Criptografía pasado, presente y futuro

1. Los orígenes

El origen de la criptografía fue la inquietud por proteger la información que era transmitida. A lo largo del tiempo ha ido evolucionando. Podemos preguntarnos quién tenía esa inquietud por proteger la información, la respuesta es bastante clara, desde sus orígenes eran emperadores, militares, diplomáticos, comercio electrónico, banca, televisiones de pago,….y en la actualidad todos.

La información que se tiene que proteger puede ser de lo más diversa, pero en general podemos clasificarla en:

- Información valiosa para una organización.
- Aquella información cuya difusión no autorizada puede ocasionar un perjuicio a la nación/estado/organización (información clasificada).
- La información cedida por terceros.

¿Cómo la hemos protegido hasta el momento?

- No difundiéndola.
- Almacenamiento seguro: en una caja fuerte, bajo llave….
- Cifrado.
- Esteganografía.

¿Qué es la criptografía?

Consiste en modificar la información haciéndola inteligible mediante transformaciones. Estas transformaciones deben permitir que el mensaje sea recuperado más adelante, bien por el propietario o bien por el destinatario.

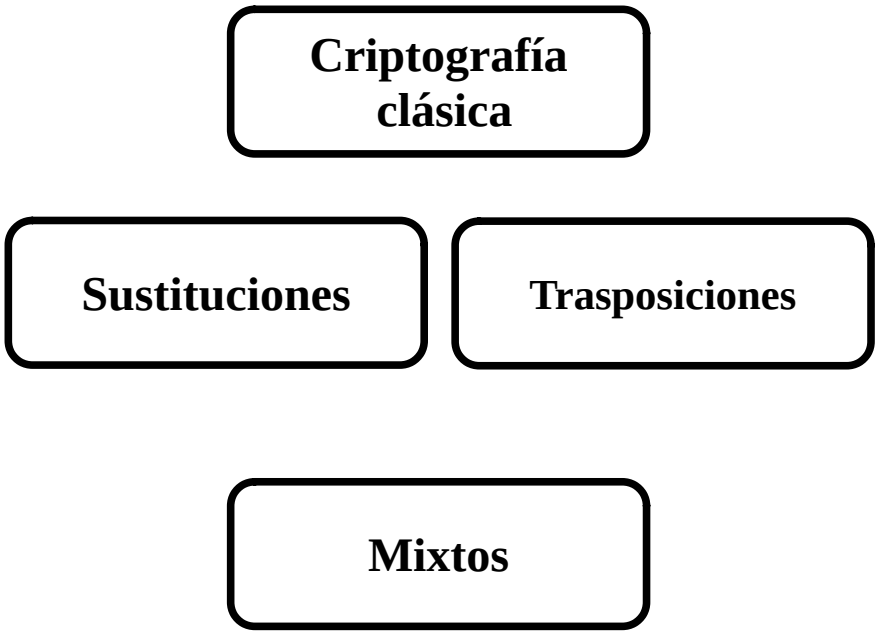
¿Qué es la esteganografía?

Consiste en modificar el soporte que transmite la información, es decir, ocultar el hecho de la existencia de información secreta, de modo que si se desconoce que tal información eiste, el adversario no la buscará.

2. Criptografía clásica

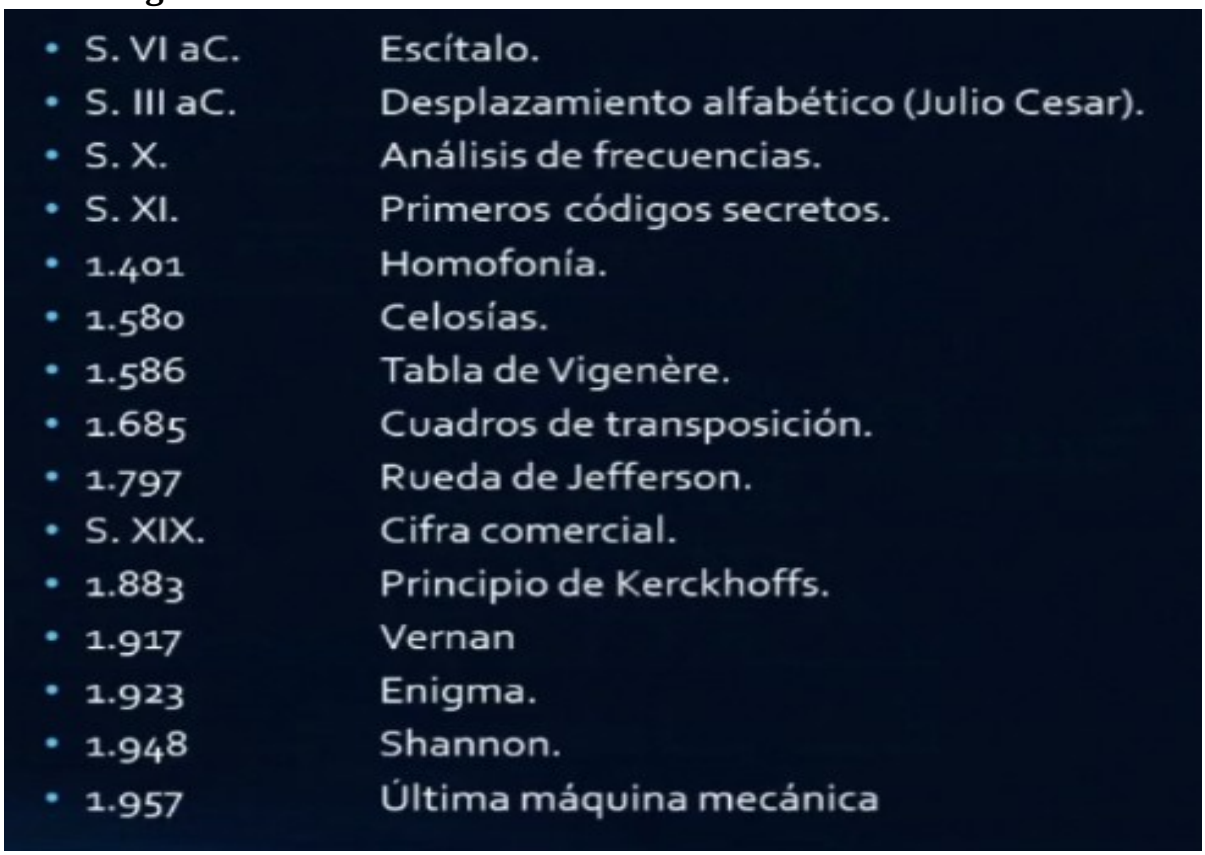
- **La escítala**: Datada del siglo IV a.C. Consiste en:
  - Enrollar un lazo alrededor de un bastón (grosor del palo)
  - Escribir un mensaje en claro por filas.
  - Desenrollar el lazo y enviarlo creando una trasposición de los elementos.
- **Cifrado César:** Datada del siglo III a.C. Consiste en cambiar cada letra del texto por la situada a una cantidad fija de lugares en el alfabeto. Es una sustitución porque se reemplaza cada elemento del texto por otro, se disfrazan los caracteres y se disimula la frecuencia.

Podemos considerar que:

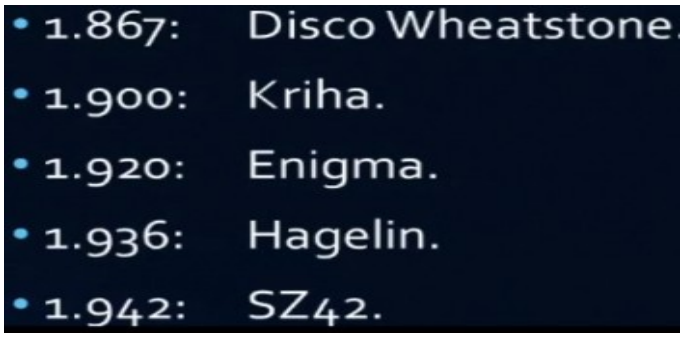


Al hacer pruebas se ha visto que un sistema en el que primero se realiza una sustitución más trasposición da más fortaleza al sistema.

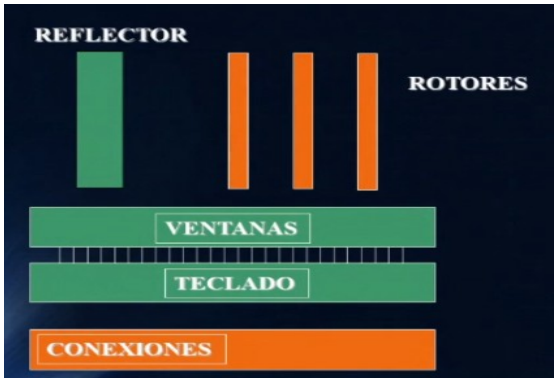
Cronología:



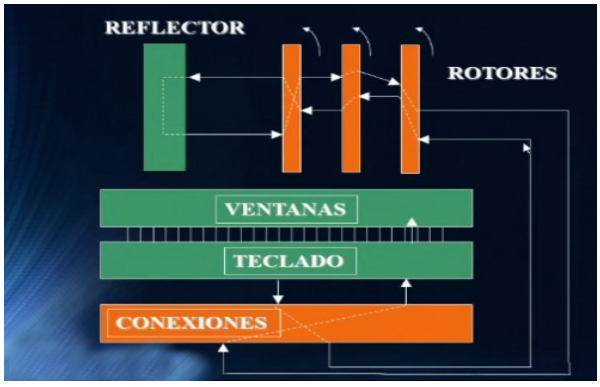
En la segunda mitad del siglo XIX ya apareció la primera máquina de cifrado para luego continuar a principios del siglo XX los primeros instrumentos capaces de cifrar y descifrar información. Algunos fueron:



Enimga: Podía tener tres o cuatro rotores distintos. La de la imagen tiene cuatro, que es la utilizada por la armada alemana.



Su funcionamiento:



¿Qué sucedió con la criptografía clásica?

A partir de la Teoría de Shanon en 1948 en la que se dice que la información es medible y tiene unas determinadas características y la llegada de los ordenadores, sumados a la necesidad de las grandes empresas y bancos de guardar secretos se llegó a crear el primer cifrado estándar internacional creado por IBM, el DES (Data Encryption Algorithm). Todo esto llevó al nacimiento de la criptografía moderna. La criptografía pasó de ser un arte a ser una ciencia.

3. El presente:

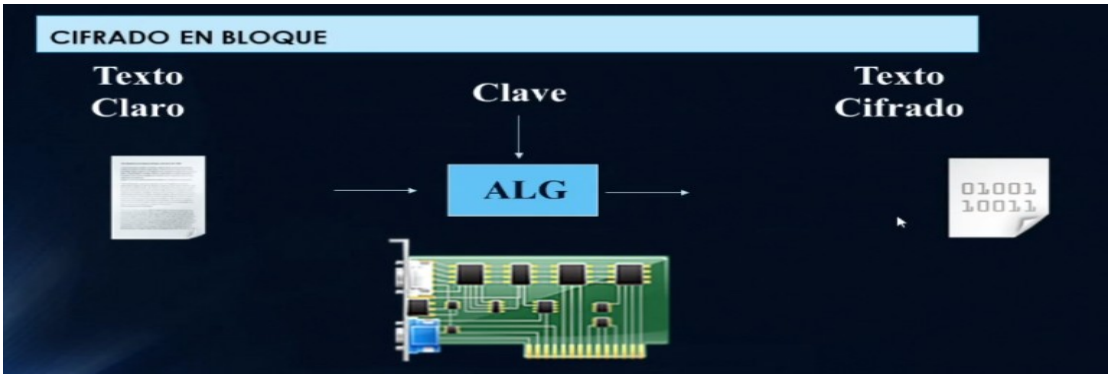
3.1. La criptografía moderna

El siguiente esquema representa la criptografía moderna:

Clave secreta: En la criptografía de clave secreta solo existe una clave tanto para cifrar como para descifrar. En la criptografía de clave publica existen dos claves una pública y una privada.

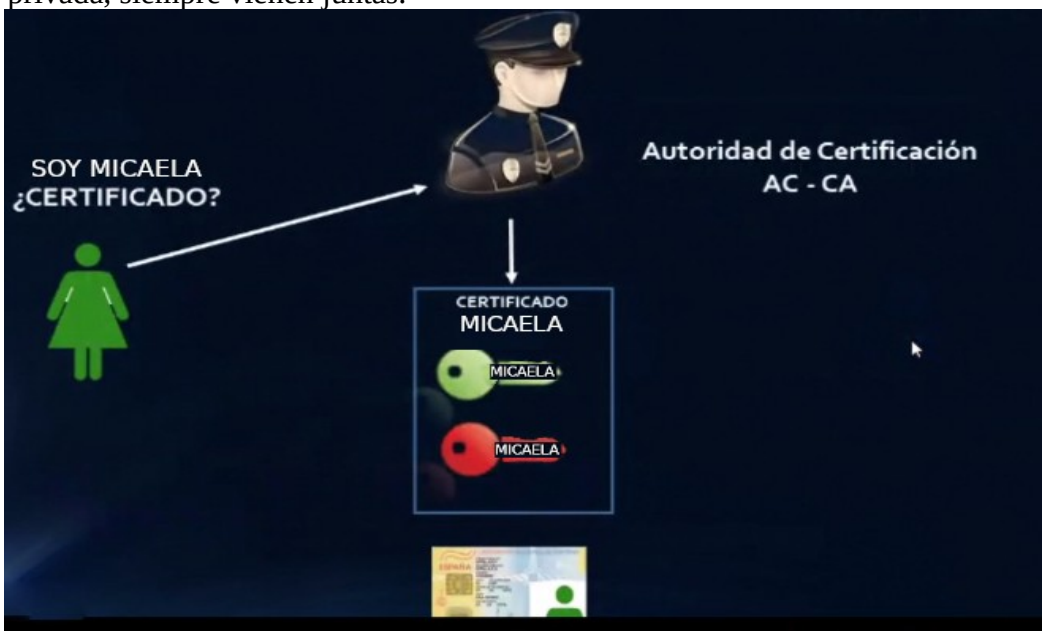
En la criptografía de clave secreta el gran problema es la distribución segura de la clave. Existen dos métodos:

- Cifradores en serie.
- Cifradores en bloque: El DES, de 64 bits aunque por cada byte se destina un bit para el control por tanto se queda solo en 56 bits, luego se pasó al Triple-DES que ofrecía una seguridad de 112 bits y luego se pasó al AES que es el que conocemos ahora con claves de 128, 192 y 256 bits.

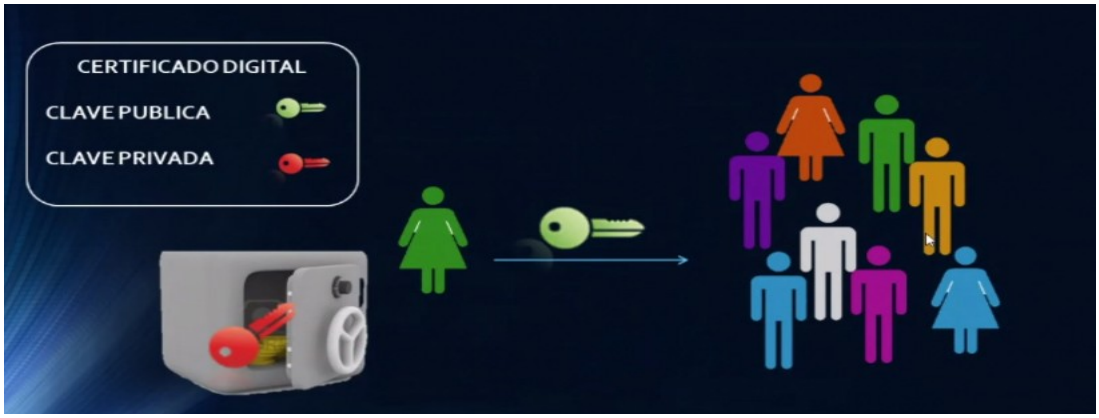


Clave pública:

Sirven para autenticación y para firma. Los certificados digitales se obtienen a través de una autoridad de certificación tales como la policía nacional con el DNI-e, la FNMT, la ACCV……. En la criptografía de clave pública siempre tendremos dos claves, la pública y la privada, siempre vienen juntas.



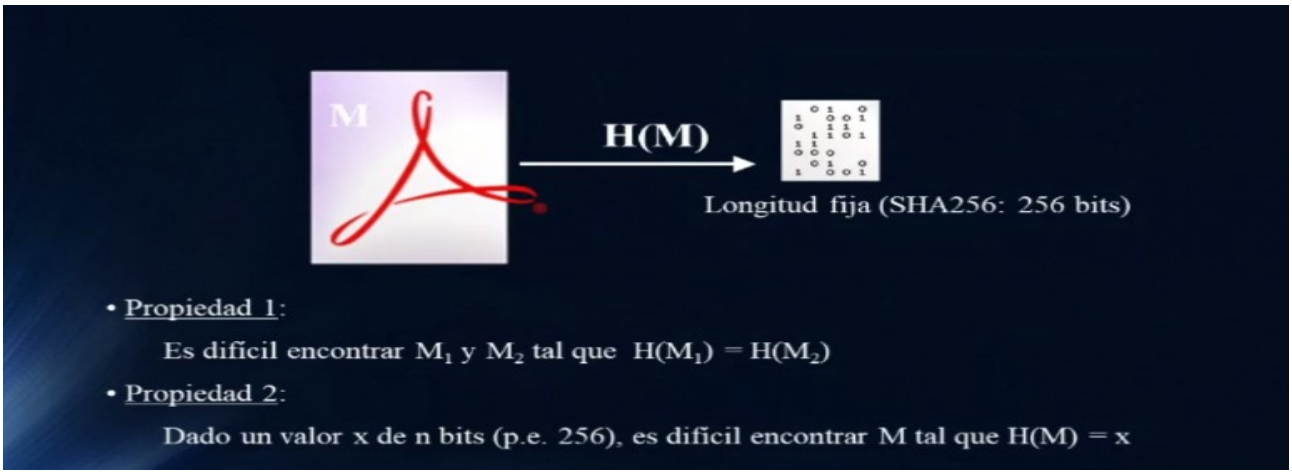
Veamos cómo funcionan:



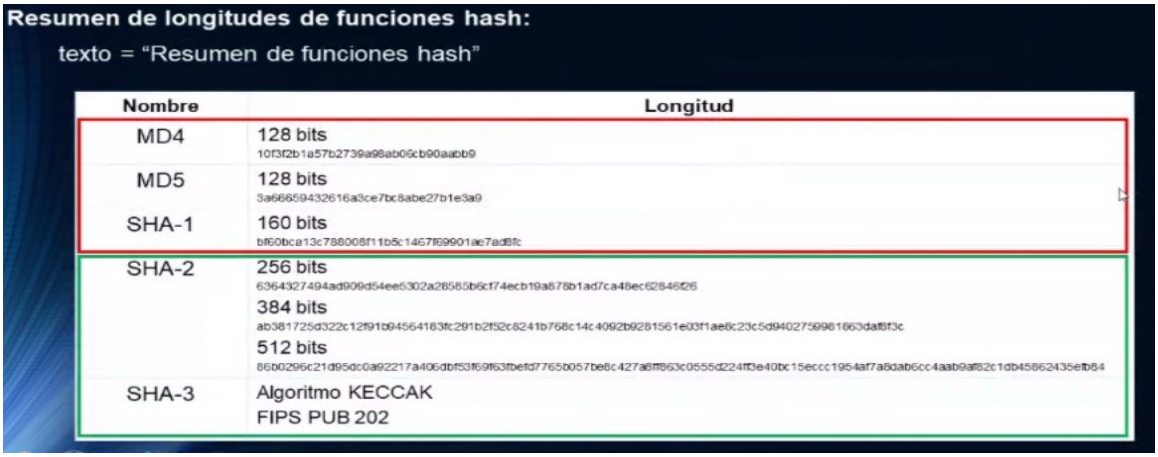
Imaginemos que he obtenido un certificado digital para poder autenticarme y para poder firmar. Para comunicarme, guardo la clave privada y envío la clave pública. Supongamos que una persona X cifra un mensaje con la clave pública, para descifrarlo usaré mi clave privada. Eso es más o menos lo que sucede cuando procedemos a la autenticación delante de organismos oficiales y cuando queremos firmar documentos, lo hacemos mediante nuestra clave privada junto con unas funciones matemáticas denominadas hash.

La criptografía de clave pública también se denomina criptografía asimétrica. Dentro de este tipo de criptografía podemos encontrar también la criptografía de curvas eliptícas.

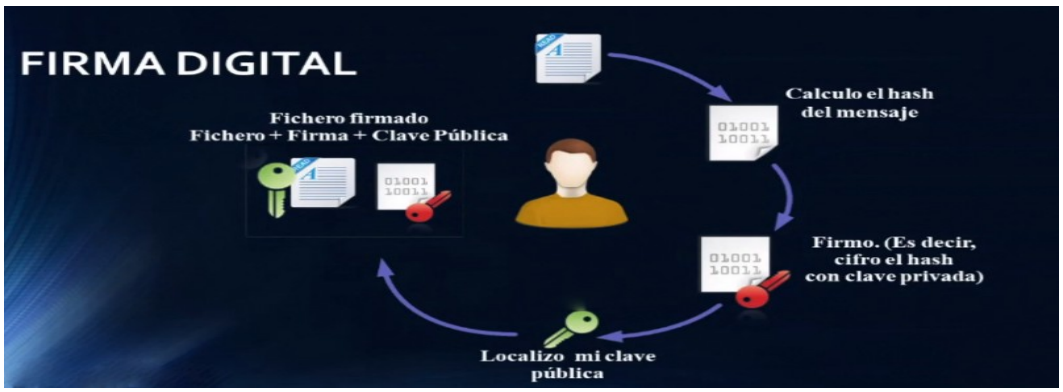
3.2. Las funciones Hash



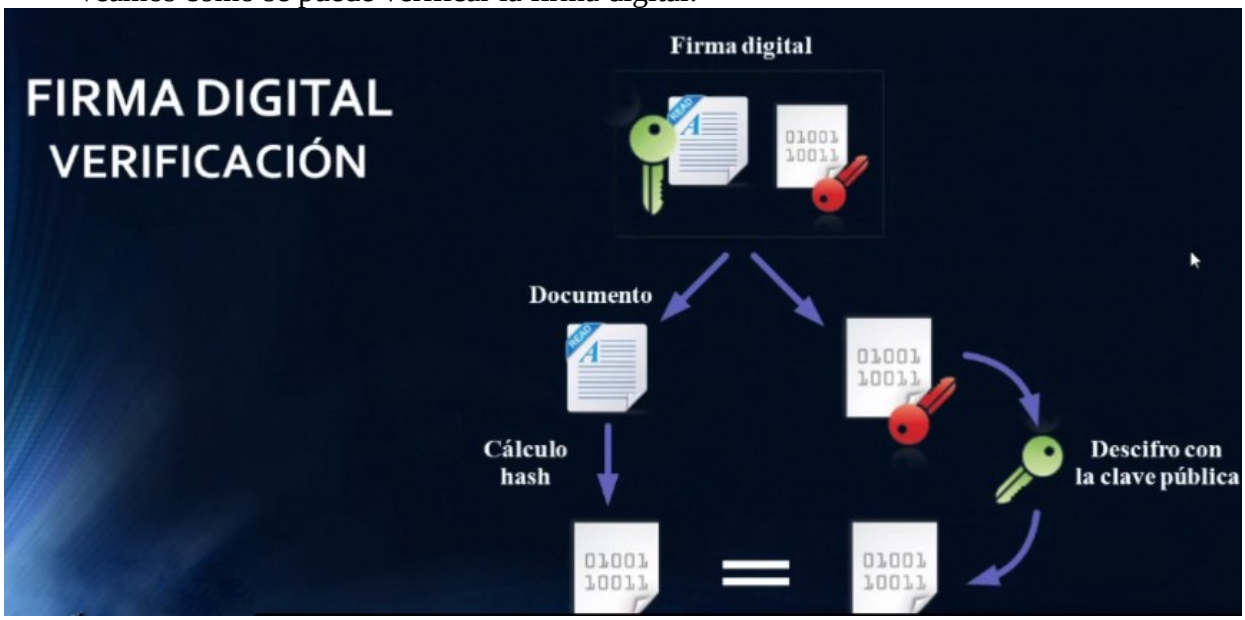
Las de la zona roja ya no se consideran seguras.



Veamos cómo se procede a firmar un documento:

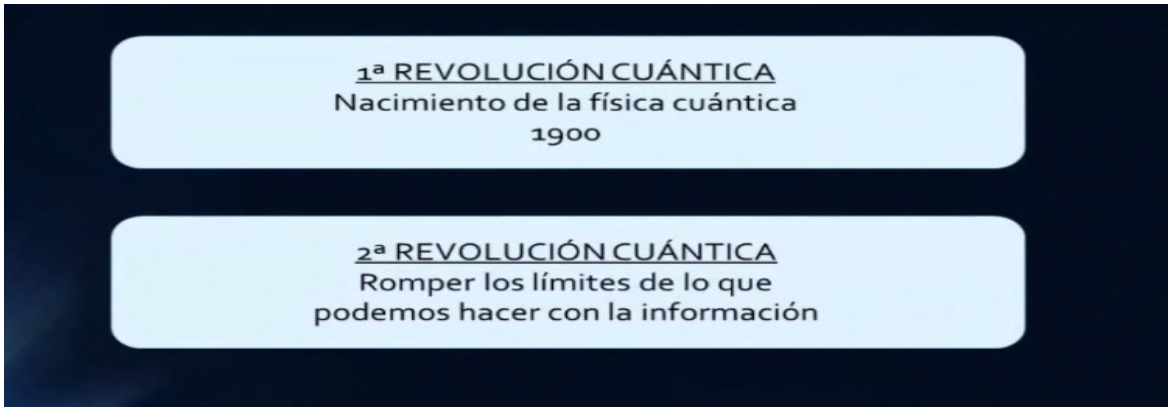


Veamos cómo se puede verificar la firma digital:



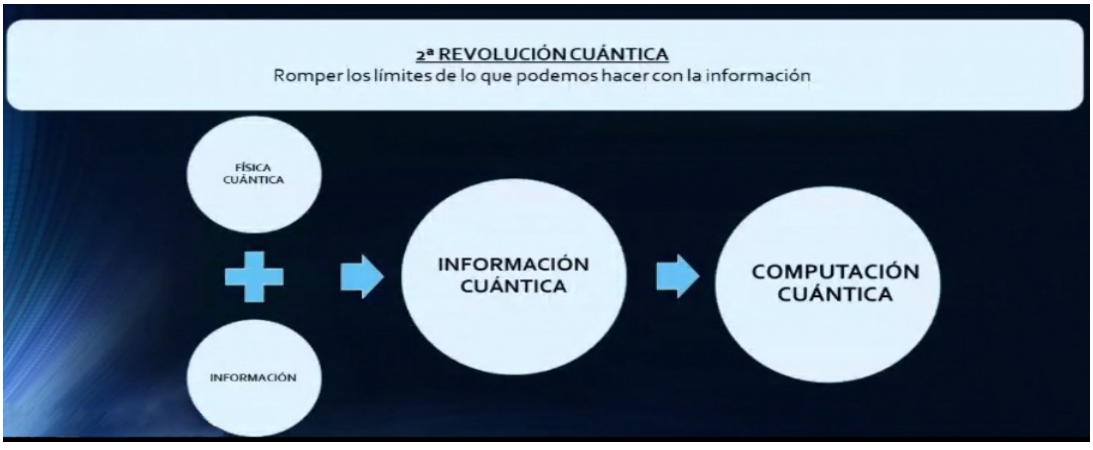
4. El futuro

4.1. La física cuántica



Supongamos que a las partículas microscópicas (átomos, fotones….) le pusiéramos información:

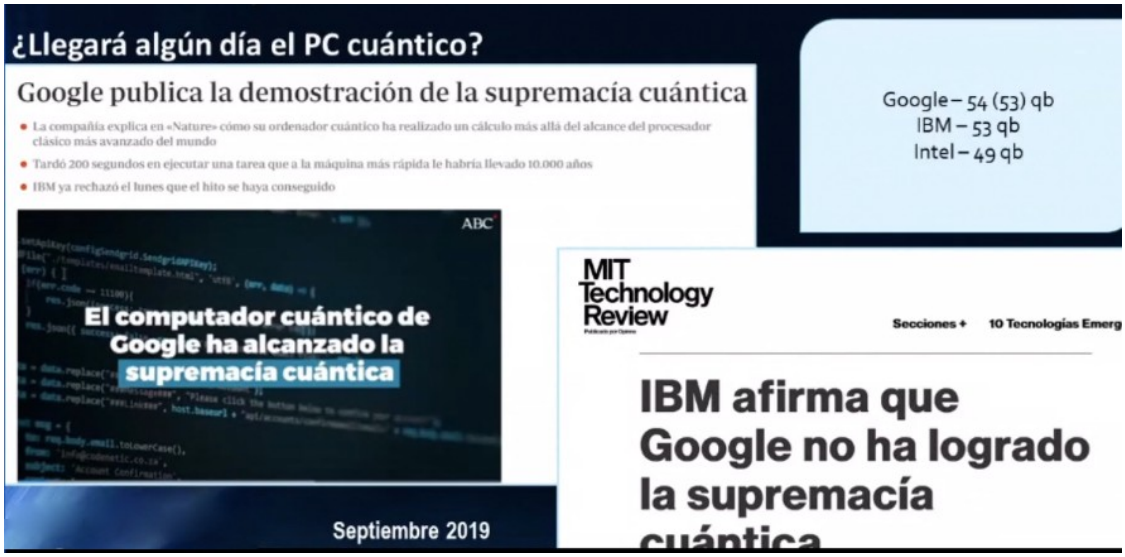
- La unidad mínima de información cuántica se llama bit cuántico o qubit.
- Estos bits cuánticos se rigen por la leyes de la física cuántica. Los bits cuánticos pueden tener diversos estados: estado 0, estado 1 o ambos estados a la vez.



Obviamente el bit cuántico o qubit necesita de un ordenador cuántico. Un ordenador cuántico hace lo mismo que uno clásico pero de una forma distinta. Un ordenador cuántico se rige por las leyes de la física cuántica, por una teoría probabilística, se asignan probabilidades de ocurrencia.

La potencia de cálculo de un ordenador cuántico podría llegar a la de 100 millonees de ordenadores actuales, teniendo en cuenta que x qubits equivalen a 2^x bits.

La carrera para su construcción ya ha empezado , se sabe que IBM lo está intentando en lo que se llamará el IBM Q, al igual que Google y Microsoft. Dwave Systems anunció un ordenador cuántico con un procesador de 128 qubits.



Noticia de abril de 2020:
https://www.muycomputerpro.com/2020/04/30/amazon-ibm-microsoft-google-computacion-cuantica

¿Llegará algún día el PC cuántico?

¿Qué es la supremacía cuántica?

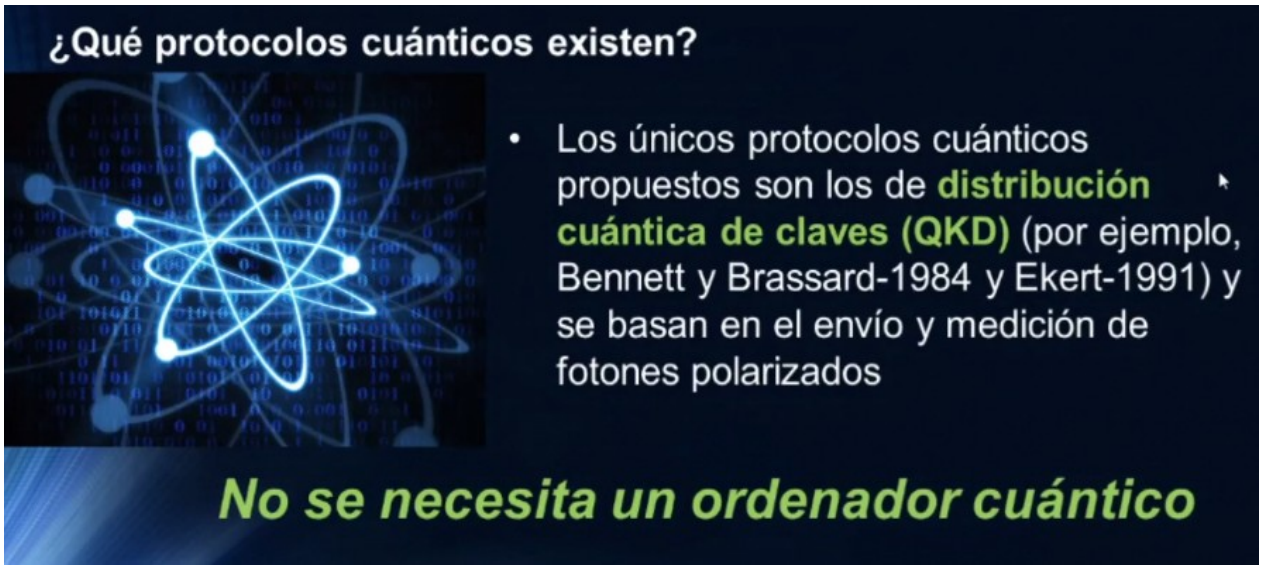
- Es el desarrollo de un ordenador cuántico que haga algún calculo que un superordenador no pueda hacer.
- Con 40-50 qubits soy capaz de hacer 2^{40}-2^{50} operaciones a la vez
- Por ahora estos cálculos no son relevantes para la seguridad de la información.

Pero:

¿PC cuántico vs problemas matemáticos?

- Sin embargo, romper los problemas matemáticos para las claves actuales (unos 2.000 bits) requeriría **4 días** con un ordenador cuántico de unos **7 millones de *qb***

~ 2030 y $1billón



Los ordenadores cuánticos se utilizaran para biotecnología, matemáticas, etc.…. Seguiremos trabajando con los ordenadores normales y superodenadores apoyados en los pc cuánticos.

4.2. Criptografía cuántica

La criptografía cuántica es la criptografía que utiliza principios de la mecánica cuántica para garantizar la absoluta confidencialidad de la información transmitida. Los protocolos de distribución se usarían para el intercambio de claves.


EL PAÍS Materia SUSCRÍBETE INICIAR SESIÓN

China crea un sistema de comunicación cuántica desde el espacio imposible de espiar

El país asiático transmite claves secretas desde un satélite a dos estaciones terrestres separadas por más de 1.000 kilómetros, 10 veces más que lo conseguido hasta ahora

NUÑO DOMÍNGUEZ

16 JUN 2020 - 9:39 CEST

https://elpais.com/ciencia/2020-06-15/china-crea-un-sistema-de-comunicacion-cuantica-desde-el-espacio-imposible-de-espiar.html

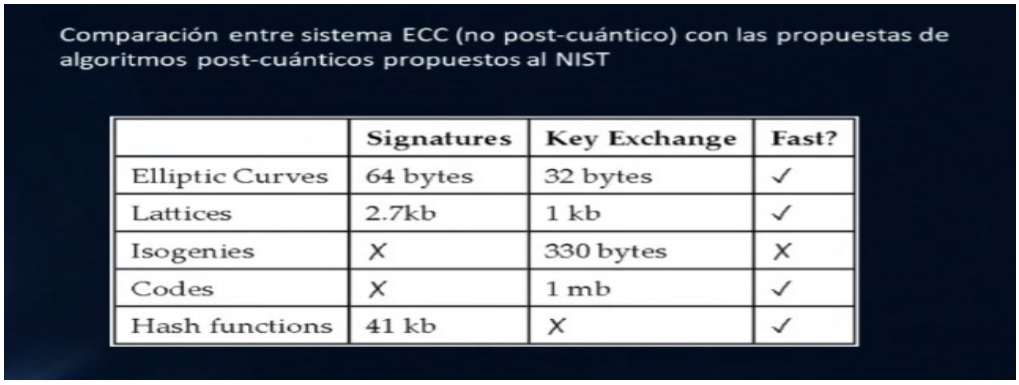
4.3. Criptografía post-cuántica

La esperanza para la criptografía asimétrica está en estudiar nuevos y viejos problemas matemáticos para los que todavía no hay algoritmos conocidos que rompan o que no sean vulnerables a la computación cuántica cuando ésta llegue.

Se barajan los siguientes algoritmos post-cuánticos:

- Criptografía basada en Teoría de Códigos. (Code-based).
- Firmas digitales basadas en hashed (Hash-based).
- Criptografía multivariante cuadrática (MQC).
- Criptografía basada en isogenias (isogeny-based, homomorfismos de grupos, curvas elípticas).
- Criptografía basada en retículos (lattice-based)

Comparativa :



	Signatures	Key Exchange	Fast?
Elliptic Curves	64 bytes	32 bytes	✓
Lattices	2.7kb	1 kb	✓
Isogenies	X	330 bytes	X
Codes	X	1 mb	✓
Hash functions	41 kb	X	✓

En resumen, existe una amenaza importante a la criptografía actual como consecuencia de la computación cuántica y de diferentes algoritmos de ataque:

- Criptografía asimétrica: algoritmo de Shor.
- Criptografía simétrica: algoritmo de Grover.

Esto nos urge a desarrollar nuevos algoritmos criptográficos y a adoptar medidas para prevenir la amenaza cuántica.