CURSO
BLOCKCHAIN

Módulo 1

Conceptos Informáticos

CURSO
BLOCKCHAIN

Conceptos Informáticos básicos (1h 40m)

1) Sistemas Numericos: Decimal, Binario, Hexadecimal
2) Matemáticas: Logica, funciones.
3) Algoritmo: Instrucciones, Memoria.
4) Criptografia: Simetrica, Asimetrica, Hash
5) Ciberseguridad: Privacidad, Integridad, relación con la criptografía.
6) Ejemplos: Firma Electrónica, Certificados SSL, Comunicación cifrada extremo a extremo (WhatsApp), Hash para la integridad de datos.
7) Ataques: defacement, DOS, Web spoofing, redes sociales, Personificaciones de emails, phishing, malwares para robo de claves, Man in the Middle, Inyecciones, Extensiones corruptas.

CURSO BLOCKCHAIN

Sistemas Numericos

Entendiendo sistema binario

Sistema decimal

¿Cual es el último numero?

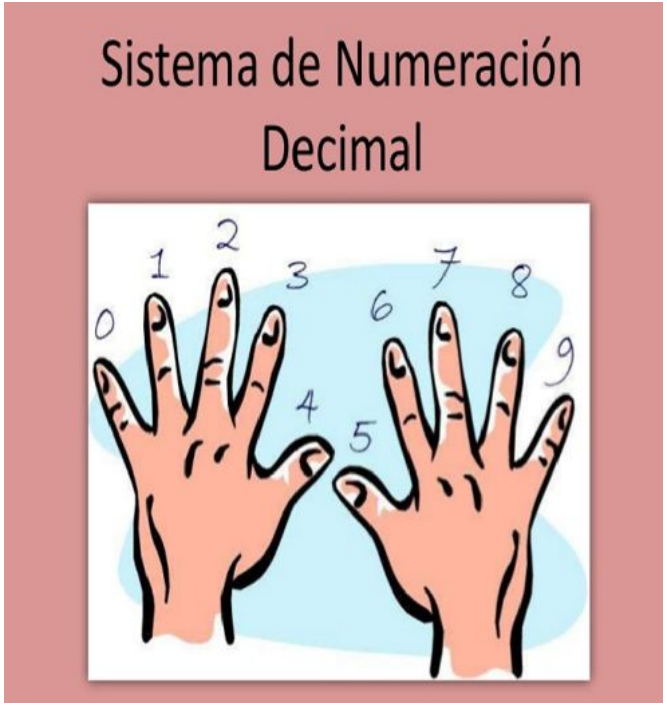
9

¿Con que numero sigo cuando llego al último?

10

¿A que valor representa el 10?

10



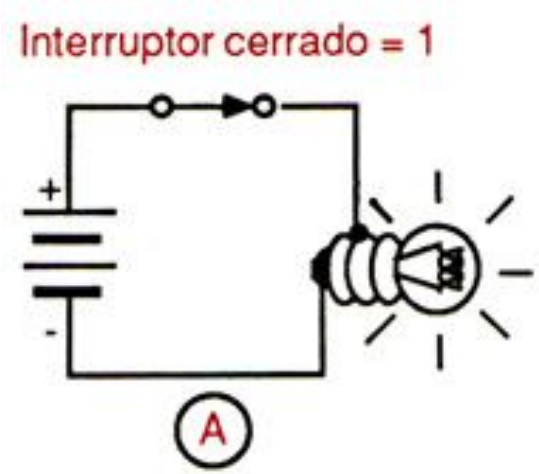
CURSO BLOCKCHAIN

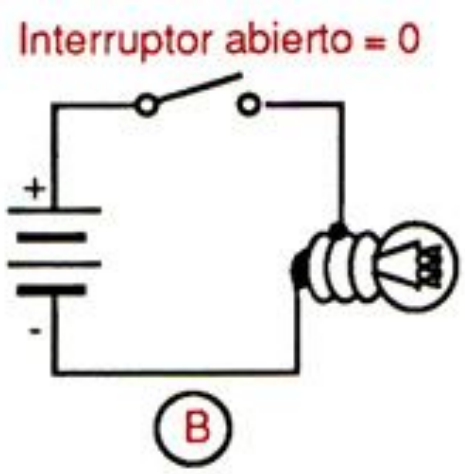
Sistema Binario

Ultimo numero= 1

Siguiente = 10

BIT= **B**inary dig**IT**



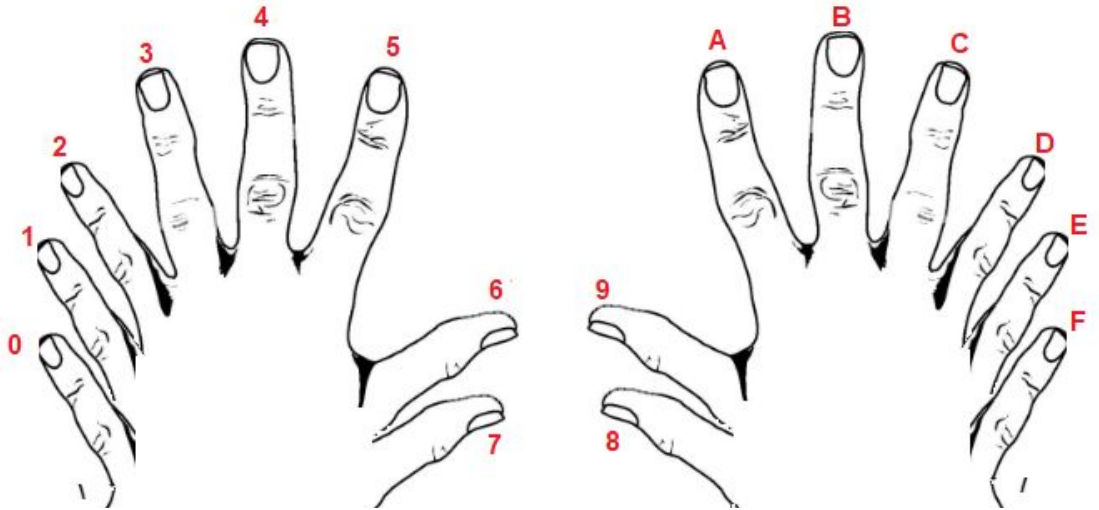


CURSO BLOCKCHAIN

Sistema Hexadecimal

¿Como seguimos contando más allá de F?

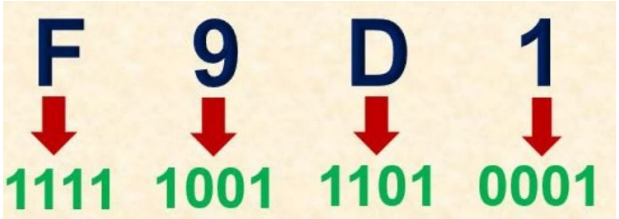
10



Porque sistema octal y sistema hexadecimal

Es una forma de compactar la expresión binaria. Cualquier número exponencial de 2 (binario) serviría ⇒ 2 (binario), 4(muy corto y no se usa), 8(sistema octal), 16(sistema hexadecimal 0-9+A-F), 32 (Deberíamos usar todo el abedecedario y la compactación sería minima, solo 1bit más que el hexadecimal, por lo que no se usa)

Hexadecimal-Binario (nibble)

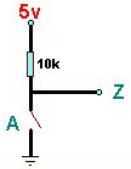
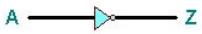
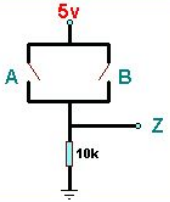
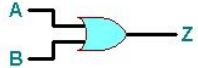
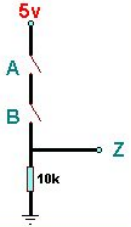
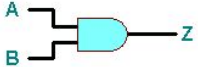
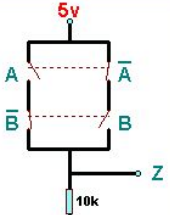
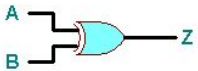


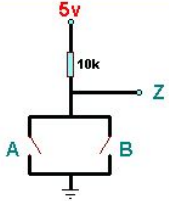
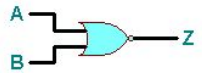
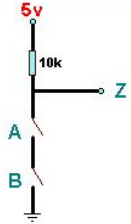
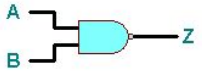
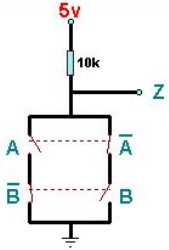
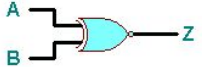
Octal Binario

Codificacion ascii ⇒ C => 0100 0001 = 0x41 = 65 💡💡💡💡

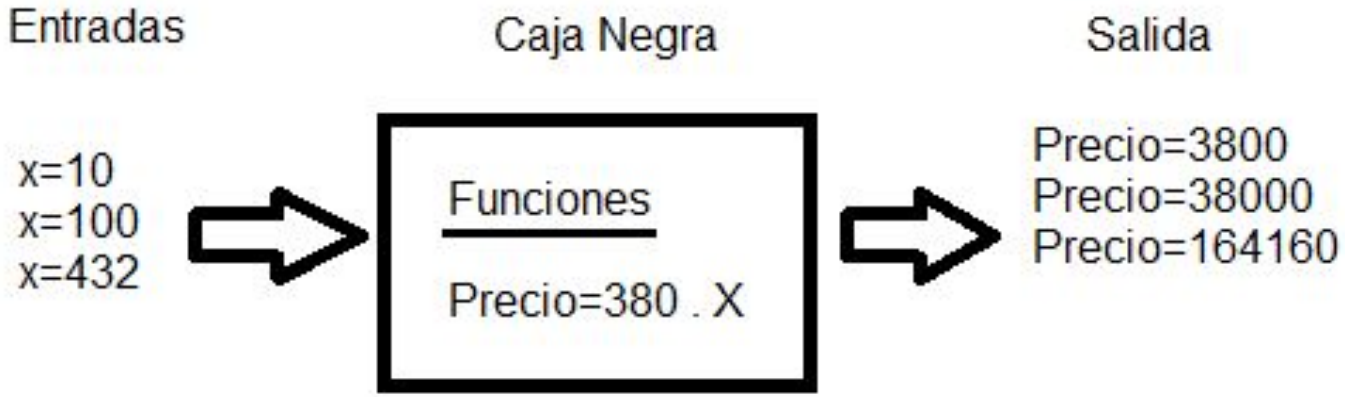
CURSO BLOCKCHAIN

Matemática Binaria (Lógica)

Función	Tabla de verdad	Con interruptores	Con compuertas
NOT $Z = \overline{A}$	A Z 0 1 1 0		
OR $Z = A + B$	A B Z 0 0 0 0 1 1 1 0 1 1 1 1		
AND $Z = A \cdot B$	A B Z 0 0 0 0 1 0 1 0 0 1 1 1		
XOR $Z = A \oplus B$ $Z = \overline{A \odot B}$	A B Z 0 0 0 0 1 1 1 0 1 1 1 0		

Función	Tabla de verdad	Con interruptores	Con compuertas
NOR $Z = \overline{A + B}$	A B Z 0 0 1 0 1 0 1 0 0 1 1 0		
NAND $Z = \overline{A \cdot B}$	A B Z 0 0 1 0 1 1 1 0 1 1 1 0		
XNOR $Z = A \odot B$ $Z = \overline{A \oplus B}$	A B Z 0 0 1 0 1 0 1 0 0 1 1 1 $Z = A \cdot B + \overline{A} \cdot \overline{B}$		

Funciones


Entradas
Caja Negra
Salida
x=10
x=100
x=432
Funciones
Precio=380 . X
Precio=3800
Precio=38000
Precio=164160

Arquitectura de Computadora

Algoritmos: Secuencia de instrucciones o procedimientos para alcanzar algún fin.
Ejemplo anterior:

1) Recibo un valor en dolares en una variable X
2) Multiplico la variable X por 380 (El precio del dolar).
3) Entrego el resultado para su lectura.

Memoria: Este algoritmo o procedimiento necesita guardarse en una memoria y que no se borre nunca porque sino perdemos el programa (ROM). Las Variables que yo le ingresé y el precio que me muestra también necesitan guardarse en una memoria pero que pueden borrarse cuando ya no lo use (RAM)

Quiz

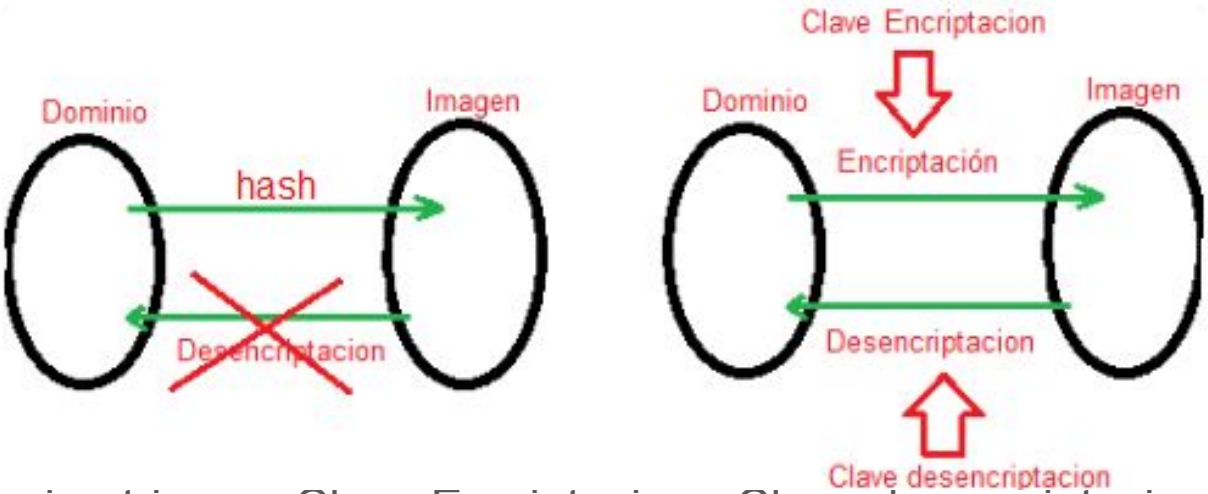
Si les digo que estoy pensando un numero del 1 al 999 y que tienen solo una oportunidad para adivinarlo. ¿Que número es?

CURSO
BLOCKCHAIN

Criptografía

Introducción

Criptografía



simetrica => Clave Encriptacion= Clave desencriptacion

Asimetrica => Clave Encriptacion != Calve desencriptacion (ECDSA)

Hash => Salida fija (Normalmente) usado como firma (Keccak)

Encriptación asimétrica

Supongo clave privada= 3 y 33

Supongo clave publica= 7 y 33

Mensaje a encriptar= X= 9

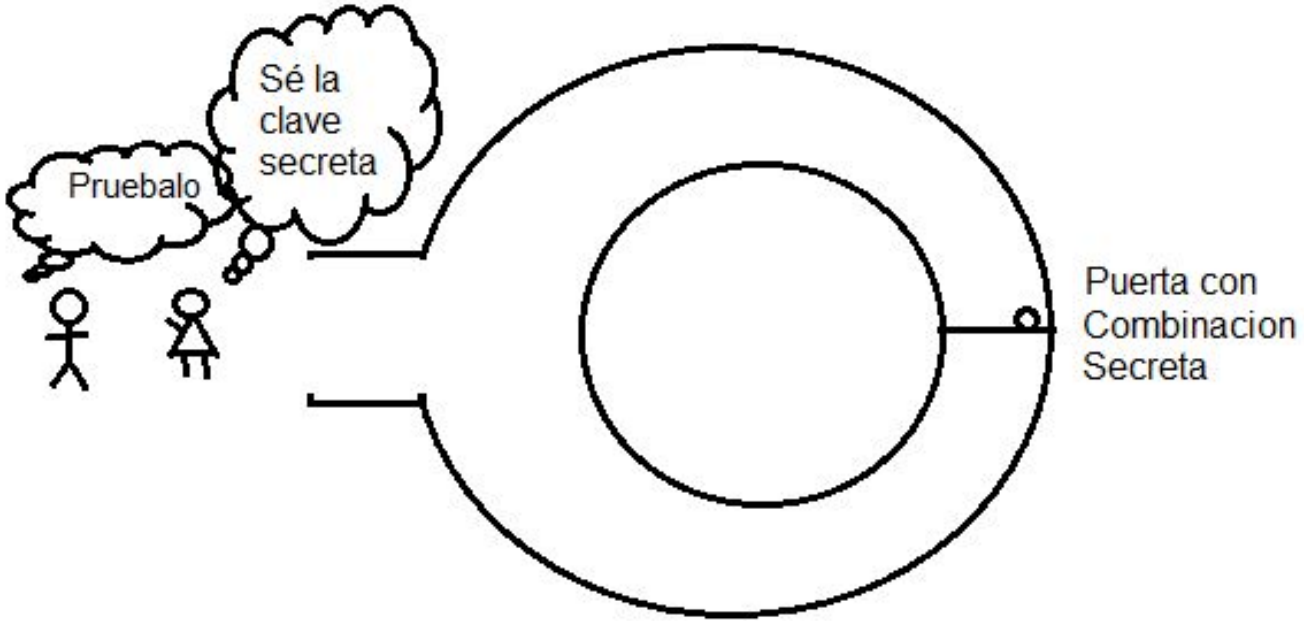
y = 9^3 mod 33 = 3 (3 es mi mensaje encriptado)

Ahora para desencriptar no hacemos la inversa, Usamos la clave publica

X= 3^7 mod 33 = 9 (volvemos a obtener nuestro mensaje que era 9)

Un procedimiento similar es ocurrirá con la curva eliptica, solo que partiremos de una clave privada y encontraremos una pública como la multiplicación de esta por un punto generador G. Las multiplicaciones encima no serán tradicionales sino elípticas.

Prueba de conocimiento cero (ZK proof)



Seguridad Informática

Privacidad

Editor	Lector	Tipo
Yo	yo	Simetrica
Yo	Todos	Asimetrica
Todos	Yo	Asimétrica
Todos	Todos	Nada
Todos	Nadie	Hash
Nadie	-	Absurdo

Integridad

HASH

Pregunta

Cuál es la diferencia entre un hash (keccak) y una encriptación asimétrica (ECDSA)?

Ataques Informáticos1

1) Defacement: Modificar contenido de un sitio. Puedo desprestigiar o modificar su flujo de visitas. (En web3 puedo vicular smart contracts maliciosos)
2) DOS: Denial of Service. Genera muchos llamados a su servidor para saturar su funcionamiento. SI el atacante previamente logra controlar varias computadoras usando virus puede ejecutarla desde todos esos puntos e intensificar el efecto. (En web3 podemos sacar de su vida útil un smart contract)
3) Phishing: Envío de mensajes fraudulentos haciéndose pasar por una entidad para obtener los datos de las personas. (En web3, las claves privadas o mnemonicos)
4) Web Spoofing: Imitación de una web para obtener datos. (En web3 puedo hacer que la usen y vincularla a smart contracts maliciosos)

Ataques Informáticos 2

1) Redes Sociales: Los atacanetes pueden buscar redes sociales no utilizadas por las empresas para personificarlas, difamarlas o redirigir a sus victimas a web spoofing o realizar phishing.
2) Malwares: virus, gusanos, troyanos, ransomware (Encripta memoria y luego piden rescate en BTC), spyware (roba claves).
3) MiM: Man in the middle. En conexiones de internet publicas, un hacker puede interceptar los datos de internet que una persona manda o recibe. Muchas veces los hacker generan redes con nombres similares a redes públicas para confundir a la gente y que caigan en sus redes y así robar información. (Wallets, bancos en un celular solo con internet privado o en su defecto datos moviles. No redes publicas).
4) Inyecciones: Violaciones de integridad en las bases de datos, pudiendolas borrar, consultar o modificar los datos en ella si no está correctamente programada.

Ataques informáticos 3

1) Extensiones corruptas: Extensiones poco conocidas o similares a las originales, pueden contener código malicioso capaz de modificar websites haciendo defacement, modificar datos que uno copia y así enviar dinero a direcciónes no deseadas, etc.

2) **fuerza bruta=** Consiste en probar toda la combinatoria y encriptarla hasta que los hashes coincidan.
3) **Rainbow tables=** Son bases de datos que ya contienen billones de pares mensaje/encriptación. Son las más usadas para romper passwords comunes como 1234, admin, probando, etc.
4) **Ingeniería social=** Cualquier técnica que al hacker se le ocurra para explotar al eslabón débil de la cadena “el usuario”.

Bibliografía

Understanding Cryptography (Christof Paar)

SHA3 and the hash function keccak (Christoph Paar)

https://impulsomatematico.com/2019/10/16/numeros-primos-como-encriptar-y-desencriptar-mensajes-con-ellos-y-algunas-otras-curiosidades/

https://learndigital.withgoogle.com/activate/course/cybersecurity-remote-work

Resumen

1) Encriptar: Volver ilegible algo y el proceso inverso es desencriptar
2) Clave privada: clave que solo yo debo conocer y según el uso me va a servir para encriptar cosas o desencriptarlas.
3) Clave Publica: Clave que cualquiera puede tener derivada de mi clave privada pero de la cual no podemos deducir la clave privada y que según el uso servirá para encriptar o desencriptar mensaje.
4) Hash: Palabra de una determinada longitud que siempre es constante en cantidad de caracteres y que varía si le cambio el contenido a hashear.
5) Seguridad Informática: Encargada de proteger privacidad e integridad de los datos
6) Bits: cada digito en un sistema numérico binario.

Consultas

¿?

Reto

https://cursoblockchain.com.ar/

Contrato

Esta carta de contrato estipula la relación entre Pablo y María para el mantenimiento de una residencia. Pablo se compromete a ofrecer sus servicios de limpieza y mantenimiento de la residencia a cambio de una compensación monetaria mensual. María está obligada a pagar la cantidad acordada dentro de los primeros 5 días laborables de cada mes. Ambos acuerdan cumplir con estas obligaciones durante un periodo de 12 meses.

Actividad

1) Integridad
   a) Crear un Hash del contrato y anotarlo
   b) Cambiar algún dato del contrato
   c) Aplicarle el hash nuevamente y comparar con el primero.
   d) Cuales conclusiones saca?

2) Autentificación

   a) Suponiendo que eres pablo, create un par de clave privada y publica para la firma.
   b) Firma el documento y pasale a María el documento, tu firma digital y tu clave publica.
   c) Siendo maría verifica que la firma de Pablo y el documento sea correcto.
   d) Que pasaría si maría intentara de firmar como pablo con la información que tiene de Pablo? Que es lo que Pablo nunca puede revelar.

3) Alternativo: Si pueden trabajar de a dos siendo Pablo y María y realizando las actividades 1 y 2 buscando alterar los datos, lograr la firma del otro sería la actividad ideal. Esto es similar al juego criptoanarquía que jugaban los cypherpunks, precursores del Bitcoin que ya estaremos hablando.