GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura i Esport

ceedcv CENTRE ESPECÍFIC D'EDUCACIÓ A DISTÀNCIA DE LA COMUNITAT VALENCIANA

Unidad 4.1
Criptografía

Índice

Sumario

Licencia

1. Introducción a la criptografía

La criptografía es un campo de estudio y práctica que se ocupa de la seguridad de la información a través de técnicas específicas. Su objetivo principal es garantizar la confidencialidad, la autenticidad e integridad de los datos en situaciones donde la información puede ser vulnerable a accesos no autorizados o manipulaciones.

En términos más simples, la criptografía utiliza métodos matemáticos y algoritmos para transformar la información de manera que solo aquellos que poseen la clave adecuada puedan entenderla. Se centra en proteger la comunicación y el almacenamiento de datos sensibles, evitando que terceros no autorizados puedan comprender o alterar la información.

La criptografía se aplica en diversos contextos, desde la seguridad en las comunicaciones en línea y transacciones financieras hasta la protección de datos almacenados en dispositivos electrónicos.

La criptografía se basa en diversos principios clave como son:

- **Confidencialidad**: Este principio implica codificar el contenido del mensaje, asegurando que solo los destinatarios autorizados puedan comprenderlo. Los algoritmos de cifrado desempeñan un papel crucial en este proceso.
- **Autenticación**: Se utiliza métodos criptográficos para verificar el origen de un mensaje, asegurando que provenga de la fuente declarada y no de un tercero no autorizado. Esto es esencial para evitar la suplantación de identidad y garantizar la legitimidad de las comunicaciones. La signatura digital es la herramienta más usada en este aspecto.
- **Integridad**: La integridad en criptografía demuestra que el contenido de un mensaje no ha sufrido alteraciones desde el momento en que fue enviado. Esto se logra mediante el uso de funciones hash y firmas digitales, que permiten verificar si un mensaje ha sido modificado durante la transmisión.

Estas características forman la base de los protocolos de seguridad y las prácticas criptográficas que son esenciales en entornos digitales. La criptografía desempeña un papel crítico en la protección de la privacidad, la confidencialidad de la información y la integridad de las comunicaciones en un mundo cada vez más interconectado.

Algunos conceptos clave que estudiaremos en esta unidad son:

- **Cifrado**: Proceso de convertir información en un formato ilegible (cifrado) que solo puede ser revertido por aquellos que poseen la clave secreta (descifrado). Hay diferentes algoritmos de cifrado, como AES (Advanced Encryption Standard) y RSA (Rivest-Shamir-Adleman).
- **Clave**: Una clave es un valor secreto utilizado por un algoritmo de cifrado para cifrar y descifrar datos. Puede ser una clave simétrica (la misma clave se utiliza tanto para cifrar como para descifrar) o asimétrica (se utilizan claves distintas para cifrado y descifrado).
- **Hashing**: Una función de hash toma una entrada (o mensaje) y produce una cadena de caracteres de longitud fija, que suele ser una representación única de la entrada. Se utiliza para verificar la integridad de los datos y generar resúmenes criptográficos.
- **Firma Digital**: Una firma digital es un esquema matemático que se utiliza para demostrar la autenticidad e integridad de un mensaje o documento digital. Se utiliza comúnmente en transacciones electrónicas y documentos legales.
- **Protocolos de Seguridad**: Conjuntos de reglas y procedimientos que garantizan la seguridad de las comunicaciones. Ejemplos incluyen TLS (Transport Layer Security) para la seguridad en las comunicaciones web y IPsec para la seguridad en las comunicaciones de red.

2. Historia de la criptografía

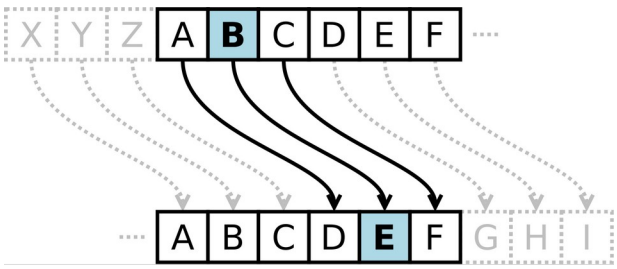
La criptografía durante la historia ha venido marcada ingeniosas técnicas desarrolladas por civilizaciones antiguas, mentes brillantes de la Edad Media y los desafíos sin precedentes enfrentados durante eventos históricos como la Segunda Guerra Mundial.

Repasaremos los hitos clave que han dado forma a la evolución de la criptografía y su papel fundamental en la protección de la información y la seguridad de las comunicaciones.

2.1. Criptografía Clásica:

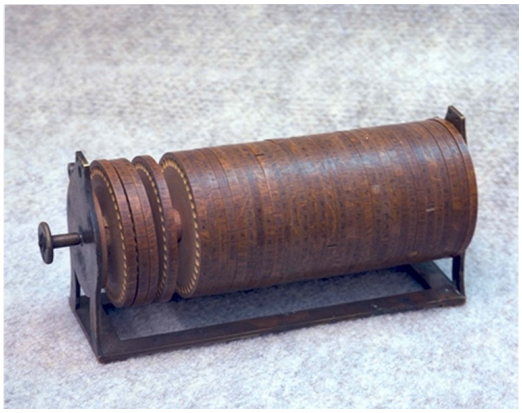
- **Año 1500 a.C.** - Una Tableta Mesopotámica: es uno de los primeros ejemplos conocidos de cifrado. Este antiguo método involucraba la sustitución de caracteres para ocultar el significado del mensaje mediante una fórmula cifrada para producir un vidriado cerámico.
- **Año 487 a.C.** - El Bastón Griego SCYTALE: Los espartanos utilizaron el bastón SCYTALE como una herramienta de cifrado. Este dispositivo consistía en un bastón alrededor del cual se enrollaba una tira de cuero o pergamino con un mensaje. El mensaje solo era legible cuando se enrollaba alrededor de un bastón del mismo diámetro.

- **Año 50 a.C.** - Técnica utilizada por Julio César: El Emperador romano Julio César empleó una técnica de cifrado simple conocida como el "Cifrado César". Esta técnica implicaba desplazar las letras del alfabeto, y es considerada uno de los primeros ejemplos de cifrado de sustitución.



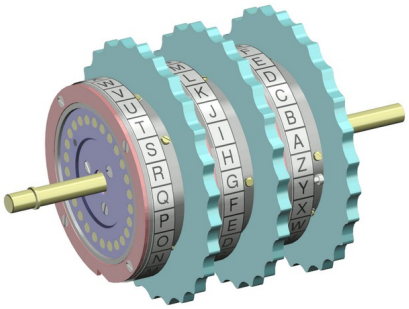
2.2. Criptografía Medieval:

- **Año 820-866 d.C.** - Al-Kindi y el Análisis de Frecuencias: Al-Kindi, un filósofo matemático y criptógrafo, inventó la técnica del análisis de frecuencias. Esta técnica se basaba en el estudio de la frecuencia de las letras en un mensaje cifrado para descifrarlo. Con esto Al-Kindi rompió los cifrados por sustitución monoalfabéticos como el "Cifrado César".
- **Año 1466 d.C.** - Leone Alberti y el Cifrado Polialfabético: Leone Alberti desarrolló el cifrado polialfabético, un avance importante que implicaba el uso de múltiples alfabetos para cifrar mensajes, complicando la tarea de descifrarlos. Se consideró como la solución contra la técnica de análisis de frecuencia de Al-Kindi.
- **Año 1798 d.C.** - Thomas Jefferson y la Rueda de Cifrado: En la década de 1790, Thomas Jefferson diseñó un sistema conocido como la "rueda de cifrado". Esta era una máquina que permitía cambiar el cifrado de un mensaje utilizando 36 anillos de letras en ruedas móviles, que podían ser utilizados para lograr codificados complejos.



2.3. 1800 y la Segunda Guerra Mundial:

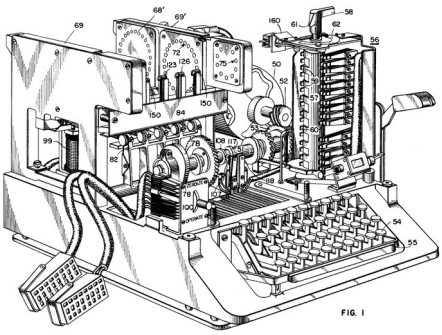
- **Año 1854** - Cifrado de Matriz de Charles Wheatstone: Charles Wheatstone inventó el Cifrado de Matriz de 5×5 como clave, luego conocido como Cifrado Playfair.
- **Año 1915-1919** - Varios inventores de distintos países y sin ninguna relación entre sí inventaron y patentaron varios modelos distintos de máquinas de rotores, que no llegaron a comercializarse. Este fue un precursor importante para las máquinas de cifrado de la Segunda Guerra Mundial.
- **Año 1923** - La Máquina de Rotores "**Enigma**", diseñada por el alemán Arthur Scherbius, fue utilizada por los alemanes durante la Segunda Guerra Mundial. Esta máquina de cifrado se volvió famosa por su complejidad y fue un desafío considerable para los criptoanalistas aliados.



Tres rotores de la máquina Enigma.

La máquina Enigma

- **Año 1944** - Las máquinas de cifrado aliadas utilizadas en la Segunda Guerra Mundial incluían la Typex británica y la SIGABA estadounidense, que desempeñaron un papel crucial en la seguridad de las comunicaciones aliadas.



Máquina SIGABA

2.4. Criptografía Moderna:

- **Años 1950-1970** - Dominio de la NSA y Protocolo Diffie-Hellman: La NSA acaparó y bloqueó la mayoría de las publicaciones sobre avances en criptografía durante este período.
- **Sin embargo, en 1976**, Whitfield Diffie y Martin Hellman introdujeron el protocolo criptográfico Diffie-Hellman, que revolucionó la seguridad de las comunicaciones. Es un protocolo de establecimiento de claves entre partes que no han tenido contacto previo, utilizando un canal inseguro y de manera anónima (no autenticada).
- **Año 1999** - Se hizo público el algoritmo de cifrado Data Encryption Standard (DES), que había sido utilizado ampliamente en aplicaciones gubernamentales y comerciales, con el OK de la NSA.

- **Año 2001** - El algoritmo DES fue oficialmente suplantado por el Advanced Encryption Standard (AES), un algoritmo más robusto y eficiente que se ha convertido en un estándar ampliamente aceptado en todo el mundo.

  Actualmente, hay tres tipos de cifrado AES: 128 bits, 192 bits y 256 bits, donde este último por su longitud en el número de bits es el más seguro.

- **Año 2006** - Surgió la criptografía postcuántica (PQC del inglés Post-Quantum Cryptography) en respuesta a las amenazas potenciales que plantea la computación cuántica para los algoritmos criptográficos convencionales. La PQC, también conocida como criptografía resistente a la computación cuántica, se enfoca en desarrollar algoritmos criptográficos que sean capaces de resistir los ataques de computadoras cuánticas. Mientras que la mayoría de los algoritmos criptográficos simétricos actuales son considerados relativamente seguros ante ataques cuánticos, la PQC se concentra en algoritmos asimétricos para garantizar una seguridad a largo plazo.

  Es importante destacar que la criptografía postcuántica difiere de la criptografía cuántica, que utiliza fenómenos cuánticos para asegurar la confidencialidad y detectar posibles espionajes. La criptografía cuántica como idea se propuso en 1970 por Stephen Wiesner, pero no fue hasta 1984 que Charles H. Bennett y Gilles Brassard propusieron un método de comunicación segura basado en el trabajo de Wiesner, conocido hoy como el protocolo BB84. En 1991 Artur Ekert desarrolló el protocolo E91 o EPR, un enfoque diferente para la distribución de claves cuánticas basado en correlaciones cuánticas peculiares conocidas como entrelazamiento cuántico.