Tipos de algoritmos criptográficos

DigitalHouse>

Certified Tech Developer
The Ultimate Degree

Algoritmos criptográficos

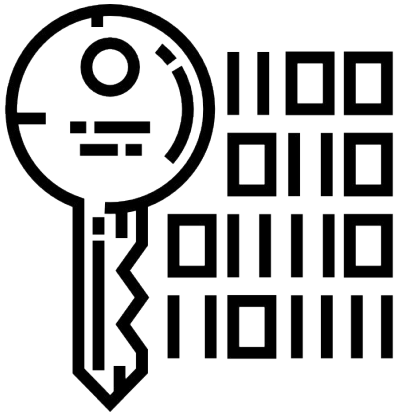
A continuación, veremos algunos ejemplos de **algoritmos criptográficos** sencillos que no están en el contexto de la aplicación informática, sino que son algoritmos que producen mensajes cifrados.

Índice

1 | Transposición

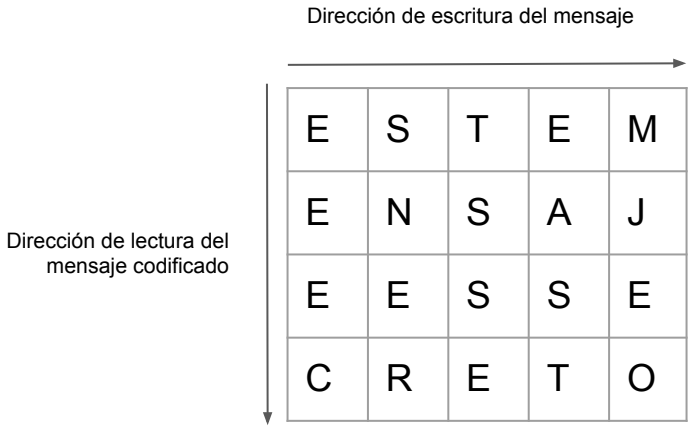
Transposición

Es un algoritmo que se basa en dividir un mensaje, **cifrarlo** en columnas y luego transcribirlo usando el nuevo orden de los caracteres dado por esas columnas. La cantidad de columnas es la **clave** que se utilizará para **codificar** y **decodificar** el mensaje.



Ejemplo de transposición

Mensaje a cifrar: “Este mensaje es secreto”. **Clave:** Utilizar una matriz de 5x4.



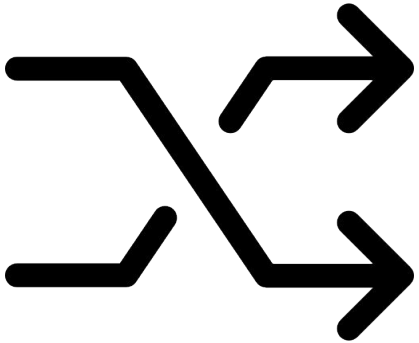
Mensaje codificado: “EEEC SNER TSSE EAST MJEO”.

2 | Sustitución

Sustitución

La **sustitución** es un algoritmo criptográfico que produce un mensaje **cifrado** a partir del reemplazo de los caracteres de un mensaje por otros. El elemento que establece las reglas para el reemplazo es la **clave**.

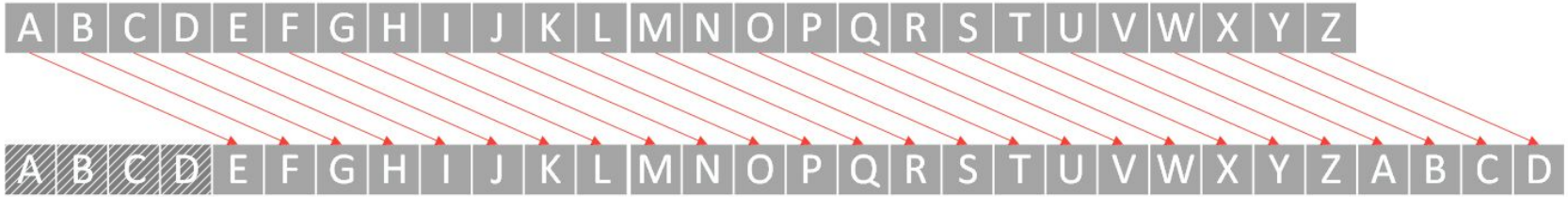
Un ejemplo de sustitución es establecer un desplazamiento de dos caracteres en el alfabeto. De este modo, todas las letras “A” del mensaje a cifrar se reemplazan por letras “C”. Este algoritmo de sustitución se lo conoce como **cifrado César** o **cifrado por desplazamiento**.



Ejemplo de sustitución con cifrado César

Mensaje a cifrar: “Este mensaje es secreto”.

Clave: Desplazamiento de 4 caracteres.

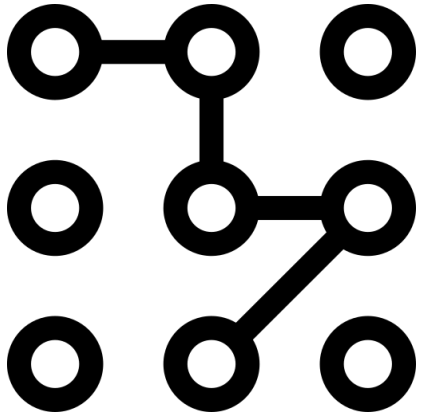


Mensaje codificado: “IWXI QIRWENI IW WIGVIXS”.

3 | Ocultación

Ocultación

En el caso de la **ocultación**, el objetivo es esconder el mensaje en otro mensaje u objeto. La **clave** en este caso son las indicaciones que permiten al individuo encontrar el mensaje.



Ejemplo de ocultación

Mensaje a cifrar: “Este mensaje es secreto”

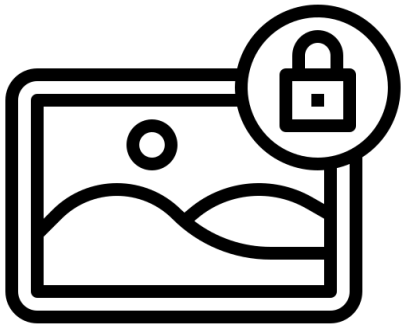
Clave: La primera letra de cada oración contendrá el mensaje.

Mensaje codificado: “**E**lefantes fueron avistados por primera vez en la costa de Nairobi. **S**umamente sorprendidos, los conservacionistas se acercaron para observarlos. **T**ímidos, pero no asustados, los elefantes mantuvieron su posición. **E**l más pequeño de la manada jugaba cerca del agua. **M**ientras tanto, el elefante que lideraba la familia se aseguraba de que haya una distancia prudencial entre los científicos y su familia. **E**n algunas oportunidades los científicos pudieron acercarse. **N**o podían determinar cuánto tiempo los elefantes estaban allí, de modo que querían aprovechar el tiempo. **S**ubidos a los árboles, algunos científicos pudieron tomar fotografías panorámicas. **A** la distancia podía observarse una segunda manada aproximándose. **J**ugaban. **E**lefantes pequeños. **E**lefantes grandes. **S**orprendidos los científicos decidieron alejarse. **S**abían que lo que habían presenciado era un evento único. **E**n tanto el gobierno lo permita, los científicos volverán al sitio. **C**uando sea posible volveremos, dijo el jefe de la expedición. **R**ara vez puede uno ser testigo de un evento como este. **E**lefantes volviendo a un área donde se los creía extintos. **T**odos celebraron el evento. **O**tra parte del equipo prefirió quedarse documentando el suceso para no perder detalles del mismo”.

4 | Esteganografía

Esteganografía

La **esteganografía** es una forma de ocultación, pero vale la pena mencionarla por separado, ya que es una forma habitual de cifrar mensajes. Consta de **ocultar un mensaje dentro de un archivo de datos** —imagen, audio— sin alterar el contenido original del archivo.



DigitalHouse>