COLOMBIA POTENCIA DE LA VIDA

TIC

Módulo 1

LECCIÓN 1

Generalidades de la tecnología blockchain

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

Bases de la criptografía:

Empecemos haciendo la pregunta de ¿qué es la criptografía? La criptografía es una práctica que busca salvaguardar la información mediante el uso de algoritmos codificados, hashes y firmas. Puede aplicarse a datos en reposo como un archivo en una unidad de almacenamiento, en tránsito como en la comunicación de dos aplicaciones que requieren el intercambio de información o en uso cuando un computador hace operaciones determinadas.

La criptografía persigue cuatro objetivos principales:

- **Confidencialidad:** Restringir la información solo a usuarios autorizados..

- **Autenticación:** confirmar la autenticidad de la información o identidad de un usuario.

- **Integridad:** garantizar que la información no haya sido manipulada.

- **No repudio:** prevenir que un usuario niegue compromisos o acciones previas.

Utilizando algoritmos criptográficos de bajo nivel, como cifrado, firma digital y funciones de hash, se logran estos objetivos de seguridad. En el caso de usar un hash, se está garantizando que el archivo en cuestión es único, ya que, si recibe alguna alteración o cambio, el hash en cuestión va a ser diferente, permitiendo alertar al sistema de una discrepancia en la autenticidad e integridad del archivo.

Ahora que conocemos las características y objetivos fundamentales de la criptografía surge la pregunta ¿para qué se utiliza la criptografía? Esta tiene sus orígenes en el envío de información sensible entre militares, políticos y altos mandos de los gobiernos, y ha evolucionado hasta convertirse en el medio para asegurar aplicaciones web y sistemas de procesamiento computacionales. Uno de sus usos más comunes es para asegurar la transferencia de información en internet con HTTPS (HyperText Transfer Protocol Secure) y en comunicaciones de texto y voz, etc.

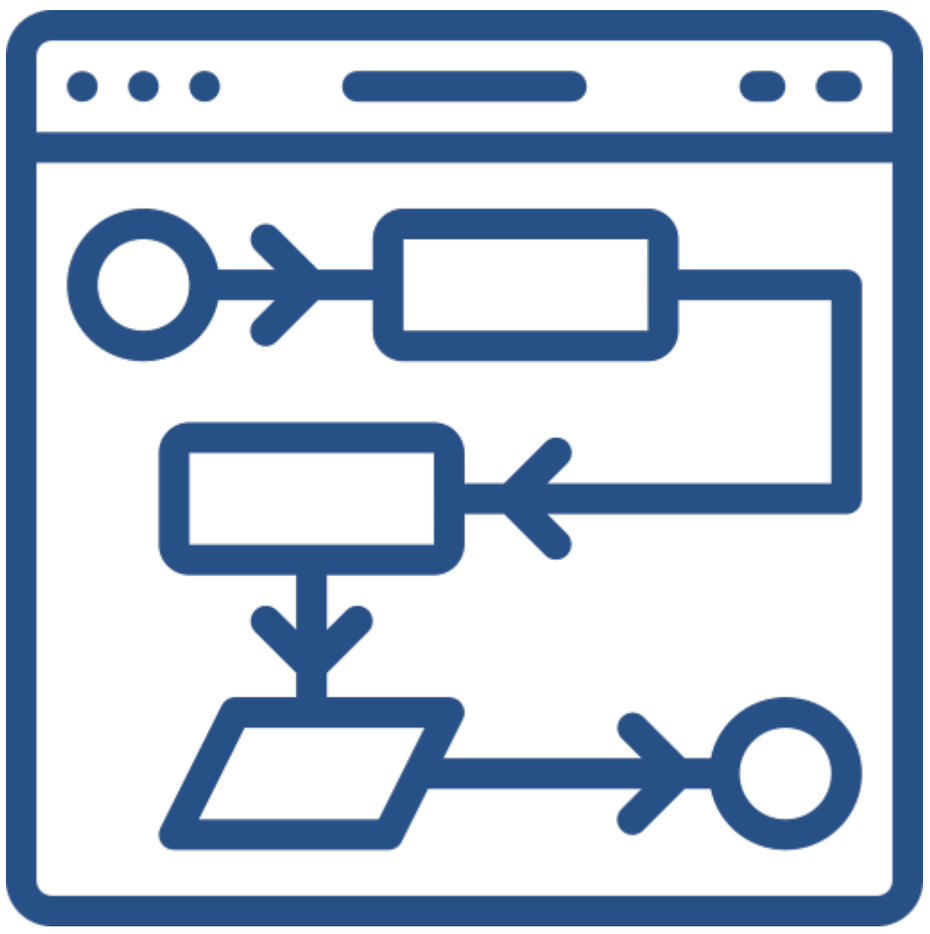
El cifrado

El cifrado es un procedimiento que transforma un mensaje de texto plano en un texto cifrado mediante algoritmos avanzados y una o varias claves, es decir, el texto plano ahora es un texto codificado que al ser leído por alguien que no sea el remitente o quien posea la clave de descifrado, no le será posible entender lo que dice el mensaje. Se clasifica en técnicas simétricas y asimétricas, dependiendo del funcionamiento de las claves, siendo esencial para la seguridad en la sociedad moderna y diversas aplicaciones digitales.

Los algoritmos criptográficos de clave simétrica emplean una única clave criptográfica tanto para cifrar el texto plano como para descifrar el texto cifrado. En este método, todos los destinatarios del mensaje necesitan poseer acceso a la misma clave compartida para el cifrado simétrico. La criptografía asimétrica, o de clave pública, se basa en algoritmos que aprovechan problemas matemáticos difíciles de invertir. Un ejemplo es el problema de factorización, donde calcular N = p * q es fácil, pero recuperar p y q a partir de N es complicado. Un algoritmo común en este contexto es RSA, que utiliza una clave pública para cifrar y otra clave privada para descifrar. La clave pública se comparte ampliamente, mientras que la clave privada se mantiene en secreto, formando así un par de claves.

Técnicas de encriptación antiguas: Algoritmo César.

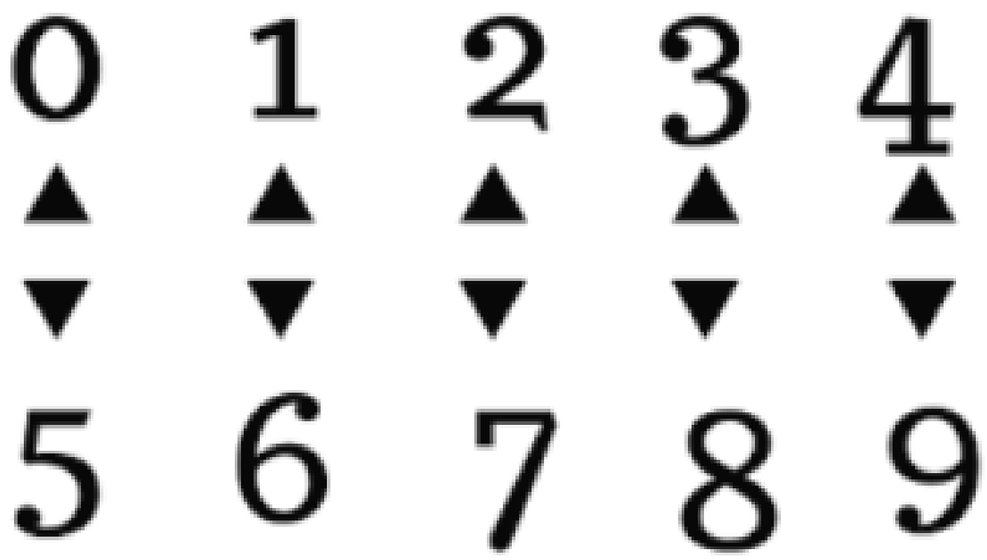
El cifrado César, nombrado en honor a Julio César, es una técnica simple y antigua de cifrado monoalfabético. Aunque es considerado débil debido a su fácil decodificación, a veces se incorpora en partes de esquemas de cifrado más complejos. Clasificado como un cifrado por sustitución, desplaza el alfabeto del texto plano por un número fijo. Sus ventajas incluyen su facilidad de uso y eficiencia en sistemas simples, pero presenta limitaciones debido a su estructura simple y proporciona seguridad mínima debido a patrones de letras predecibles.



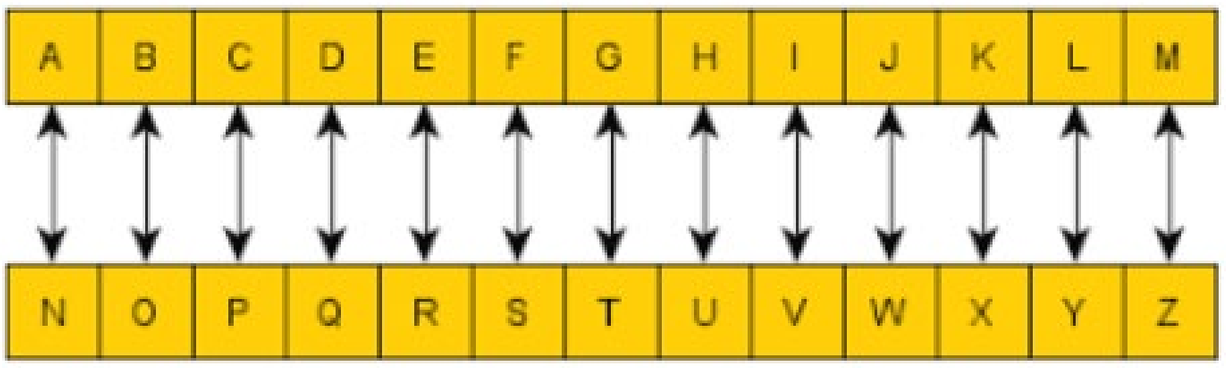
En la antigüedad, Julio César (100 a.C. 44 a.C.) utilizó un cifrado simple sustituyendo cada letra del alfabeto por otras tres posiciones adelante, conocido como cifrado César. En el siglo XIX, la sección de anuncios personales en periódicos se usaba para intercambiar mensajes cifrados, y el cifrado César ya estaba en uso en 1915, adoptado por el ejército ruso. Este cifrado, parte de los sustitutivos, es el más simple, con solo 25 combinaciones posibles. A menudo, se implementa en un dispositivo de rueda, donde dos alfabetos impresos se alinean, y su aplicación práctica incluye girar una rueda para lograr un desplazamiento específico al cifrar o descifrar letras.

Existen varios tipos de cifrados César, ahora vamos a ver algunos de ellos:

ROT5:
Los algoritmos ROT, como ROT5, son cifras de desplazamiento simples diseñadas para ocultar texto en lugar de proporcionar seguridad criptográfica. Un ejemplo de uso sería publicar la solución de un rompecabezas en línea. Al codificar la solución con ROT, garantizas que los lectores que accidentalmente lean tu mensaje no descubran la solución. En el caso de ROT5, se enfoca en codificar los números del 0 al 9.

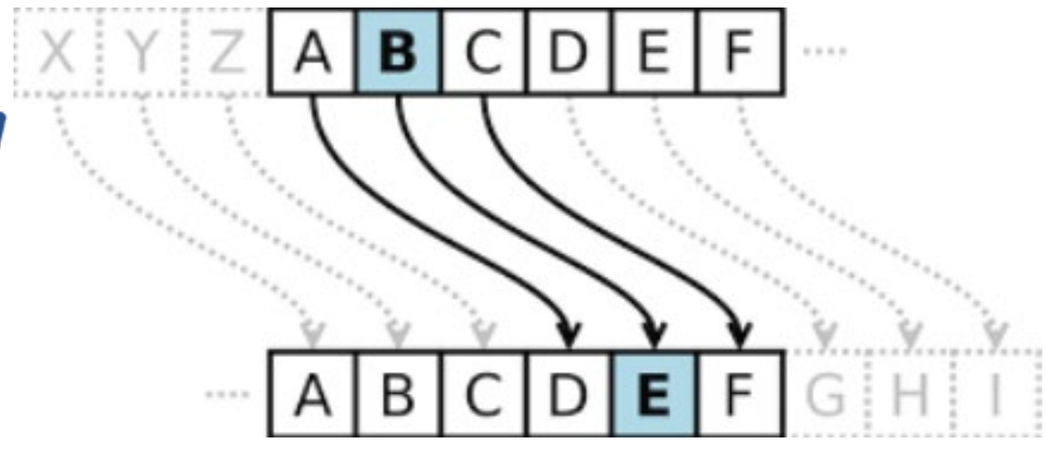


ROT13: Es un método de cifrado de sustitución de letras simple que opera reemplazando cada letra en un mensaje con la letra que se encuentra 13 posiciones adelante en el alfabeto. Por ejemplo, 'a' se reemplazaría por 'n', 'b' por 'o', y así sucesivamente. A diferencia de otros cifrados, ROT13 es auto inverso, lo que significa que el mismo código se puede utilizar tanto para codificar como para decodificar. Además, no codifica números ni puntuación.



ROT47: El cifrado ROT47, abreviatura de "Cifrado César por 47 caracteres", es una forma simple de sustitución de caracteres que reemplaza un carácter en el rango ASCII con el carácter que está 47 posiciones después de él en la tabla ASCII. Este algoritmo es reversible, lo que significa que aplicar el mismo algoritmo dos veces recuperará el texto original. Derivado de ROT13, el ROT47 incluye letras y símbolos mixtos, haciendo que el texto codificado parezca más evidente que ha sido cifrado.

César 4: Implica sustituir cada carácter por el que se encuentra cuatro posiciones después en el alfabeto, siendo un método poco seguro ya que es fácilmente descifrable probando cambios simples.



César 9: En el caso de Cifrado César 9, se aplica la misma lógica, sustituyendo cada letra por la que está nueve posiciones adelante en el alfabeto.

Descifrar el Cifrado César, aunque fue efectivo en la antigua Roma, es actualmente uno de los códigos más fáciles de descifrar. Se puede realizar un ataque de fuerza bruta probando todos los cambios posibles o utilizando análisis de frecuencia para identificar letras comunes en el cifrado. Si se trata de un Cifrado César con clave, los métodos pueden complicarse, pero siguen siendo relativamente accesibles..

Cifrado Vigenère.

El cifrado de Vigenère es un método para cifrar texto alfabético mediante la sustitución polialfabética. En este cifrado, se utiliza una tabla de Vigenère, que consiste en alfabetos escritos 26 veces en diferentes filas, cada uno desplazado cíclicamente respecto al anterior. Durante el proceso de encriptación, se elige un alfabeto específico de acuerdo con una palabra clave repetitiva. El descifrado implica encontrar la posición de la letra cifrada en la fila correspondiente a la clave y utilizar la etiqueta de la columna para obtener el texto original. Este método proporciona una capa adicional de complejidad en comparación con el cifrado César convencional.

En la siguiente imagen se puede apreciar la base de este cifrado:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y

La efectividad del cifrado César y otros cifrados de sustitución ha disminuido significativamente debido a su vulnerabilidad frente al análisis de frecuencia. Estos cifrados mantienen las distribuciones de caracteres del texto original, lo que facilita la identificación de letras comunes, como la letra 'E'. En el caso del cifrado César, que establece un mapeo uno a uno entre letras del texto sin formato y cifrado, descifrarlo mediante análisis de frecuencia implica descubrir la asignación de cada letra.

El cifrado César ya no se considera efectivo para cifrar textos secretos, ya que la tecnología actual permite romperlo en pocos minutos. El uso de pistas contextuales y datos de frecuencia, junto con las debilidades inherentes de estos cifrados, hace que sean vulnerables a métodos de descifrado más avanzados.