educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 1

educación IT
CODE YOUR FUTURE

Historia de la Criptografía

Hitos

- **3600 a. C.:** los sumerios desarrollaron la escritura cuneiforme y los egipcios la jeroglífica.
- **1900 a. C.**: grabado de piedra en la tumba de Menet Khufu, con modificaciones en la escritura jeroglífica.
- **1600 a. C.**: los fenicios inventan el alfabeto.
- **500 a. C.**: el Atbash comienza a utilizarse.

  En Alejandría se propone el uso de antorchas para enviar mensajes, conocido como *Fryctoria.*
- **480 a. C.**: en la batalla de Salamina, la victoria griega es gracias al aviso de Demarato, usando la esteganografía.
- **430 a. C.**: Heródoto deja constancia del uso de la criptografía en varias de sus historias.
- **400 a. C.**: Eneas el Táctico escribe su tratado militar en el que dedica un capítulo completo a la criptografía.

  Los espartanos usan la escítala para comunicarse con seguridad.

- **120 a. C.**: Polibio crea su cuadrado, su matriz de cinco filas y cinco columnas donde a cada letra le corresponde una celda.
- **100 d. C.**: Suetonio escribe su Vida de los doce césares , en donde se describen algunas técnicas criptográficas, como el cifrado de Julio César.
- **300 d. C.**: se escribe el Kamasutra , que incluye la escritura secreta como una de las artes a conocer por las mujeres.
- **801 d. C.**: nace Al-Kindi, pionero en el análisis de frecuencias.
- **999 d. C.**: accede al papado Silvestre II, que utilizó las tironianas en varios escritos, incluidas dos de sus bulas.
- **1379 d. C.**: Gabriel de Lavinde crea los nomenclátores para el Papa.
- **1450 d. C.**: se escribe el Manuscrito Voynich, que utiliza algún código aún por descifrar, si bien se sigue trabajando sobre él.
- **1466 d. C.**: León Battista Alberti, creador del disco que lleva su nombre, inicia la idea de las cifras polialfabéticas.
- **1474 d. C.**: Cicco Simonetta publica sus 12 puntos sobre el criptoanálisis.

- **1500 d. C.**: se publica la obra de Tritemio, donde aparecen las tablas que llevan su nombre.
- **1518 d. C.**: se imprime el libro Poligrafía , escrito por Tritemio, siendo el primer libro impreso dedicado a la criptografía.
- **1540 d. C.**: nace Philips van Marnix, criptógrafo holandés.
- **1553 d. C.**: Bellaso publica varios retos criptográficos, algunos de los cuales aún están por resolver. Describe también una cifra similar a la cifra Vigènere.
- **1585 d. C.**: Vigenère publica su tratado, donde describe el método ideado por Bellaso y que será considerado como una cifra indescifrable durante mucho tiempo.
- **1586 d. C.**: tiene lugar la conjura de Babington, que acabó con la condena a muerte de María Estuardo.
- **1588 d. C.**: se publica el libro de cifras de Vigenère.
- **1626 d. C.**: durante el asedio de Realmont, Antoine Rossignol comienza su carrera como criptógrafo.
- **1671 d. C.**: Leibniz inventa una máquina calculadora.

- **1711 d. C.:** se crea la Oficina del Gabinete Secreto en Viena.
- **1753 d. C.**: comienza a diseñarse y desarrollarse el telégrafo.
- **1790 d. C.**: Thomas Jefferson diseña su rueda para cifrar mensajes.
- **1854 d. C.**: se crea el cifrado Playfair.
- **1863 d. C.**: Kasiski pública la ruptura de los cifrados polialfabéticos.
- **1883 d. C.**: Auguste Kerckhoffs escribe La criptografía militar y pública el principio que lleva su nombre.
- **1885 d. C.**: se descubren los papeles de Beale, una serie de documentos cifrados que podrían ocultar un tesoro, y que siguen sin descifrarse.
- **1890 d. C.**: Bazeries rompe la cifra de los Rossignol, usada por los reyes franceses dos siglos antes. Además, crea un dispositivo similar a la rueda de Jefferson.
- **1904 d. C.**: en la guerra ruso - japonesa se emplea por primera vez el análisis de tráfico de señales.

- **1914 d. C.**: los rusos hunden el SMS Magdeburg, capturando importantes libros de códigos.

  Gracias a la intercepción de los mensajes rusos, los alemanes vencen en la batalla de Tannenberg.

- **1915 d. C.**: William Friedman, uno de los más importantes criptógrafos estadounidenses, avanza en la aplicación de la estadística al criptoanálisis. Los franceses comienzan a utilizar los códigos de trinchera.

- **1916 d. C.**: Alemania crea su oficina de criptografía, el Abhorchdienst.

- **1917 d. C.**: el telegrama Zimmermann es enviado, capturado y descifrado, provocando la entrada de Estados Unidos en la Primera Guerra Mundial.

- **1918 d. C.**: aparece la idea de cifra irrompible, basada en una clave de longitud infinita.

  Se inventa la máquina Enigma.

  Los indios Choctaw sirven en el ejército utilizando su idioma, desconocido para el resto, para asegurar las comunicaciones.

  Se introduce el cifrado ADFGVX en Alemania.

- **1919 d. C.**: la Alemania de Weimar utiliza la clave de un solo uso para algunas de sus comunicaciones.

  Se patenta la máquina de rotores.

  Vernam patenta el cifrado que lleva su nombre.

- **1929 d. C.**: se cancela el *Black Chamber* estadounidense.

- **1931 d. C.**: se publica el libro de Herbert Yardley, en el que describe el *Black Chamber* de Estados Unidos y cómo habían espiado las comunicaciones de otros países.

- **1932 d. C.**: los criptógrafos polacos comienzan a romper los cifrados de Enigma.

- **1935 d. C.**: los criptógrafos alemanes rompen el código administrativo naval británico.

- **1939 d. C.**: los japoneses comienzan a usar el código JNd. C.:25.

  El código Púrpura sustituye al código Rojo.

  Polonia comparte su conocimiento de Enigma con Francia y Reino Unido.

- **1940 d. C.**: se recuperan dos rotores de Enigma del submarino Ud. C.:33 , por parte de los aliados.

  La *Bombe* británica comienza a operar.

  Se rompe el código principal de la Abwehr.

- **1941 d. C.**: se rompen los códigos de la Luftwaffe en África.

  se descifran los mensajes de la Enigma naval de febrero gracias a documentos capturados.

  Alemania comienza a leer el nuevo código naval británico, utilizado por los aliados para comunicarse con los convoyes atlánticos.

- **1942 d. C.**: el tráfico del agregado militar de Estados Unidos en El Cairo comienza a ser leído por los alemanes.

  Se modifica la Enigma naval (*Shark* para los británicos) para los submarinos en el Atlántico, con un cuarto rotor.

  Se lee de forma regular el código JN-25B.

  Comienza la colaboración de Estados Unidos y los británicos contra Enigma.

  Se rompe la Enigma naval gracias a las comunicaciones meteorológicas.

- **1943 d. C.**: los Aliados cambian sus códigos y los alemanes no pueden conocer el contenido de sus comunicaciones en el Atlántico.
- **1944 d. C.**: la *Colossus I* es entregada y se encargan cincuenta *Bombes* adicionales.

  El proyecto Venona comienza a tomar forma.
- **1946 d. C.**: el proyecto Venona rompe los cifrados soviéticos.
- **1949 d. C.**: Claude Shannon publica un artículo que da soporte matemático a una cifra indescifrable.
- **1951 d. C.**: se crea la NSA.
- **1968 d. C.**: se publica la idea de la computación cuántica, de Stephen Wiesner.
- **1973 d. C.**: Clifford Cocks, dentro del GCHQ, descubre una función que permite la criptografía asimétrica.
- **1976 d. C.**: se acepta el como un estándar.

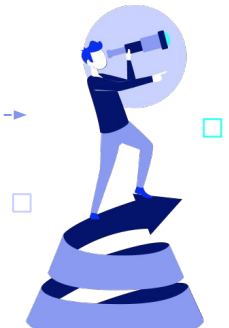
  Se publica el esquema de cifrado de clave pública de Diffie, Hellman y Merkle.
- **1977 d. C.**: se publica el sistema RSA.
- **1984 d. C.**: Charles H. Bennett y Gilles Brassard propusieron un método de comunicación segura basado en el trabajo de Wiesner, conocido como Protocolo BB84.

- **1991 d. C.**: Artur Ekert desarrolló el protocolo E91 o EPR para la distribución de claves cuánticas basado en el entrelazamiento cu**ántico.**
- **1994 d. C.**: Peter Shor propone su algoritmo que emplea matemáticas asociadas a la teoría de números, el análisis de Fourier, números complejos, entre otros. Este algoritmo dejaría obsoleto a algoritmos como el RSA.
- **2008 d. C.**: una colaboración entre la Universidad de Cambridge y Toshiba, usando el protocolo BB84 consiguió el sistema de intercambio con claves seguras (QKD) a 1 Mbit/s, en más de 20 km de fibra óptica, y 10 kbit/s, en más de 100 km de fibra.
- **2015 d. C.**: la Universidad de Ginebra y Corning Inc. lograron la distancia de QKD más larga para fibra óptica (307 km). En el mismo experimento, se generó una tasa de intercambio de clave secreta de 12,7 kbit/s.
- **2017 d. C.**: el Instituto de Computación Cuántica y la Universidad de Waterloo, Canadá, lograron la primera demostración de la distribución de claves cuánticas desde un transmisor terrestre a un avión en movimiento. Reportaron enlaces ópticos con distancias entre 3-10 km y generaron claves seguras de hasta 868 kilobytes de longitud.

- **2017 d. C.**: el protocolo BB84 se implementó con éxito a través de enlaces de satélite a estaciones terrestres en China y Austria. Las claves se combinaron y el resultado se usó para transmitir imágenes y videos entre Pekín y Viena.
- **2023 d. C.**: NIST estandariza algoritmos de cifrado resistentes a los ataques de las computadoras cuánticas. Se espera que estén listos para su uso en 2024.

Hitos más relevantes

- **3600 a. C.** — Escritura cuneiforme y jeroglífica.
- ...
- **500 a. C.** — Atbash.
- **480 a. C.** — Uso de la esteganografía.
- **430 a. C.** — Criptografía.
- **400 a. C.** — Criptografía en táctica militar; Escítala.
- **120 a. C.** — Matriz de Polibio.
- ...
- **1518 d. C.** — 1er libro impreso de criptografía.
- **1585 d. C.** — Tratado de Vigenère.
- **1854 d. C.** — Cifrado Playfair.
- **1883 d. C.** — Principio Kerckhoffs.
- **1904 d. C.** — Análisis de tráfico de señales.
- **1915 d. C.** — Estadística al criptoanálisis.
- **1918 d. C.** — La cifra irrompible; máquina Enigma; comunicaciones Choctaw; cifrado ADFGVX.
- **1919 d. C.** — Clave solo uso; Máquina de rotores; Cifrado Vernam.
- **1932 d. C.** — Cifrados de Enigma.
- **1951 d. C.** — Creación de la NSA.
- **1968 d. C.** — Computación cuántica
- **1973 d. C.** — Criptografía asimétrica
- **1976 d. C.** — Cifrado DES; cifrado de clave pública.
- **1977 d. C.** — Sistema RSA
- **1984 d. C.** — Protocolo BB84.
- **1991 d. C.** — Protocolo E91 o EPR
- **1994 d. C.** — Algoritmo Peter Shor
- **2008 d. C.** — QKDa 1 Mbit/s
- **2015 d. C.** — Distancia de QKD más larga para fibra óptica (307 km).
- **2017 d. C.** — Distribución de claves cuánticas; Protocolo BB84: enlaces de satélite
- **2023 d. C.** — Cifrado resistente a los ataques de las computadoras cuánticas.



¡Sigamos trabajando!