educación IT
CODE YOUR FUTURE

Introducción a la Ciberseguridad

Módulo 5

educación IT
CODE YOUR FUTURE

Introducción a la criptografía

Criptografía

La palabra *criptografía* es un término genérico que describe todas las **técnicas que permiten cifrar mensajes o hacerlos ininteligibles** sin recurrir a una acción específica.

El verbo asociado es ***cifrar.***

La criptografía se basa en la aritmética:
En el caso de un texto, consiste en transformar las letras que conforman el mensaje en una serie de números (en forma de bits ya que los equipos informáticos usan el sistema binario) y luego realizar cálculos con estos números para:

- **Modificarlos y hacerlos incomprensibles.** El resultado de esta modificación (el mensaje cifrado) se llama *texto cifrado*, en contraste con el mensaje inicial, llamado *texto plano.*
- **Asegurarse de que el receptor pueda descifrarlos.** El hecho de codificar un mensaje para que sea secreto se llama *cifrado.* El método inverso, que consiste en recuperar el mensaje original, se llama *descifrado.*

Como mencionamos, en la jerga de la criptografía, la información original que debe protegerse se denomina *texto plano.* **El cifrado es, entonces, el proceso de convertir el texto plano en un texto ilegible, llamado *texto cifrado* o *criptograma.***

Por lo general, la aplicación concreta del algoritmo de cifrado se basa en la existencia de una **clave:** información secreta que adapta el algoritmo de cifrado para cada uso distinto.

Cifrado

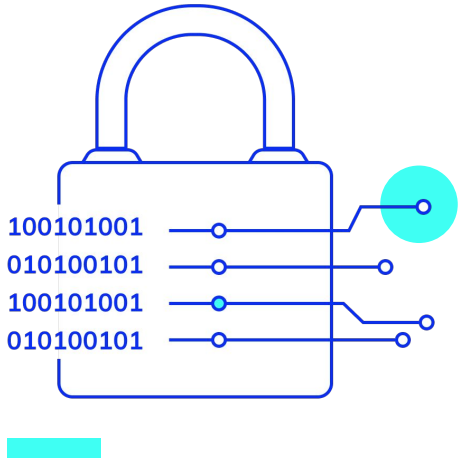
Las dos técnicas más sencillas de cifrado, en la criptografía clásica, son la **sustitución** (que supone el cambio de significado de los elementos básicos del mensaje: las letras, los dígitos o los símbolos) y la **transposición** (que supone una reordenación de los mismos); la gran mayoría de las cifras clásicas son combinaciones de estas dos operaciones básicas.

Descifrado

El **descifrado** es el proceso inverso que **recupera el texto plano a partir del criptograma y la clave.** El protocolo criptográfico especifica los detalles de cómo se utilizan los algoritmos y las claves.

Criptosistema

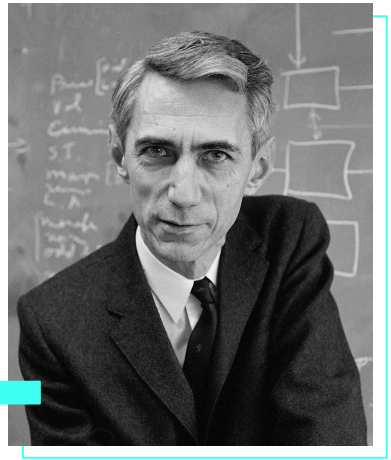
El conjunto de protocolos, algoritmos de cifrado, procesos de gestión de claves y actuaciones de los usuarios, es lo que constituyen en conjunto un **criptosistema,** que es con lo que el usuario final trabaja e interactúa.



Criptografía moderna

Shannon

La era de la criptografía moderna comienza realmente con **Claude Shannon, el padre de la criptografía matemática.** En 1949 publicó varios trabajos que establecieron una sólida base teórica para la criptografía y el criptoanálisis. Y, a la vez, la criptografía desapareció de la escena para quedarse dentro de las organizaciones gubernamentales secretas como la NSA. Muy pocos trabajos se hicieron públicos hasta mediados de los 70's, cuando todo cambió.



Claude Shannon (1916-2001)

Un estándar de cifrado

A mediados de los 70 se vivieron dos importantes avances públicos. El primero fue la publicación del borrador del ***Data Encryption Standard (DES)*** en el Registro Federal estadounidense el 17 de marzo de 1975. La propuesta fue enviada por IBM, por invitación de la Oficina Nacional de Estándares (ahora NIST), en un esfuerzo por desarrollar sistemas de comunicación electrónica segura para las empresas como los bancos y otras organizaciones financieras grandes.

El DES fue el primer cifrado accesible públicamente que fue avalado por una agencia nacional como la NSA. La publicación de sus especificaciones por la NBS estimuló el interés público y académico por la criptografía.

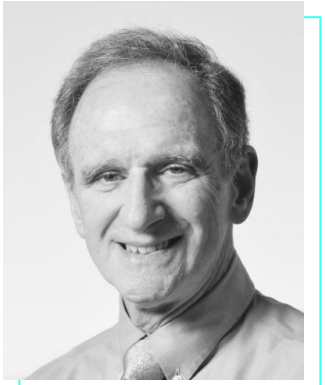
DES fue suplantado oficialmente por el *Advanced Encryption Standard (AES)* en 2001. Tras una competición abierta, el NIST seleccionó el Rijndael, enviado por dos criptógrafos belgas, para convertirse en el AES.

El DES y otras variantes más seguras (como el Triple DES), aún se utilizan y se han incorporado en muchos estándares nacionales y de organizaciones. Sin embargo, se ha demostrado que **el tamaño de su clave, 56 bits, es insuficiente ante ataques de fuerza bruta.**

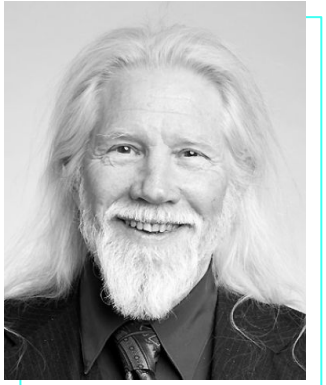
Diffie-Hellman

El segundo desarrollo, en 1976, fue quizás más importante todavía, ya que cambió de manera fundamental la forma en que los criptosistemas pueden funcionar. Fue la publicación del artículo ***New Directions in Cryptography,*** de Whitfield Diffie y Martin Hellman. Introdujo un **método radicalmente nuevo para distribuir las claves criptográficas,** dando un gran paso adelante para resolver uno de los problemas fundamentales de la criptografía, la distribución de claves, y ha terminado llamándose ***intercambio de claves Diffie-Hellman.***

El artículo también estimuló el desarrollo público casi inmediato de un **nuevo tipo de algoritmo de cifrado,** los ***algoritmos de cifrado asimétrico.***



Martin Hellman



Whitfield Diffie

Principios de Kerckhoffs

Auguste Kerckhoffs publicó en 1883 seis principios relativos a las **propiedades deseables de un sistema criptográfico**:

1. Si el sistema no es teóricamente irrompible, al menos debe serlo en la práctica.
2. La efectividad del sistema no debe depender de que su diseño permanezca en secreto.
3. La clave debe ser fácilmente memorizable de manera que no haya que recurrir a notas escritas.
4. Los criptogramas deberán dar resultados alfanuméricos.
5. El sistema debe ser operable por una única persona.
6. El sistema debe ser fácil de utilizar.

> **Nota:** de estos seis, el segundo suele ser conocido como *Principio de Kerckhoff.*

educación IT
CODE YOUR FUTURE

¡Sigamos trabajando!