1. Algoritmo de Feistel.

el Cifrado de Feistel es un método de **cifrado en bloque** con una estructura particular. También es conocida como Red de Feistel o Cadena de Feistel. Gran número de algoritmos de cifrado por bloques lo utilizan, siendo el más conocido el algoritmo Data Encryption Standard (DES).

Ventaja: Las redes de Feistel presentan la ventaja de ser **reversibles** por lo que las operaciones de cifrado y descifrado son idénticas, requiriendo únicamente invertir el orden de las subclaves utilizadas.

Algoritmo: Este algoritmo se denomina simétrico por rondas, es decir, realiza siempre las mismas operaciones un número determinado de veces (denominadas rondas). Los pasos de la red de Feistel son:

- Se selecciona una cadena, N, normalmente de 64 o 128 bits, y se la divide en dos subcadenas, L y R, de igual longitud (N/2)
- Se toma una función, F, y una clave Ki
- Se realizan una serie de operaciones complejas con F y Ki y con L o R (solo uno de ellas)
- La cadena obtenida se cambia por la cadena con la que no se han realizado operaciones, y se siguen haciendo las rondas.

2. Algoritmos DES, 3DES.

DES (Data Encryption Standard) es un **esquema de encriptación simétrico.** Se basa en un sistema monoalfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones. DES **utiliza** una **clave simétrica de 64 bits**, de los cuales 56 son usados para la encriptación, mientras que los 8 restantes son de paridad, y se usan para la detección de errores en el proceso.

3DES: Triple DES se le llama al algoritmo que hace triple cifrado del DES. También es conocido como TDES o 3DES. Cuando se descubrió que una clave de 56 bits no era suficiente para evitar un ataque de fuerza bruta, TDES fue elegido como **forma de agrandar el largo de la clave** sin necesidad de cambiar de algoritmo de cifrado. La **longitud de la clave** usada será de **168 bits** (3x56 bits), aunque su eficacia sólo sea de 112 bits. Se continúa cifrando bloques de 64 bits.

Usos de Triple DES: la mayoría de las **tarjetas de crédito** y otros **medios de pago electrónicos** tienen como estándar el algoritmo Triple DES

3. Algoritmos AES, IDEA.

Advanced Encryption Standard (AES), es un **esquema de cifrado por bloques** adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. AES tiene un **tamaño de bloque fijo de 128 bits** y **tamaños de llave de 128, 192 o 256 bits.** La mayoría de los cálculos del algoritmo AES se hacen en un campo finito determinado. AES opera en una matriz de 4×4 bytes, llamada state.

IDEA: International Data Encryption Algorithm es un **cifrador por bloques.** IDEA fue utilizado como el cifrado simétrico en las primeras versiones de PGP (PGP v2.0). IDEA **opera con bloques de 64 bits** usando **una clave de 128 bits** y consiste de ocho transformaciones idénticas (cada una llamada un ronda) y una transformación de salida (llamada media ronda). El proceso para cifrar y descifrar es similar. Gran parte de la seguridad de IDEA deriva del intercalado de operaciones de distintos grupos — adición y multiplicación modular y O-exclusivo (XOR) bit a bit — que son algebraicamente "incompatibles" en cierta forma.

IDEA utiliza tres operaciones en su proceso con las cuales logra la confusión, se realizan con grupos de 16 bits y son:

- Operación O-exclusiva (XOR) bit a bit (indicada con un $\oplus$ azul)
- Suma módulo 216 (indicada con un cuadrado verde)
- Multiplicación módulo 2^{16} +1, donde la palabra nula (0x0000) se interpreta como 2^{16} (indicada con un círculo rojo)

4. RSA, El Gammal, Massey Omura.

RSA: (Rivest, Shamir y Adleman). Es un **sistema criptográfico de clave pública** desarrollado en 1979. Es el primer y **más utilizado algoritmo** de este tipo y es **válido tanto para cifrar como para firmar digitalmente. La seguridad** de este algoritmo **radica en el problema de la factorización de números enteros**. Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto. **El algoritmo consta de tres pasos: generación de claves, cifrado y descifrado.**

Se parte de dos números primos grandes (p, q) y su producto n=p*q. Calculemos también el número F=(p-1)(q-1). El número n es público, pero p y q no lo son. La clave pública e será un número tal que F y e sean primos relativos. Con “primos relativos” queremos decir que no tengan divisores comunes, es decir, que su máximo común divisor sea uno. Mientras que la clave privada d es un número que cumpla que e*d mod F = 1; se dice en este caso que d es el inverso (multiplicativo) de e módulo F. No siempre existe el inverso multiplicativo, y la condición necesaria para que exista inverso es que los números e y F sean primos relativos.

El Gammal: **Es un algoritmo,** procedimiento o esquema de cifrado **basado en problemas matemáticos de logaritmos discretos.** Usado en la criptografía asimétrica. El Gamal consta de tres componentes: el generador de claves, el algoritmo de cifrado, y el de descifrado. En las **firmas digitales** que es muy utilizado, un tercero puede **falsificar firmas si encuentra la clave secreta** x del firmante **o** si encuentra **colisiones en la función de Hash** . Se considera que ambos problemas son suficientemente difíciles. El firmante debe tener cuidado y **escoger una clave** diferente de forma uniformemente **aleatoria para cada firma.** Así asegura que clave o aún información parcial sobre la clave no es deducible. **Malas selecciones de claves** pueden **representar fugas de información** que facilitan el que un atacante deduzca la clave secreta.

Sin embargo, en la actualidad, el algoritmo de computación de logaritmos discretos es subexponencial con una complejidad de $\lambda = 1/3$, la misma que la de factorizar dos números primos, y por tanto, incapaz de realizar tal tarea en números grandes en un tiempo razonable.

Massey Omura: **Utiliza exponenciación en campos de Galois GF(2n) para encriptar y desencriptar.** Esto es E(e,m)=me y D(d,m)=md donde los cálculos son realizados en cuerpos finitos de característica dos. Para cualquier exponente e con 0<e<2n-1 y mcd(e,2n-1)=1, el correspondiente exponente de desencriptación es d tal que de $\equiv 1 \pmod{2n-1}$. Dado que el grupo multiplicativo del cuerpo GF(2n) tiene orden 2n-1, por el teorema de Lagrange se tiene que mde=m para todo m en GF(2n).

Cada elemento del cuerpo finito GF(2n) está representado como un vector binario sobre una base normal; se cumple que que cada vector de la base es el cuadrado del vector precedente. Esto significa que los vectores de la base son v1, v2, v4, v8, ... donde v es un elemento del cuerpo de orden máximo, es decir 2^n-1.

5. Algoritmos criptográficos de curvas elípticas. y2= x3 + ax + b, 8a3 + 27 b2 <>0

6. Propiedades de las curvas elípticas.

- Es una **variante de la criptografía asimétrica** o de clave pública basada en las matemáticas de las curvas elípticas.
- Elliptic Curve Digital Signature Algorithm es una **modificación del algoritmo DSA**.
- Se definen mediante ecuaciones cúbicas (de tercer grado).
- Han sido utilizadas para probar el último teorema de Fermat y en factorización de enteros.
- Las curvas elípticas son regulares, es decir, no tienen vértices ni autointersecciones.
- La definición formal de una curva elíptica es la de una curva algebraica proyectiva no singular sobre K de género 1.

- El hecho de que requiere claves más pequeñas que otros sistemas de clave pública lo hacen un buen candidato para aplicaciones donde los requisitos de tamaño de memoria son más exigentes, como por ejemplo en sistemas de identificación mediante tarjetas.
- Mecanismo alternativo para distribución de claves.
- Requiere claves de longitud menor que las RSA.

7. Curvas elípticas mod m.

8. Soluciones de curvas elípticas mod m.

9. Aplicaciones de las curvas elípticas

Curvas elípticas en criptografía

Criptografía de clave pública. La idea de clave pública. Sistema de cifrado RSA. Criptografía basada en grupos.
Curvas elípticas. Ley de adición. Curvas elípticas sobre campos finitos. Teorema de Hasse. Implementación de curvas elípticas.
Criptosistemas de curva elíptica. Análogos de los criptosistemas Diffie-Helman, ElGamal y DSA. Comparando la curva elíptica con otros tipos de criptografía. Curva elíptica del problema de logaritmo discreto.
Escoger los parámetros del sistema criptográfico. Selección de un campo finito subyacente y una curva elíptica apropiada. Algoritmos para determinar el orden del grupo.
Otras aplicaciones de las curvas elípticas. Método de factorización de la curva elíptica de Lenstra. Algoritmo de prueba de primalidad de curva elíptica.

Curvas elípticas de alto rango.

Curvas elípticas sobre los racionales. Teorema de Mordell. Teorema de Mazur. Conjetura de abedul y Swinerton-Dyer.
Subgrupo de Torsión. Teorema de Lutz-Nagell. Construcción de curvas con torsión prescrita.
Construcción de curvas elípticas con alto rango. El método polinomial de Mestre. Método de campo finito. Cálculo del rango.
Curvas de alto rango con torsión prescrita. Resultados de Kulesz, Campbell y Womack. Aplicación de m-tuplas diofánticas.

10. Robustez de las claves de curvas elípticas.

NIST y ANSI X9 han establecido unos requisitos mínimos de tamaño de clave de 1024 bits para RSA y DSA y de 160 bits para CCE

11. Criptomoneda

Es un medio digital de intercambio, el cual mediante criptografía fuerte asegura las transacciones financieras, controlar la creación de unidades adicionales y verificar la transferencia de activos. Son un tipo de divisa alternativa y de moneda digital. Además tienen un control descentralizado, en contraposición a las monedas centralizadas y a los bancos centrales.
El control descentralizado de cada moneda funciona a través de una base de datos descentralizada, usualmente una cadena de bloques, que sirve como una base de datos de transacciones financieras pública.

12. El dilema de los generales bizantinos

El problema de los generales bizantinos (PGB) es un experimento mental para plantear, de una forma metafórica, el problema que se da entre un conjunto de sistemas informáticos que tienen un objetivo común. Deben encontrar un plan de acción común a partir de una estructura jerárquica, donde uno de los sistemas que tiene mayor rango proporciona una orden a partir de la cual el resto de sistemas tiene que operar. Se trata además de un problema clásico de las redes distribuidas como Bitcoin y otras criptomonedas.
El "Problema de los Generales Bizantinos" (PGB) ilustra cómo funciona el algoritmo de consenso conocido como "Proof of Work" y que es en fondo un protocolo que evita que se hagan ataques DDoS o spam a la red de Bitcoin.
El concepto de "Proof of Work" nace previo al Bitcoin. Fue pensado originalmente como método para evitar el spam por email.

Principio de desconfianza mutua

El principio de desconfianza mutua se basa en el problema de los generales bizantinos, este principio analiza problema de los generales bizantinos, en el cual problema se presenta como una analogía con un escenario de guerra, donde un grupo de generales bizantinos se encuentran acampados con sus tropas alrededor de una ciudad enemiga que desean atacar. Después de observar el comportamiento del enemigo los generales deben comunicar sus observaciones y ponerse de acuerdo en un plan de batalla común que permita atacar la ciudad y vencer. Para ello, los generales se comunican únicamente a través de mensajeros. Además, existe la posibilidad que algunos de los generales sean traidores y, por lo tanto, decidan enviar mensajes con información errónea con el objetivo de confundir a los generales leales. Un algoritmo que solucione el problema debe asegurar que todos los generales leales acuerdan un mismo plan de acción y que unos pocos traidores no pueden conseguir que el plan adoptado por los generales leales sea equivocado.
A partir del problema de los generales bizantinos se busca la mejor solución para una comunicación segura. Uno de los grandes logros que supone Bitcoin, más allá de ser la primera criptomoneda con una aceptación extendida por todo el mundo, es el hecho de ofrecer la primera solución práctica al problema de los generales bizantinos.

13. Registro y validación distribuidos: mineros.

Un registro distribuido es una forma de base de datos digital que es actualizada y mantenida por cada miembro de manera independiente en un gran espacio de red. En este tipo de registro no hay ninguna autoridad central para transmitir los registros a cada miembro.
En su lugar, todos los nodos mantendrán el registro y lo construirán de forma independiente. Pero en ese caso, los nodos de la red deberán tener acceso a las listas de transacciones y dar su propia conclusión antes de agregarla al registro distribuido.
Después del acuerdo, el registro distribuido se actualiza, y todos los nodos de la red actualizarán también su propio registro. El sistema hace que la arquitectura general de la interfaz sea bastante compleja en comparación con los sistemas de bases de datos típicos.
Los registros distribuidos vienen con un sistema dinámico especial que pueden superar las capacidades de los sistemas típicos de registros basados en papel. En resumen, con diferentes tipos de DLT, podrás formar nuevas tecnologías y habilitar la seguridad en todo el mundo digital.
Por lo general, en este tipo de sistemas típicos, siempre hay una cuestión de confianza. Sin embargo, esta nueva DLT está introduciendo un nuevo tipo de tecnología que elimina los problemas de "confianza" y construye todo sobre la transparencia total.
Con esta nueva invención del sistema de registro distribuido, ahora puedes experimentar la revolución de la recopilación de información y comunicarte más allá de las formas tradicionales. Puedes aplicarlo tanto a datos dinámicos como a esquemas de datos estáticos.
Los registros distribuidos simplemente devuelven el poder a tus manos. trata más de administrar todo el sistema que de una simple base de datos.
El minado de bloques consiste en la realización de una serie de complejos cálculos que requieren tiempo y (cada vez más) electricidad, pero cuando el proceso esos bloques quedan registrados de forma permanente en esa cadena de bloques, y no pueden ser modificados sin que se alteren todos los bloques.

14. Blockchain, cadenas de bloqueo, validación y trazabilidad.

Un blockchain es un gigantesco libro de cuentas en los que los registros (los bloques) están enlazados y cifrados para proteger la seguridad y privacidad de las transacciones. Es, en otras palabras, una base de datos distribuida y segura (gracias al cifrado) que se puede aplicar a todo tipo de transacciones que no tienen por qué ser necesariamente económicas.

Esa cadena de bloques tiene un requisito importante: debe haber varios usuarios (nodos) que se encarguen de verificar esas transacciones para validarlas y que así el bloque correspondiente a esa transacción se registre en ese gigantesco libro de cuentas.

Jeff Garzik recomienda que los CIO planifiquen una implementación blockchain en cuatro etapas para su validación:

Etapa 1: Identificar un caso de uso y asignar un plan tecnológico. La elección de casos de uso adecuados es fundamental.

Etapa 2: Crear una prueba de concepto.

Etapa 3: Realizar una prueba de campo que implique un ciclo de producción limitado con datos orientados al cliente y, a continuación, realizar pruebas adicionales con productos y volúmenes de datos más orientados al cliente.

Etapa 4: Realizar un despliegue de volumen completo en la producción.

La trazabilidad se refiere a la posibilidad de conocer el origen de un producto y poder seguir su curso a lo largo de su cadena de transformación y distribución. Las reglas de la trazabilidad están definidas por normas emitidas por organismos de control nacionales o internacionales y varían según la naturaleza de las mercancías.

En la Supply Chain, la blockchain ofrece múltiples ventajas. Permite a las partes interesadas ganar eficiencia operativa, pero también mejorar su imagen de marca.

15. Bitcoin y otras criptomonedas

Bitcoin es una moneda, como el euro o el dólar estadounidense, que sirve para intercambiar bienes y servicios. Sin embargo, a diferencia de otras monedas, Bitcoin es una divisa electrónica que presenta novedosas características y destaca por su eficiencia, seguridad y facilidad de intercambio.

Su mayor diferencia frente al resto de monedas, se trata de una moneda descentralizada, por lo que nadie la controla. Bitcoin no tiene un emisor central como los dólares o los euros, la criptomoneda es producida por las personas y empresas de alrededor del mundo dedicando gran cantidad de recursos a la minería.

Entre sus características principales están:

- No hay intermediarios: Las transacciones se hacen directamente de persona a persona.
- Es imposible su falsificación o duplicación gracias a un sofisticado sistema criptográfico.
- Las transacciones son irreversibles.
- No es necesario revelar tu identidad al hacer negocios y preserva tu privacidad.
- El dinero te pertenece al 100%; no puede ser intervenido por nadie ni las cuentas pueden ser congeladas.

Entre otras monedas tenemos el peerCoin que fue la moneda digital en combinar la prueba de estado y la prueba de trabajo, consume menos energía, lo que quiere decir que no hay un número exacto monedas, o sea, se pueden crear ilimitadamente a diferencia de las Bitcoin que se estima que solo puedan existir 21 millones.

Ripple

Este sistema usa un protocolo distinto a las altcoins funcionando también como cambio de moneda distribuido, un sistema de pago y una moneda.

Dogecoin

Contrario a Bitcoin, esta moneda cuenta con un bloque de tiempo de 1 minuto y no existe un límite a la cantidad de Dogecoin que pueden ser creadas lo que convierte a esta criptomoneda en la forma de pago ideal para realizar pequeñas transacciones financieras.

16. Protección con blockchain

Las blockchains están protegidas por una variedad de mecanismos, entre los que se incluyen técnicas avanzadas de criptografía y modelos de comportamiento y toma de decisiones matemáticos (teoría de juegos y criptomonedas).

17. El internet del Valor

El Internet del valor también se ha creado sobre estándares abiertos pero encuentra su base en la tecnología Blockchain. el Internet del valor tenemos una herramienta nueva para compartir y gestionar valor de activos o bienes digitales sin la necesidad de depender de una entidad central de confianza que centralice el proceso.

El internet del valor que nos trae Blockchain se define a través de los tokens o activos digitales que representan derechos sobre bienes y/o servicios que pueden ser objeto de comercio. En este nuevo internet se puede intercambiar valor a través de estos tokens, como por ejemplo a través de las criptomonedas que son un tipo de token.

18. Dinero Digital

Se refiere al dinero que se emite de forma electrónica, a través de la utilización de una red de ordenadores, Internet y sistemas de valores digitalmente almacenados como el caso del Bitcoin. Es decir es un medio de pago digital equivalente de una determinada moneda.

19. Números extendidos

Teorema 1.1 Si un número primo divide el producto de dos enteros, entonces debe dividir al menos uno de esos números enteros.

Podemos considerar que nuestros enteros extendidos son todos los números de la forma $m + n\sqrt{10}$, donde m y n son enteros ordinarios. Dichos enteros extendidos pueden sumarse, restarse, multiplicarse e incluso dividirse utilizando la igualdad.

$$\frac{a+b\sqrt{10}}{m+n\sqrt{10}} = \frac{a+b\sqrt{10}}{m+n\sqrt{10}} \times \frac{m-n\sqrt{10}}{m-n\sqrt{10}}$$

$$= \frac{a \times m - 10b \times n + (b \times m - a \times n)\sqrt{10}}{m^2 - 10n^2}.$$

Tiene sentido decir que $m + n\sqrt{10}$ es un divisor de $a + b\sqrt{10}$ si y sólo si su relación es otro entero extendido. Así, $2 + \sqrt{10}$ es un divisor de $12 + 3\sqrt{10}$ porque:

$$\frac{12+3\sqrt{10}}{2+\sqrt{10}} = \frac{-6-6\sqrt{10}}{-6} = 1+\sqrt{10}.$$

Ahora se puede hablar de indivisibles en este sistema de enteros extendidos. En el ejercicio 1.2 se muestra que los números 2, $4+\sqrt{10}$ y $4-\sqrt{10}$ son indivisibles. Los llamo indivisibles y no primos porque no satisfacen el teorema 1.1:

$$(4+\sqrt{10}) \times (4-\sqrt{10}) = 6,$$

que es divisible por 2 y, sin embargo, 2 no divide ni $4+\sqrt{10}$ ni $4-\sqrt{10}$.

Las dos primeras aplicaciones del Teorema 1.1 usan el caso especial donde los dos enteros son iguales. Si un p primo divide a^2, entonces debe dividir a. Por lo tanto, si p divide a^2, entonces p^2 divide a^2.

20. Teorema fundamental de la aritmética

El teorema fundamental de la Aritmética o teorema de factorización única afirma que todo entero positivo mayor que 1 es un número primo o bien un único producto de números primos.

Teorema 1.4 (Teorema fundamental de la aritmética) La factorización en números primos es única hasta el orden.
Lo que esto dice es que puede haber varias formas de ordenar los números primos que entran en una factorización:

$$\begin{aligned} 30 &= 2 \times 3 \times 5, \text{or} \\ &= 3 \times 5 \times 2, \end{aligned}$$

pero no podemos cambiar los números primos que entran en la factorización. En nuestros enteros extendidos de la forma $m+n\sqrt{10}$ esto no es cierto. Como ejemplo, 6 tiene dos factorizaciones distintas en indivisibles:

$$\begin{aligned} 6 &= 2 \times 3 \\ &= (4+\sqrt{10}) \times (4-\sqrt{10}). \end{aligned}$$

Sea n un entero con factorización no única:

$$\begin{aligned} n &= p_1 \times p_2 \times \cdots \times p_r \\ &= q_1 \times q_2 \times \cdots \times q_s, \end{aligned}$$

donde los números primos no son necesariamente distintos, pero donde la segunda factorización no es simplemente una reordenación de la primera. El primo q_1 divide n y por lo tanto divide el producto del p_1's. Mediante la aplicación repetida del Teorema 1.1, hay al menos una p_i que es divisible por q_1. Si es necesario, reordenar los p_i para que q_1 divida p_1. Dado que p_1 es primo, q_1 debe ser igual a p_1.Esto dice que:

$$\begin{aligned} \frac{n}{q_1} &= p_2 \times p_3 \times \cdots \times p_r \\ &= q_2 \times q_3 \times \cdots \times q_s. \end{aligned}$$

Dado que las factorizaciones de n eran distintas, estas factorizaciones de $\frac{n}{q_1}$ también deben ser distintas. Por lo tanto, $\frac{n}{q_1}$ es un divisor adecuado de n con factorización no única.

21. Criba de eratóstenes, propiedades.

La criba de Eratóstenes es un algoritmo que permite encontrar todos los números primos menores o iguales a un entero n dado.
Para encontrar todos los números primos menores o iguales a n, enumeramos todos los enteros de 2 a n. Luego nos abrimos paso en la lista. El primer entero (es decir, 2) debe ser primo. Marcamos todos los múltiplos de 2 que son más grandes que 2. El primer entero después de 2 que no ha sido tachado (es decir, 3) debe ser primo. Tachamos todos los múltiplos de 3 que son mayores que 3. Continuamos de esta manera. Cuando hemos encontrado un nuevo número primo, tachamos todos los múltiplos de ese nuevo número primo que son más grandes que el número primo en sí y luego pasamos al siguiente entero que no se ha tachado y que debe ser primo nuevamente.Una vez que hemos encontrado un primo más grande que la raíz cuadrada de n, todos los enteros restantes que no se han tachado deben ser primos. Si alguno de ellos fuera compuesto, tendrían que tener un factor menor o igual a su raíz cuadrada.
Si:

$$n = a \times b \text{ then } a \leq \sqrt{n} \text{ or } b \leq \sqrt{n}.$$

22. Números pseudoprimos: números de mersenas, números perfectos
Números Pseudoprimos

Si n es impar y compuesto y n satisface $2^{n-1} \equiv 1 \pmod{n},$ Entonces decimos que n es una pseudoprima.

números de Mersena

Un primo de Mersenne es un primo de la forma M (n) para algún entero n.

$$M(n) = 2^n - 1.$$

Por lo tanto, 3, 7, 31 y 127 son los primeros cuatro primos de Mersenne.

Número perfecto

Se dice que un entero positivo es perfecto si es la suma de sus divisores apropiados (esos divisores positivos son estrictamente menores que ellos mismos).

$$\begin{aligned} 6 &= 1+2+3, \\ 28 &= 1+2+4+7+14, \\ 496 &= 1+24+8+16+31+62+124+248, \end{aligned}$$

23. Pseudoprimos fuertes: pruebas de primalidad fuerte.

Pseudoprimos fuertes:

Se dice que un entero impar n es un pseudoprimo fuerte para la base b si es compuesto, relativamente primo a b, y divide uno de los factores en el lado derecho de la Ecuación:

$$b^{n-1} - 1 = (b^t - 1) \times (b^t + 1) \times (b^{2t} + 1) \times (b^{4t} + 1) \times \cdots \times (b^{2^{a-1} \times t} + 1),$$

Pruebas Primaldad Fuerte

Sea m un número entero primo a n tal que m es un residuo cuadrático módulo p y no es un residuo cuadrático módulo q. (Dichos enteros m existen según el teorema del resto chino). Entonces n fallará en la prueba de pseudoprimo fuerte para la base m**.**

24. El algoritmos de Euclides

El algoritmo de Euclides es un método antiguo y eficiente para calcular el máximo común divisor (GCD)

La propiedad básica de este algoritmo es:

Dados dos enteros a y b; $b \neq 0$ existen enteros m y r tales que

$$a = m \times b + r, \quad \text{with} \quad 0 \leq r < |b|.$$

25. Factorización de números compuestos:

Los **números compuestos** son aquellos números que tienen más de dos divisores, es decir, aquellos números que no son números primos.

La **factorización** de un número consiste en expresar como productos de potencias de números primos.

26. Teorema de Fermat

El pequeño teorema de Fermat es uno de los teoremas clásicos de teoría de números relacionado con la divisibilidad, Se formula de la siguiente manera:.

Si p es un número primo, entonces, para cada número natural a, con $a>0$, $a^p \equiv a \pmod p$

Si p es un número primo, entonces, para cada número natural a, con $a>0$, coprimo con p , $a^{p-1} \equiv 1 \pmod p$

27. Teorema de Euler

Es una generalización del pequeño teorema de Fermat, y como tal afirma una proposición sobre la divisibilidad de los números enteros. El teorema establece que:

Si a y n son enteros primos relativos, entonces n divide al entero $a^{\varphi(n)} - 1$

Si a y n son enteros primos relativos, entonces $a^{\varphi(n)} \equiv 1 \pmod n$.

28. Teorema de Wilson

El teorema de Wilson es una proposición clásica vinculada con la divisibilidad y la primalidad de números enteros. A continuación, se presenta su enunciado:

Si p es un número primo, entonces $(p-1)! \equiv -1 \pmod p$

29. Teorema de Montgomery

Es una conjetura la cual dicta que la correlación de pares entre pares de ceros de la función zeta de Riemann es:

$$1 - \left(\frac{\sin(\pi u)}{\pi u}\right)^2 + \delta(u),$$

30. Teorema de Lenstra

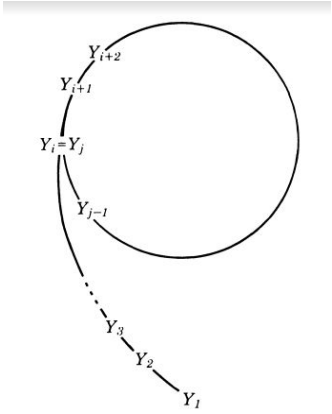
O el método de factorización de curva elíptica es un algoritmo de tiempo de ejecución rápido y sub-exponencial para la factorización de enteros, que emplea curvas elípticas. Para la factorización de propósito general.

Grupo Jeff

1. Pollard Rho, Pollard Rho-1

Pollard Rho

El origen del nombre del algoritmos se da a que la secuencia de Yi forma un círculo con una cola que se asemeja a la letra griega rho.



Precauciones con Pollard Rho:

- No se debe insertar al algoritmo un número primo solo números compuestos.
- Este algoritmo puede tardar mucho tiempo si se ingresa un número primo
- Por razones de seguridad y comodidad, es una buena idea que este programa se auto interrumpa de vez en cuando, digamos cada 1000 o 10000 ciclos
- Incluso si la entrada es compuesta, no hay garantía de que este algoritmo produzca la factorización en su vida.

Pollard Rho-1

Al igual que pollard rho asumimos que el número n que se debe factorizar es un número compuesto de una prueba de pseudoprima y no tiene ningún pequeño divisor.
El algoritmo pollard p-1 es una de las restricciones en los números primos pyq en el sistema criptográfico de clave pública RSA.

2. Funciones cuadráticas

Es una variable de una función polinómica definida por:

$$y = ax^2 + bx + c$$

con a diferente de 0. También se da el caso que se le llama Trinomio cuadrado perfecto.También se denomina función cuadrática a funciones definidas por polinomios cuadráticos de más de una variable, por ejemplo:

$$f(x, y) = Ax^2 + Bxy + Cy^2 + Dx + Ey + F$$

En este caso el conjunto de puntos que resultan al igualar el polinomio a cero representan lugares geométricos que siempre es posible reducir a una de las formas:

$$\left(\frac{x}{a}\right)^2 \pm \left(\frac{y}{b}\right)^2 = c^2, \qquad \left(\frac{x}{a}\right)^2 \pm \frac{y}{b} = c$$

3. Residuos Cuadráticos

Se denomina residuo cuadrático módulo m a cualquier entero r coprimo con m para el que tenga solución la congruencia:

$$x^2 \equiv r \pmod{m}$$

o lo que es lo mismo cuando r es un cuadrado no nulo módulo m, y que por lo tanto tiene una raíz cuadrada en la aritmética de módulo m. A los enteros que no son congruentes con cuadrados perfectos módulo m se les denomina no-residuos cuadráticos.

4. Símbolo de Legendre

Sea p un primo impar y n un entero. El símbolo de Legendre (n/p) se define como 0 si p divide n, +1 si n es un residuo cuadrático módulo p y -1 de lo contrario.

5. Símbolo de Jacobi

El símbolo de Jacobi, denotado como $(\frac{m}{n})$, es una función aritmética que toma dos argumentos y devuelve un valor entero comprendido en el intervalo [-1, 1].

Definición:
Sea n un entero y m cualquier entero impar positivo,

$$n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_r^{a_r},$$

donde los p_i son números primos impares que pueden repetirse. El símbolo de Jacobi $(\frac{m}{n})$ tiene el valor:

$$(m/n) = (m/p_1)^{a_1} \times (m/p_2)^{a_2} \times \cdots \times (m/p_r)^{a_r},$$

donde para todo i, pi es primo y ai es un número natural, denotando mediante (m/p_i) el símbolo de Legendre. Obviamente, cuando n es un número primo impar, el correspondiente símbolo de Jacobi se reduce al de Legendre.

6. Criba cuadrática

Es un algoritmo de factorización de enteros y, en la práctica, el segundo método más rápido conocido (después de la criba general del cuerpo de números). Su tiempo de ejecución únicamente depende el tamaño del entero a ser factorizado, y no sobre una estructura especial o propiedades.

En el algoritmo se define el tamaño máximo de la base y de los números aleatorios (-c,c). Los pasos son:

1. Debemos seleccionar una base de números que son residuo cuadrático de n, para hacer esto solo debemos aplicar el algoritmo de Jacobi, este algoritmo devolverá 1 si es residuo cuadrático y -1 si no lo es. Se seleccionara los números hasta el rango indicado por ejemplo si el rango es 30 se escogerán los números que cumplen ser residuo cuadrático hasta ese número.
2. Debemos sacarle la raíz cuadrada al número n.
3. Obtenemos un vector de números x tales que será la suma de la raíz cuadrada más el rango de aleatorios.
4. Encontraremos un vector de números tales que será la función de x , donde elevaremos a x al cuadrado y restamos el número.
5. A este vector de f(x) seleccionaremos solo los que son lisos(suaves), en otras palabras los que su factorización en números de la base cumplen con el rango de números, le asignaremos a cada factor que cumple el número de su exponente y al que no cero.
6. A la matriz anterior obtenida le sacaremos módulo 2 para obtener solo una matriz binaria.
7. Escogeremos las filas de la matriz que cumple que su suma en módulo 2 da cero.
8. En los vectores de x multiplicaremos a todos los números que cumplieron el paso anterior y sacaremos módulo 2 obteniendo una variable X.
9. En los vectores de f(x) multiplicaremos a todos los números que cumplieron el paso 7 y obtendremos una variable Y^2 y le sacaremos la raíz para obtener Y.
10. obtenidos X y Y sacaremos el máximo común divisor de X+Y con n y obtendremos un factor no trivial de n, y sacamos también el máximo común divisor de X-Y con n y se obtendrá el otro factor no trivial estos dos factores será los factores de n.

Ejemplo:
Factorizar n=87453
Sea B=30 el máximo rango de números de la base
Sea (–C,C)= (-35,35) el rango de números aleatorios
Pasos
1. Encontramos los números que son residuo cuadrático de n.

P	2	3	5	7	11	13	17	19	21	23	29
Jacobi(p,n)	1	1	-1	-1	-1	1	1	1	-1	-1	1

2. m=$\sqrt{}$n, m= 295
3, 4 ,5, 6. Donde obtendremos esta matriz de números lisos

x	f(x)	-1	2	3	13	17	19	29
265	-17238	1	1	1	0	1	0	0
278	-10179	1	0	1	1	0	0	1
296	153	0	0	0	0	1	0	0
299	1938	0	1	1	0	1	1	0
307	6786	0	1	0	1	0	0	1
316	12393	0	0	0	0	1	0	0

7: Una posible solución que cumple que su suma sea cero es fila 3 y fila 6.

x	f(x)	-1	2	3	13	17	19	29
296	153	0	0	0	0	1	0	0
316	12393	0	0	0	0	1	0	0

8: X=296*316 = 6073
9: Y^2 = 153*12393, Y= 1377

10: mcd(X-Y,n)= 587 y mcd(X+Y,n)= 149
Para verificación 587*149= 87463

7. Criba cuadrática multi polinomial

En la criba cuadrático básica utilizamos un polinomio de la forma $g(x) = (x+b)^2 - n$ donde $b = \lceil \sqrt{n} \rceil$. El problema con el uso de un solo polinomio es que los valores de g(x) aumentan a medida que x aumenta, lo que hace que sea menos probable que sean suaves. Finalmente, el algoritmo "se queda sin gas" cuando los valores de g(x) crecen demasiado.

La sugerencia de Montgomery fue utilizar múltiples polinomios de la forma $g_{a,b}(x) = (ax+b)^2 - n$ con a, b enteros con 0 <b ≤ a. La gráfica de $g_{a,b}(x)$ es una parábola, y sus valores serán más pequeños cuando $a \approx \sqrt{(2n)}/m$. Por lo tanto, elegimos b para que $b^2 - n$ sea divisible por a, digamos $b^2 - n$ = a c para algún entero c, y $a = q^2$ para algún entero q. Luego calculamos $g_{a,b}(x) / a = a\,x^2 + 2\,bx + c$, y, después de cribar sobre el rango −m .. m, cuando $g_{a,b}(x)$ es uniforme sobre la base de factores, registramos la relación $((ax + b)\,q^{-1})^2 = a\,x^2 + 2\,bx + c$.

8. Aproximación a números irracionales por el método de fracciones continuas

Una fracción continua es una expresión de la forma:

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{a_5 + \dots}}}}$$

donde a1 es un número entero y los ai son números naturales. A estas fracciones continuas a veces se las llama simples para distinguirlas de aquellas que tienen numeradores distintos de uno, a las que se llama fracciones continuas generalizadas. A los números ai se les llama elementos o, también, cocientes incompletos.

Euler demostró que todo número racional puede expresarse mediante una fracción continua finita y que todo número irracional puede expresarse mediante unas fracción continua infinita.

- Sea n un número natural que no sea cuadrado perfecto.

$$n = m^2 + a \implies \sqrt{m^2 + a} = m + x \iff x = \frac{a}{2m + x}$$

$$\boxed{\sqrt{n} \sim m + \cfrac{a}{2m + \cfrac{a}{2m + \dots}}}$$

- Por ejemplo: $\sqrt{7} \sim 2 + \cfrac{3}{4 + \cfrac{3}{4 + \dots}} \sim [2; 1, 1, 1, 4, 1, 1, 1, 4, \dots]$

9. Algoritmo de fracciones continuas

Algoritmo 6 Fracciones continuas

La ***entrada*** es un número impar N, una cota C.
La ***respuesta*** es p y q.

PASO 1 Iniciamos con: $m_0 = a_0 = \lfloor \sqrt{N} \rfloor$, $x_0 = \sqrt{N} - a_0$ y $b_0 \equiv a_0^2 \pmod N$.
PASO 2 Para $i = 1, \dots,$ hacer
$a_i = \lfloor 1/x_{i-1} \rfloor, x_i = (1/x_{i-1}) - a_i$.
Si $i = 1$ entonces $m_i = a_0 a_1 + 1$ y $b_i \equiv m_i^2 \pmod N$.
En otro caso $m_i = a_i m_{i-1} + m_{i-2}$ y $b_i \equiv m_i^2 \pmod N$.
Descartar los b_i que tienen factores primos mayores a C. De los restantes elegimos algunos valores de b_i tales que sus factores primos aparezcan un número par de veces, para encontrar una congruencia $\prod m_i^2 \equiv \prod p_i^2 \pmod N$.

10. Criptoanálisis por fracciones continuas

El método de fracciones continuas fue desarrollado por Morrison y Brillhart en 1970 lo que les permitió factorizar el séptimo número de Fermat F7 = 22 7 + 1. Para poder comprender un poco mejor este método de factorización se recordarán algunos conceptos relacionados con el tema. Cualquier n´umero real x puede representarse por fracciones continuas de la forma siguiente:

$$x = a_0 + \cfrac{z_1}{a_1 + \cfrac{z_2}{a_2 + \cfrac{z_3}{a_3 + \dots}}}$$

Nótese que x es racional si y sólo si su fracción continua es finita. El número racional

$$\frac{m_i}{n_i} = [a_0, \dots, a_i]$$

se llama el i-ésimo convergente de x. Se tiene que x es el límite de la sucesión de racionales mi/ni y de hecho proporcionan una aproximación óptima a x en el sentido de que los denominadores son primos relativos [6]. El numerador y el denominador se pueden obtener recursivamente de la siguiente forma:

$$\begin{aligned}
\frac{m_0}{n_0} &= \frac{a_0}{1} \\
\frac{m_1}{n_1} &= \frac{a_0 a_1 + 1}{a_1} \\
&\vdots \\
\frac{m_i}{n_i} &= \frac{a_i m_{i-1} + m_{i-2}}{a_i n_{i-1} + n_{i-2}}, \quad i \geq 2
\end{aligned}$$

Una vez calculada la fracción continua simple se procede en el algoritmo a calcular el valor de mi/ni , el i-ésimo convergente de $\sqrt{\ }$ N y se calcula bi $\equiv$ m2 i (mod N). De los valores bi resultantes sólo se tomarán aquellos cuyos factores primos sean menores a una cota C, el valor máximo de la cota usualmente usado es de 10000, claro que esto depende del valor que se desea factorizar pues un número de 20 dígitos puede ser factorizado con una cota no menor a 3000, pero entre mayor sea la cota utilizada el Algoritmo 6 tardará un poco más en obtener la factorización del número.

11. Pruebas de primalidad por fracciones continuas

Se pueden usar los siguientes algoritmos:

Aproximación a la raíz cuadrada de dos:

si un entero no es un cuadrado perfecto, entonces su raíz cuadrada no es racional. Sin embargo, los únicos números que podemos calcular son los números racionales. Los griegos tropezaron con una manera rápida y precisa de aproximarse a la raíz cuadrada de 2 que fue descrita por Theon of Smyrna en el siglo II A. D. y es casi seguro que es mucho mayor.

Algorithm 10.1 *This approximates the square root of 2 to within an error of less than* $1/2n^2$.

```
INITIALIZE:      READ n
                 a ← 1
                 b ← 1

MYSTERY_LOOP:    WHILE b < n DO
                       b ← a + b
                       a ← 2 × b - a

TERMINATE:       WRITE a/b
```

Por ejemplo si n=5000

$$
\begin{aligned}
1/1 &= 1 \\
3/2 &= 1.5 \\
7/5 &= 1.4 \\
17/12 &= 1.416\,666\,66\ldots \\
41/29 &= 1.413\,793\,10\ldots \\
99/70 &= 1.414\,285\,71\ldots \\
239/169 &= 1.414\,201\,18\ldots \\
577/408 &= 1.414\,215\,68\ldots \\
1393/985 &= 1.414\,213\,19\ldots \\
3363/2378 &= 1.414\,213\,62\ldots \\
8119/5741 &= 1.414\,213\,55\ldots,
\end{aligned}
$$

También se puede utilizar el Algoritmo de Bháscara Brouncker

Este algoritmo sirve para representar aproximaciones a raíces cuadradas, por ejemplo la raíz cuadrada de 13:

$$
\begin{aligned}
\sqrt{13} = 3.6055512\ldots &= 3 \times 1 + 0.6055512\ldots \\
1 &= 1 \times 0.6055512\ldots + 0.3944487\ldots \\
0.6055512\ldots &= 1 \times 0.3944487\ldots + 0.2111025\ldots \\
0.3944487\ldots &= 1 \times 0.2111025\ldots + 0.1833461\ldots \\
0.2111025\ldots &= 1 \times 0.1833461\ldots + 0.0277563\ldots \\
0.1833461\ldots &= 6 \times 0.0277563\ldots + 0.0168079\ldots \\
0.0277563\ldots &= 1 \times 0.0168079\ldots + 0.0109484\ldots \\
0.0168079\ldots &= 1 \times 0.0109484\ldots + 0.0058594\ldots.
\end{aligned}
$$

```
INITIALIZE:     READ n
                sqrt ← ⌊√n⌋
                A1 ← sqrt
                B0 ← 0; B1 ← sqrt
                C0 ← 1; C1 ← n - sqrt × sqrt
                P0 ← 1; P1 ← sqrt
                Q0 ← 0; Q1 ← 1
                i ← 1

MYSTERY_LOOP:   WHILE Ci ≠ 1 DO
                    k ← i - 1
                    j ← i
                    i ← i + 1
                    Ai ← ⌊(sqrt + Bj)/Cj⌋
                    Bi ← Ai× Cj - Bj
                    Ci ← Ck + Ai× (Bj - Bi)
                    Pi ← Pk + Ai× Pj
                    Qi ← Qk + Ai× Qj

TERMINATE:      WRITE Pi, Qi, i
```

Test de Primalidad:
Se pueden usar los números de mersenne para poder probar la primalidad de las fracciones continuas, es necesario aplicar el algoritmo de Lucas Lehmer, el cual propone que toda potencia par es congruente con 1 mod 3 $M(n) = 2^n - 1$, es decir, si no cumple con esta propiedad el número no es primo.

12. Propiedades de los números extendidos.

Estos números se utilizan en las secuencias de Lucas
Llamaremos enteros extendidos. Como ejemplo, podemos considerar que nuestros enteros extendidos son todos los números de la forma m + raiz(10), donde m y n son enteros ordinarios. Dichos enteros extendidos pueden sumarse, restarse, multiplicarse e incluso dividirse utilizando la igualdad.

13. Aplicación de los números extendidos en las cribas cuadráticas.

Los números extendidos son utilizados en la implementación de la criba de fracciones continuas para su resolución.

14. Secuencias de Lucas

$x_n = P\,x_{n-1} + Q\,x_{n-2}$ Son ciertas sucesiones de enteros que satisfacen la relación de recurrencia. Comienza con 1,3 (en lugar de 1,1 como la de fibonacci) y cada elemento se calcula como la suma de los dos previos.
lucas=[1,3];

n	$U_n(P,Q)$	$V_n(P,Q)$
0	0	2
1	1	P
2	P	$P^2 - 2Q$
3	$P^2 - Q$	$P^3 - 3PQ$
4	$P^3 - 2PQ$	$P^4 - 4P^2Q + 2Q^2$

```
var limite=20;
secLucas(2);
alert ("Sec Lucas:"+lucas); //1,3,4,7,11,18,29,47, ...
function secLucas(n){
```

```
if (n<=limite) {
    lucas[n]=lucas[n-1]+lucas[n-2];
    secLucas(n+1)}}
```

15. Curvas Elípticas

Curvas elípticas surge de la aritmética de las curvas elípticas. Considera la ecuación: $y^2 = x^3 + ax + b,$ Esto simplemente garantiza que la ecuación cúbica $z = x^3 + ax + b,$ Tiene tres raíces distintas. La ecuación solo se puede resolver para y cuando el lado derecho es positivo, y luego y es simplemente + o - la raíz cuadrada del lado derecho. Si la Ecuación tiene tres raíces reales, Esta curva tiene la curiosa propiedad de que, si una línea no vertical la intersecta en dos puntos, también tendrá un tercer punto. de intersección. Se considera que una tangente a la curva tiene dos puntos de intersección en el punto de tangencia. Podemos calcular el punto de intersección adicional utilizando el siguiente lema. Se calcula el tercer punto de la siguiente manera $\lambda = \frac{y_1 - y_2}{x_1 - x_2}.$

16. Pruebas de primalidad con curvas elípticas

Es un algoritmo de propósito general, lo que significa que no depende de que el número sea de una forma especial. Actualmente, ECPP es en la práctica el algoritmo más rápido conocido para probar la primalidad de los números generales, pero se desconoce el tiempo de ejecución en el peor de los casos. La ECPP corre heurísticamente en el tiempo:

$$O((\log n)^{5+\varepsilon})$$

La prueba de primalidad de curva elíptica ofrece una alternativa a la prueba de primalidad de Pocklington, que puede ser difícil de implementar en la práctica.

1. Criptoanálisis con curvas elípticas

Cuando en el año 1985 se propuso el uso del grupo de puntos de una curva elíptica, la razón principal fue que para él no existía un ataque análogo al Index Calculus (Algoritmo probabilístico para el logaritmo discreto). Desprovistos de esta técnica criptoanalítica, capaz de resolver el PLD (Problema del Logaritmo Discreto) en tiempo subexponencial en el grupo multiplicativo de un cuerpo finito, la complejidad del problema pasaba a ser a priori exponencial en el grupo de puntos de una curva elíptica. Gracias a ello los criptosistemas basados en curvas elípticas pueden ofrecer el mismo nivel de seguridad que sus análogos en cuerpos finitos utilizando claves de longitud mucho más corta. El hecho de que existan numerosas curvas diferentes con cardinal similar puede ser también considerado como una ventaja adicional.

Muchos investigadores han tratado sin éxito extender el método del Index Calculus a las curvas elípticas. No obstante, el hecho de que dicho ataque no pueda ser utilizado no garantiza que no exista ningún otro algoritmo capaz de resolver el Problema del Logaritmo Discreto Elíptico en un tiempo inferior al exponencial. De hecho, las curvas elípticas están dotadas de una cierta estructura que convierte, a algunas más que a otras, en blancos potenciales para el diseño de algoritmos eficientes para la resolución del PLDE.

2. Cuerpos de números

En criptografía las operaciones de cifra se realizan dentro de un cuerpo de cifra o módulo. En teoría de números estas operaciones en un cuerpo se les denomina congruencias y se representan por el signo ≡. Así, la expresión a ≡ b mod n significa que a es congruente con b módulo n.

3. Criptoanálisis con la criba de cuerpo numérico

En la actualidad, algunas versiones de GNFS han conseguido factorizar claves RSA de 512 bits, y el siguiente paso, las claves de 1024 están siendo objetivo de futuras factorizaciones, no muy lejanas. La empresa de seguridad Laboratorios RSA sigue confiando en las claves de 1024 para uso corporativo, pero si es necesario extremar la seguridad de ciertos datos, nos recomiendan ya usar tamaños de clave de 2048. Esto quiere decir que no en mucho tiempo, ya sean nuevas mejoras en las implementaciones de GNFS o con nuevos algoritmos de factorización, se podrá comprometer la seguridad de las claves de uso corporativo. GNFS, al igual que la Criba Cuadrática, es altamente paralelizable, basándose en los principios de búsqueda de elementos válidos sobre un intervalo de criba.

4. La conjetura de Riemann

La hipótesis de Riemann es una afirmación, no demostrada, que hace referencia a los ceros de la función zeta de Riemann. Bernhard Riemann calculó los seis primeros ceros no triviales de esta función y observó que todos estaban sobre una misma recta. En una memoria publicada en 1859, Riemann comentó que este podría muy bien tratarse de un hecho general. La hipótesis de Riemann afirma que todos los ceros no triviales de la función zeta se encuentran en la recta x = 1/2. Más de diez billones de ceros calculados hasta hoy, todos alineados sobre la recta crítica, corroboran la sospecha de Riemann, pero nadie aún ha podido probar que la función zeta no tenga ceros no triviales fuera de esta recta.

5. Aplicaciones de Blockchain para protección de valor

Además de Bitcoin, las aplicaciones de Blockchain en el sistema financiero involucran:

- **Proteger y agilizar:** pagos, transferencias y envíos de remesas, lo que lleva al abaratamiento de los costos de estos servicios.
- **Mercados de valores:** un ejemplo de protección de en este campo en es la bolsa de valores Nasdaq, una de las mayores del mundo.
- **Mercados de predicción descentralizados:** un ejemplo es Augur, un mercado de predicción descentralizado que permite a sus usuarios comprar y vender acciones anticipándose a un suceso en base a la probabilidad de que se produzca uno u otro desenlace.

Aparte del sistema financiero, Blockchain se puede utilizar para protección de valor en:

- ***Gestión de identidades***

La tecnología blockchain **permite a los usuarios crear su propia identidad digital (especie de ID) a prueba de manipulación.** Con esta ID podremos acceder a aplicaciones y sitios web, firmar documentos digitales, etc. Algunas **compañías que ofrecen este tipo de servicios** son Onename, Keybase o ShoCard.

- ***Registro y Verificación de Datos***

Blockchain se puede utilizar para **almacenar cualquier otro tipo de información, generando así un registro distribuido inalterable**, mucho más seguro que las bases de datos tradicionales. Alguna empresas que ofrecen este tipo de servicios son Tierion, Proof of Existence o Factom.
Algunos **sectores empresariales** en los que sería útil este tipo de registro y verificación son:

- Clínicas y Hospitales.
- Registro de la propiedad.
- Registro de Vehículos.
- Protección de la propiedad intelectual.
- Incluso se podría crear un registro internacional de antecedentes penales.

6. Usos de blockchain.

- ***Finanzas y Economía***

La aplicaciones financieras de la cadena de bloques son múltiples: automatización de transferencias, pagos de rentas de alquiler o creación de exchanges.

- ***Fintech y banca***

La unión de las **fintech y el blockchain** es ya algo relativamente común. Por otro lado, las ventajas que ofrece el **blockchain a la banca** reside en la automatización del proceso, que elimina intermediarios y comprobaciones manuales y se traduce en una reducción considerable de costes.
Un **ejemplo de aplicación blockchain en la banca es el Banco Santander**, que ya lo usa para realizar transferencias internacionales ultrarrápidas.

- ***Big Data***

Las herramientas que ofrece el Big Data permiten analizar todos los datos de una cadena de bloques (blockchain) y obtener información muy útil para empresas.

- ***Servicios de Notaría***

Blockchain permitir crear registros inmutables y hacer un seguimiento de un documento o una cadena de sucesos, eliminando la necesidad de que una autoridad centralizada o tercero lo certifique.

- ***Lógica y Transporte***

Compañías como Provenance.Org, SkuChain o Everledger utilizan la tecnología blockchain para hacer seguimientos y garantizar la procedencia de distintos productos.

- ***Internet de las Cosas IoT***

La tecnología blockchain permite el intercambio de datos de forma segura y fiable al tiempo que elabora un registro inmutable de todos los mensajes intercambiados entre los diferentes dispositivos inteligentes conectados.

- ***Ejecución automática de contratos***

Programas de software que recogen los términos de un contrato entre las partes y se almacenan en la blockchain. Se autoejecutan cuando se cumplen las condiciones especificadas en el propio contrato.

- ***Seguridad Automatizada***

La combinación de las identidades digitales basadas en la blockchain con los contratos inteligentes y las cerraduras electrónicas del Internet de las cosas, permitirá también crear sistemas de seguridad automatizados que garanticen o impidan el acceso a algo.

- ***Votar por Internet***

La blockchain puede garantizar que una persona no pueda votar más de una vez en una misma elección, al tiempo que garantiza la privacidad de su voto.

7. Construcción de los registros distribuidos con blockchain

Blockchain significa cadena bloques, una cadena de bloques que contiene información. Un bloque tiene específicamente 3 cosas: la información que almacena el bloque, su código y el código del bloque anterior. En blockchain cada bloque tiene un lugar específico e inamovible dentro de la cadena. La cadena completa se guarda en cada nodo de la red que conforma la blockchain, por lo que se almacena una copia exacta de la cadena en todos los participantes de la red (**registro distribuido**).

A medida que la información aumenta, surge la necesidad de almacenarla en un nuevo bloque. Cuando el bloque está listo para añadirse a la cadena, un conjunto de nodos especiales llamados mineros intentan resolver un problema matemático complejo. El primero que lo consigue notifica la solución para que el resto de nodos verifiquen la correctitud de la solución, y en caso de ser correcto el bloque se añade a la cadena. Una vez el bloque se añade, todos los nodos de la red sincronizan sus copias de la cadena de manera que todos tengan el mismo **registro distribuido**.

8. Aplicación de los algoritmos de hash sah256 y ripemd160 en blockchain.

El algoritmo de Hash SHA256 está directamente relacionado con el minado de bloques. Cuando los mineros de blockchain están seguros que una transacción es válida, pueden ponerla en un bloque junto con muchas otras transacciones e intentar minar el bloque. Esto se hace poniendo el bloque a través del algoritmo SHA-256. La salida debe comenzar con una cierta cantidad de 0 para que se considere válida. La cantidad de 0 necesarios depende de lo que se denomina la "dificultad", que cambia según la potencia informática que haya en la red.

Al igual que SHA256, RIPEMD160 es un algoritmo de hash utilizado para el proceso de minado en blockchain con la ventaja de que produce los hashes más cortos cuya singularidad todavía está suficientemente asegurada.

9. Criptomonedas: Bitcoin.

Es un protocolo y red P2P que se utiliza como criptomoneda, sistema de pago y mercancía. Su unidad de cuenta nativa se denomina bitcóin. Esas unidades son las que sirven para contabilizar y transferir valor por lo que se clasifican como moneda digital. Concebida en 2009, se desconoce la identidad última de su creador o creadores, apareciendo con el seudónimo de Satoshi Nakamoto. Se sustenta en la tecnología de «cadena de bloques», difícilmente falsificable y semejante a un gran libro contable, público y distribuido, en el que queda reflejado el histórico de todas las transacciones.
Bitcoin se caracteriza por ser descentralizado, es decir, no está respaldado por ningún gobierno o banco central. Utiliza un sistema de prueba de trabajo para impedir el doble gasto (que un mismo bitcoin sea utilizado varias veces) y alcanzar el consenso entre todos los nodos que integran la red intercambiando información sobre una red no fiable y potencialmente comprometida.

10. Diferencias conceptuales entre bitcoin, Ethereum y Ripple.

Bitcoin comparado con Ethereum

1. cantidad de decimales que pueden utilizarse para dividir cada una de estas monedas: Mientras que Bitcoin permite dividir hasta con 8 decimales, Ethereum permite usar hasta 18.
2. Ambos sistemas utilizan algoritmos protegidos por criptografía pero se trata de protocolos diferentes: Bitcoin utiliza un algoritmo llamado SHA-256d, y el de Ethereum se denomina EtHash.
3. Para confirmar y validar un bloque a la cadena Bitcoin necesita aproximadamente 10 minutos mientras que Ethereum realiza esta tarea en tan solo 10 segundos. Además la recomepsan por minado es permanente en el caso de Ethereum mientras que en Bitcoin presenta una tendencia descendente.
4. Otra diferencia sustancial es la cantidad de una y otra criptomoneda en términos de límite de emisión. Bitcoin tiene un tope de 21.000.000 de monedas y Ethereum no posee ese límite.
5. Ethereum además presenta una gran ventaja respecto de Bitcoin: Los contratos que en este sistema pueden identificarse individualmente mediante un "token".

Bitcoin comparado con Ripple

- Ripple: Su protocolo de pago es de código abierto y posibilita pagar de forma instantánea y casi sin costo en diversas monedas (yen, dólar, euro, bitcoins).
- Ripple trabaja con un algoritmo que ayuda al usuario a encontrar el atajo más rápido y económicamente conveniente entre las diferentes monedas.
- De hecho, a diferencia de Bitcoin, Ripple fue creado por una compañía llamada Ripple Labs que apunta a crear un nuevo sistema ultra rápido y eficiente de pago para el sistema bancario que sustituya a los sistemas utilizados actualmente.
- Mientras Bitcoin es una criptomoneda descentralizada, Ripple por el contrario está centralizada. Además, las monedas de Ripple no se crean mediante minería, sino que han sido creadas por Ripple Labs antes de su lanzamiento, compañía que también se encarga de colocarlas en el mercado.
- Gracias a Ripple, la criptomoneda ha ampliado su influencia en el mercado financiero y en muchos otros rubros a los que antes no tenía acceso.

11. Impacto de las criptomonedas en la economía.

- Eliminar la necesidad de intermediarios en transacciones financieras.
- Una nueva era de Crowdfunding Crowdfunding es una forma increíble de reunir dinero. El crowdfunding ha sido popular entre los empresarios y las personas que quieren comenzar su pequeña empresa.
- Separa las transacciones del dólar. El dólar estadounidense actúa como la moneda de reserva para la economía global , y las transacciones financieras convencionales que tienen lugar en todo el mundo tienen su base en el dólar. Las transacciones de criptomoneda, por otro lado, no necesitan tener ninguna conexión a la moneda patrocinada por el gobierno de los EE. UU.
- Evaden la regulación: las transacciones de criptomonedas es que son difíciles de regular debido a su naturaleza anónima.
- Habita más transacciones internacionales: Para las personas en estos países típicamente menos desarrollados, crypto ofrece una manera de involucrarse con la economía global de Internet.
- Elimina las barreras de entrada: Las criptomonedas también han permitido a los empresarios eludir las rutas tradicionales de recaudación de capital para las empresas comerciales relacionadas con criptografía y blockchain. En lugar de tener que convencer a los capitalistas de riesgo y los bancos para que inviertan en su proyecto, pueden pasar por alto el reglamento y la burocracia a través de una oferta inicial de moneda, o ICO.

12. Características de las monedas

- Descentralización: No están vinculadas a ningún organismo gubernamental ni financiero.
- Operabilidad: No estar reguladas bajo ningún mercado oficial hace que se pueda operar con ellas durante los 7 días de la semana y las 24 horas del día.
- Minería y Blockchain: En las monedas fiduciarias se imprimen billetes y se acuñan monedas, pero en el caso de las criptomonedas el sistema es muy diferente. Las monedas virtuales se crean a través de la minería. Un sistema en el que los individuos, mineros, a través de la tecnología blockchain (cadenas de bloques), validan transacciones a través de la resolución de problemas matemáticos a cambio de su recompensa, la criptomoneda.
- Transparencia: Todas las transacciones se "registran en un libro" compartido (tecnología blockchain) imposible de manipular.
- Volatilidad: Las criptomonedas pueden sufrir variaciones repentinas en su valor, aspecto que puede favorecer las posibilidades de hacer trade (negociar/especular), pero también pueden generar cientos de pérdidas.
- Aceptación: Las criptomonedas tienen el valor que los individuos le quieran dar y aceptar. Este sistema todavía está en duda en un largo plazo.
- No dependen de la política: Al estar descentralizadas de instituciones, los tipos de política monetaria, fiscal, y económica en general, de los países tienen escasa influencia en las criptomonedas.
- Regulación: Hasta el momento no existe ningún tipo de regulación sobre las criptomonedas pero lo más probable es que sean objetivo de regulación en alguno de sus aspectos por lo que las ventajas que tienen frente a las monedas tradicionales pueden llegar a desaparecer.

13. Computación cuántica

Consiste esencialmente en aprovechar y explotar las leyes de la mecánica cuántica para procesar información. En lugar de almacenar información usando bits representados por 0s o 1s, usan bits cuánticos, o qubits, para codificar información como 0s, 1s, o ambos al mismo tiempo. Esta superposición de estados y fenómenos de enredos y túneles, permite manipular enormes combinaciones de estados a la vez.

14. Principio de incertidumbre

Heisenberg enunció este principio: es imposible medir simultáneamente, y con precisión absoluta, el valor de la posición y la cantidad de movimiento de una partícula. Esto ya que la incertidumbre derivada de esta apreciación no corresponde a algún instrumento de medida, sino al mismo hecho de medir. Esto significa, que la precisión con que se pueden medir las cosas es limitada, y el límite viene fijado por la constante de Planck: $h = 6.626.10^{-34} J.s$. $\Delta x.\Delta p_x \geq \frac{h}{4\pi}$. Donde Δx : indeterminación en posición, Δp_x : indeterminación en cantidad de movimiento.

15. Concepto de Qubit

Es la unidad mínima de información cuántica. La diferencia principal entre ellos es que, el bit tradicional sólo puede entregar resultados binarios (0 y 1), mientras que el qubit, aprovechando las propiedades de la mecánica cuántica, puede tener ambos valores al mismo tiempo (0 y 1), lo que habilita una velocidad de procesamiento mucho mayor.

16. Operaciones con Qubits

Hay varios tipos de operaciones físicas que pueden realizarse en estados de qubit puros:

Puertas lógicas cuánticas: bloques de construcción para un circuito cuántico en una computadora cuántica, funcionan con uno, dos o tres qubits: matemáticamente, los qubits sufren una transformación unitaria bajo la puerta cuántica. Para un solo qubit, las transformaciones unitarias corresponden a las rotaciones del vector qubit (unidad) en la esfera de Bloch a superposiciones específicas. Para dos qubits, la puerta controlada NO se puede usar para enredarlos o desenredarlos.

Medición de base estándar: es una operación irreversible en la que se obtiene información sobre el estado de un solo qubit (y se pierde la coherencia).

Cuando se mide un qubit, el estado de superposición colapsa a un estado base (hasta una fase) y la fase relativa se vuelve inaccesible (es decir, se pierde la coherencia). Una medición de un estado qubit que se enreda con otro sistema cuántico transforma el estado qubit, un estado puro, en un estado mixto (una mezcla incoherente de estados puros) ya que la fase relativa del estado qubit se vuelve inaccesible.

17. Criptografía cuántica

Criptografía que utiliza principios de la mecánica cuántica para garantizar la absoluta confidencialidad de la información transmitida. Una propiedades importantes de esta es que si un tercero intenta espiar durante la creación de la clave secreta, el proceso se altera advirtiéndole al intruso antes de que se transmita información privada. Esto es consecuencia del teorema de no clonado. La seguridad de la criptografía cuántica descansa en las bases de la mecánica cuántica, a diferencia de la criptografía de clave pública tradicional la cual descansa en supuestos de complejidad computacional no demostrada de ciertas funciones matemáticas.

La mecánica cuántica describe la dinámica de cada partícula cuántica (fotones, electrones, etc.) en términos de estados cuánticos, asignando una probabilidad a cada posible estado de la partícula por medio de una función.

Aspectos que utiliza la criptografía de la mecánica cuántica:

Superposición: Una partícula puede poseer más de un estado a la vez.

Colapso de estados: Una partícula que se encuentra repartida entre todos sus estados accesibles, al ser medida se altera su estado superpuesto determinando en qué estado particular, de entre una variedad de estados posibles, se encuentra.

Incertidumbre: Cuanto más precisa sea la medición sobre una propiedad, mayor será la incertidumbre de la otra propiedad.

Entrelazamiento: Dos partículas cuánticas pueden tener estados fuertemente correlacionados, debido a que se generaron al mismo tiempo o a que interactuaron. Cuando hay una medición sobre una de ellas determina inmediatamente el estado de la otra, sin importar la distancia que las separe.

18. Partículas entrelazadas

Refiere al entrelazamiento cuántico, el cual describe un fenómeno de mecánica cuántica que se demuestra en los experimentos, pero inicialmente no se comprendió bien su relevancia para la física teórica. Un conjunto de partículas entrelazadas (en su término técnico en inglés: entangled) no pueden definirse como partículas individuales con estados definidos, sino como un sistema con una función de onda única para todo el sistema. El entrelazamiento es importante ya que : "Cuando dos sistemas, de los que conocemos sus estados por su respectiva representación, entran en interacción física temporal debido a fuerzas conocidas entre ellos y tras de un tiempo de influencia mutua se separan otra vez, entonces ya no pueden describirse como antes, esto es, dotando a cada uno de ellos de una representación propia. Siendo este el rasgo característico de la mecánica cuántica". Las partículas entrelazadas surgen de algunas posibles maneras, tales como:

- Electrón que desciende dos niveles energéticos dentro del átomo, generando dos fotones entrelazados.
- Colisión electrón- positrón, que genera dos fotones entrelazados

En cuanto a las mediciones posibles en dos partículas entrelazadas:

- Cantidad de movimiento y posición de ambas (EPR)
- Spines de ambas (David Bohm)

19. Ataque a sistemas de criptografía cuántica.

El caso de ataque "Quantum man-in-the-middle" el cual ataca al proceso de calibración de la llave de distribución quantum. -> **Ataque de intermediario:** Como ningún principio de la mecánica cuántica puede distinguir de amigo o enemigo, la QKD sigue siendo susceptible a ataques de intermediario.

Ataque de división del número de fotones: Ataque al número de fotones que se procesan, el cual compromete la privacidad de una clave segura. En el protocolo BB84, Alice envía estados cuánticos a Bob utilizando fotones individuales. En la práctica, muchas implementaciones utilizan pulsos de láser atenuados a un nivel muy bajo para enviar los estados cuánticos. Estos pulsos de láser contienen una cantidad muy pequeña de fotones, por ejemplo 0.2 fotones por pulso, que se distribuyen según una distribución de Poisson. Esto significa que la mayoría de los pulsos en realidad no contienen fotones (no se envía pulso), algunos pulsos contienen 1 fotón (que se desea) y algunos pulsos contienen 2 o más fotones. Si el pulso contiene más de un fotón, Eva puede dividir los fotones adicionales y transmitir el fotón individual restante a Bob. *Esta es la base del ataque de división del número de fotones, donde Eva almacena estos fotones adicionales en una memoria cuántica hasta que Bob detecta el fotón único restante y Alicia revela la base de codificación.* Eva puede medir sus fotones en la base correcta y obtener información sobre la clave sin introducir errores detectables.

Interceptar y reenviar: Eva mide los estados cuánticos (fotones) enviados por Alicie y luego envía estados de reemplazo a Bob, preparados en el estado que ella mide. En el protocolo BB84, esto produce errores en la clave que comparten Alice y Bob. Como Eva no tiene conocimiento de la base en la que están codificados los estados enviados por Alice, solo puede adivinar en qué base medir, de la misma manera que Bob. Si elige correctamente, mide el estado correcto de polarización de fotones enviado por Alice y vuelve a enviar el estado correcto a Bob. Sin embargo, si elige incorrectamente, el estado que mide es aleatorio, y el estado enviado a Bob no puede ser el mismo que el enviado por Alicia. Si Bob luego mide este estado de la misma manera que Alice envió, él también obtiene un resultado aleatorio, ya que Eva le ha enviado un estado en la forma opuesta, con un 50% de posibilidades de un resultado erróneo (en lugar del resultado correcto que obtendría) sin la presencia de Eva.