptografía militar americana hasta el periodo de la Segunda Guerra Mundial.

La Segunda Guerra Mundial traería consigo el ejemplo perfecto de criptografía analógica: la máquina Enigma. Igual que la rueda de cifrado, este dispositivo, empleado por las potencias del Eje, utilizaba ruedas rotatorias para codificar un mensaje -haciendo que fuera virtualmente imposible leerlo sin otra máquina Enigma.

Tempranas formas de tecnología informática serían empleadas para eventualmente ayudar a romper el cifrado de Enigma. El exitoso desencriptado de los mensajes de Enigma aún se considera un componente crítico de la posterior victoria aliada.

Máquina Enigma

Con el auge de las computadoras, la criptografía alcanzó niveles de progreso mucho mayores que en la era analógica. La encriptación matemática de 128-bits, mucho más fuerte que cualquier cifrado antiguo o medieval, es ahora el estándar para muchos dispositivos sensibles y sistemas informáticos. En 1990, se pondría en marcha toda una nueva forma de criptografía, apodada criptografía cuántica, por parte de científicos computacionales que esperaban elevar una vez más el nivel de protección ofrecido por la encriptación moderna.

Más recientemente, técnicas criptográficas han sido también utilizadas para hacer posibles las criptomonedas. Las criptomonedas aprovechan varias técnicas criptográficas avanzadas, como las funciones hash, la criptografía de clave pública y las firmas digitales.

Estas técnicas se utilizan principalmente para garantizar la seguridad de los datos almacenados en blockchains y para autenticar las transacciones. Una forma especializada de criptografía, llamada

Elliptic Curve Digital Signature Algorithm (ECDSA), sirve de puntal a Bitcoin y a otros sistemas de criptomonedas, al proporcionar una seguridad complementaria y garantizar que los fondos sólo pueden ser utilizados por sus legítimos dueños.