CRIPTOGRAFÍA DESDE SU ORIGEN HASTA LA ACTUALIDAD

Abdelilah El Hayani, Pablo Galán, Héctor García y Mateo Pinzón

I.E.S. Mediterráneo Cartagena

Con la colaboración de:

ÍNDICE

INTRODUCCIÓN

- La criptografía se define como la ciencia que estudia la escritura oculta.

- También se entiende por criptografía al arte de escribir de forma oculta mediante el uso de códigos secretos y ha evolucionado a la vez que los avances tecnológicos.

- Hoy en día la encriptación es usada en muchos ámbitos para proteger información.

MOTIVACIONES

- Aprender sobre la criptografía.
- Su Importancia en la historia.
- Su papel en la seguridad actual.

OBJETIVOS

1. Hacer un recorrido histórico de la evolución de la criptografía.

2. Descubrir los factores que permitieron el surgimiento de la criptografía.

3. Descubrir las funciones de la criptografía actual.

METODOLOGÍA

En este trabajo se ha realizado una revisión bibliográfica, consultando páginas web y libros sobre la criptografía y la encriptación.

ORIGEN DE LA CRIPTOGRAFÍA

APARICIÓN DE LA CRIPTOGRAFÍA

Se encuentra una **tablilla** del S.XVI a.C.en la cual un **alfarero** había esculpido una **receta secreta**.

CRIPTOGRAFÍA EN DIFERENTES CULTURAS

Las más remarcables son la **egipcia**, la **mesopotámica**, **china**, la **Grecia clásica** y la **Roma clásica**.

Aparición de la criptografía

Escítala espartana
Fuente: Vavel

No fue hasta el S.VI a.C. cuando se creó el primer **sistema crptográfico**.

Estaba basado en una **escítala**, una tela alrededor un bastón, lo que hacia que se pudiese **leer** es que la persona a la que le llegase, tenía que tener el **mismo grosor** de bastón del destinatario.

Criptografía en diferentes culturas

CIVILIZACIÓN CHINA

El método utilizado por los chinos era la **esteganografía**. Esta no se considera como criptografía realmente, ya que, se basa en ocultar el contenido a través de un **canal de información**.

CIVILIZACIÓN EGIPCIA

Por parte de los egipcios sabemos que ellos fueron los que crearon los **jeroglíficos**, los cuales fueron los primeros predecesores del cifrado.

CIVILIZACIÓN MESOPOTAMICA

Los mesopotámicos intentaban **ocultar la información**.
Para ello alteraban los **símbolos cuneiformes** que escribían por otros con el fin de alterar la misma.

GRECIA CLÁSICA

Fue el inventor, **Polybios** quien creó un sistema de señalización como alternativa al cifrado tradicional.

Básicamente, era un palo redondo envuelto alrededor de una tira larga y estrecha de pergamino con una escritura vertical. Sin la cinta el orden cambia por completo.

ROMA CLÁSICA

El método romano era muy simple, y se basaba en el **reemplazo** de un **carácter**. Cada letra se movía tres lugares superiores en orden alfabético, correspondiendo la última letra cíclicamente.

EVOLUCIÓN DE LA CRIPTOGRAFÍA

- **CRIPTOANÁLISIS**

  La **criptografía** consiste en el diseño de procedimientos para cifrar, mientras que el **criptoanálisis**, en la **ruptura** de esos procedimientos de cifrado para así **recuperar** la información original.

- **ORIGEN DEL CRIPTOANÁLISIS**

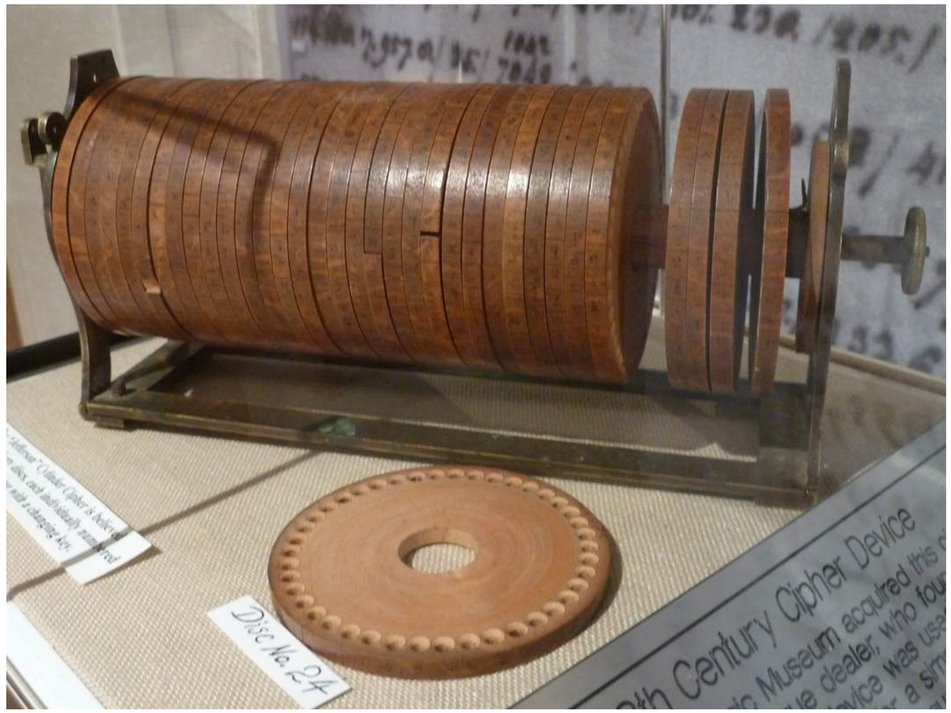
  La civilización musulmana fue la responsable del origen del criptoanálisis. Esta fue una civilización con grandes innovaciones en muchos aspectos como ciencias, matemáticas o literatura.

Criptografía en el renacimiento

La resurrección del cifrado ocurrió durante el **Renacimiento**. Tuvo lugar una expansión de uso del cifrado con la aparición del **estado moderno**.

Además, aparecieron nuevos **métodos** para **reemplazar** muchas letras y consonantes. A partir del siglo XIII. Los siglos XIV y XV vivieron un gran desarrollo.

Cilindro de Jefferson



Cilindro de Jefferson
Fuente: Cipher Machines

- **¿QUÉ ES EL CILINDRO DE JEFFERSON?**
  La rueda de cifrado, inventada por **Thomas Jefferson**, es un sistema de encriptado que utiliza ruedas o discos con las 26 letras del alfabeto distribuidas por su borde.

CRIPTOGRAFÍA MODERNA

El recorrido de la **criptografía** ha sido largo y esto ha llevado a muchos **avances** que ha hecho que la manera de encriptar y desencriptar o descifrar mensajes sea más **compleja**.

Máquinas para Encriptar

Máquina Enigma
Fuente: ABC (cultura)

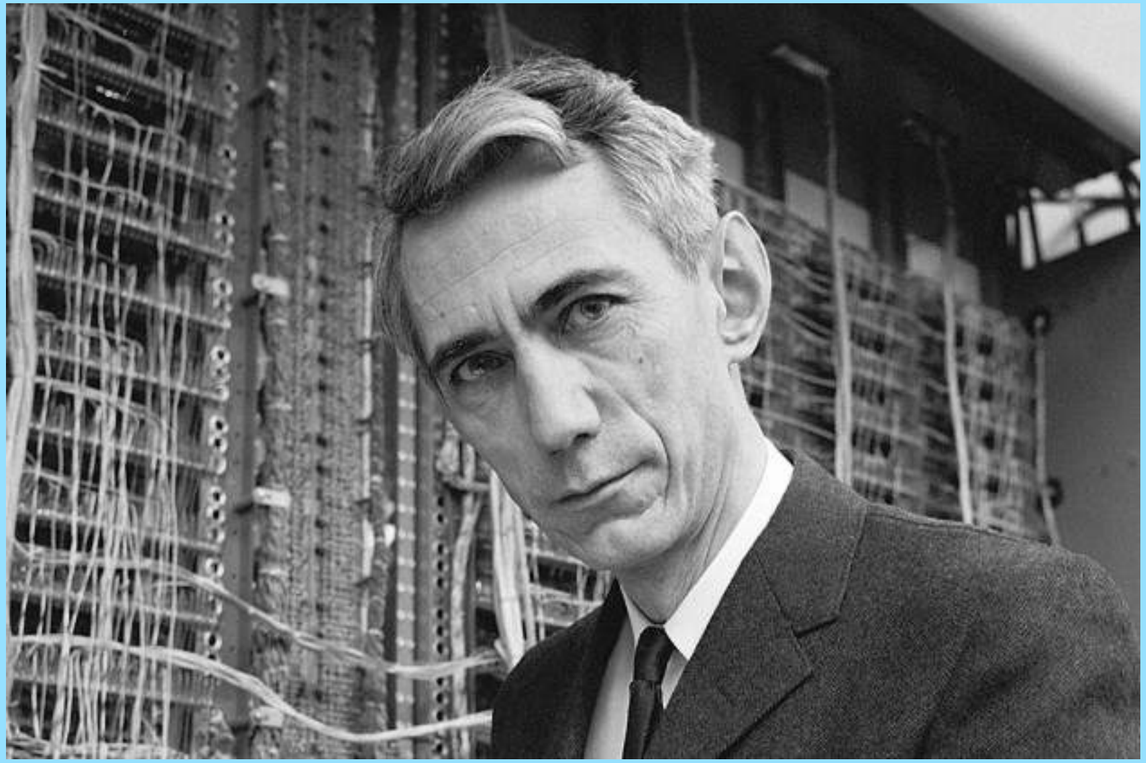
- **ENIGMA**

  Enigma fue la máquina criptográfica que utilizaban los nazis para enviar mensajes cifrados durante la **Segunda Guerra Mundial.**

- **BOMBE**

  Bombe fue el **primer ordenador** que se usó para descifrar las señales cifradas por la maquina **Enigma**.

Claude Shannon



Claude Shannon
Fuente: La voz del cora

Claude Shannon fue un **ingeniero** estadounidense que publicó **“A Communications Theory of Secrecy Systems”** en **1948**. Esto revolucionó y la criptografía dio un gran salto en el ámbito **global**.

Invención del ordenador

CONSECUENCIAS

Debido a la invención de los primeros ordenadores muchos países consideraron la criptografía como algo secreto.

DES

En 1975, IBM desarrolló DES que se convertiría en el nuevo algoritmo criptográfico en los ámbitos no militares y se expandiría por todo el mundo.

ADVANCED ENCRYPTION STANDARD

Seguido de DES, Advanced Encryption Standard lo sustituiría y este último permanecerá hasta la actualidad.

Técnicas de la criptografía moderna

CRIPTOGRAFÍA SIMÉTRICA

La criptografía simétrica es una técnica que utiliza solo una **clave secreta** para cifrar y descifrar la información.

CRIPTOGRAFÍA ASIMÉTRICA

La criptografía asimétrica utiliza dos claves (una **pública** y otra **privada**) lo
que hace que sea más seguro el traspaso de información.

ENCRIPTACIÓN ACTUAL

- **FIRMA DIGITAL**

  Conjunto de **datos** asociados a un mensaje que permiten asegurar la **identidad** del **firmante** y la **integridad** del **mensaje**

- **FUNCIÓN HASH**

  Algoritmo matemático capaz de **convertir** un bloque de **datos** en una colección nueva de **caracteres** con un tamaño específico.

Aplicaciones de la encriptación actual

SEGURIDAD

Cifrar datos:
Servicios de mensajería, redes sociales, correos electrónicos o transacciones bancarias.

ECONOMÍA

Sistemas de monedas encriptados mediante la función hash.

NFTs (Tokens no Fungibles) usados para comprobar la pertenencia de bienes digitales únicos.

CONCLUSIONES

- El arte de ocultar mensajes ha sido usado por muchas civilizaciones y culturas, con distintos mecanismos y procedimientos, pero con el mismo objetivo.

- Factores como la necesidad de ocultar información ha sido fundamental para el desarrollo de la criptografía.

- La criptografía ha sido muy importante en muchos momentos clave de la historia.

- La criptografía es usada en muchos ámbitos en la actualidad, ya que se utiliza para la seguridad en el tráfico de datos de aplicaciones de mensajería o redes sociales, y para verificar la veracidad de documentos o la pertenencia de bienes, como los NFTs.

BIBLIOGRAFÍA

Altavoz, S. A. (s. f.). Qué es la criptografía asimétrica y por qué es importante. http://www.altavoz.net. Recuperado 5 de marzo de 2022, de https://www.altavoz.net/altavoz/blog/desarrollo/que-es-la-criptografia-asimetrica-y-por-que-es-importante

Análisis de Frecuencias. (s. f.). Numerentur.org. Recuperado 25 de marzo de 2022, de https://numerentur.org/analisis-de-frecuencias/?msclkid=41c43a1bac8511ecb2c34f6ab30ad056

Baphomet y los templarios. (2008, noviembre 2). Curistoria. https://www.curistoria.com/2008/11/baphomet-y-los-templarios.html

Claude Shannon. (s. f.). Biografiasyvidas.com. Recuperado 5 de marzo de 2022, de https://www.biografiasyvidas.com/biografia/s/shannon.htm

Diffie, W., & Hellman, M. E. (s. f.). New directions in Cryptography invited paper. Tau.ac.il. Recuperado 5 de marzo de 2022, de http://www.cs.tau.ac.il/~bchor/diffie-hellman.pdf

El cifrado de Cesar. (s. f.). Ugr.es. Recuperado 5 de marzo de 2022, de https://www.ugr.es/~anillos/textos/pdf/2011/EXPO-1.Criptografia/02a04.htm

Galende Díaz, J. (1995). Criptografía. Madrid: Ed. Complutense.
Historia de la criptografía. (2018, noviembre 15). XLSemanal. https://www.xlsemanal.com/conocer/tecnologia/20180614/historia-de-la-criptografia.html

Jefferson, el criptógrafo. (2014, enero 11). Wordpress.com. https://ztfnews.wordpress.com/2014/01/11/jefferson-el-criptografo/

Maquina Enigma Alemana. (s. f.). Recuperado 5 de marzo de 2022, de https://www.areatecnologia.com/maquina-enigma-alemana.htm

Pasik, G. (2017, agosto 24). Todo sobre encriptación de datos para empresas. NextVision. https://nextvision.com/todo-sobre-encriptacion-de-datos-para-empresas/

Pool, R. S. (2020, junio 4). La fascinante historia de la criptografía. Style International. https://www.styleinternational.es/historia-criptografia/

Shannon, C. E. (1949). Communication theory of secrecy systems. The Bell System technical journal, 28(4), 656-715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

The famosos blog. (s. f.). Cifrado polialfabético. Blogspot.com. Recuperado 5 de marzo de 2022, de https://aesarg2012.blogspot.com/2012/01/cifrado-polialfabetico.html

Velasco, J. J. (2014a, abril 9). Qué debemos saber sobre Heartbleed, un grave agujero en sitios web supuestamente seguros. ElDiario.es. https://www.eldiario.es/turing/criptografia/detectan-vulnerabilidad-openssl-preocuparnos-comunicaciones_1_4944224.html

Velasco, J. J. (2014b, mayo 20). Breve historia de la criptografía. ElDiario.es. https://www.eldiario.es/turing/criptografia/breve-historia-criptografia_1_4878763.html

Wikipedia contributors. (s. f.-a). Bombe. Wikipedia, The Free Encyclopedia. Recuperado 5 de marzo de 2022, de https://es.wikipedia.org/w/index.php?title=Bombe&oldid=117440745

Wikipedia contributors. (s. f.-b). Enigma (máquina). Wikipedia, The Free Encyclopedia. Recuperado 5 de marzo de 2022, de https://es.wikipedia.org/w/index.php?title=Enigma_(m%C3%A1quina)&oldid=141743556

Xifré Solana, P. (2009). Antecedentes y perspectivas de estudio en historia de la criptografía. https://e-archivo.uc3m.es/handle/10016/6173

GRACIAS POR SU ATENCIÓN