CRYPTO & QUANTUM

Pau Sala

Information Security

ÍNDICE:

01.Diferencias

Y funciones:

Codificar

No se usa con fines de seguridad.
Los datos se transforman de un formato a otro

01

Cifrar

El cifrado generalmente se implementa para proteger los datos del exterior

02

Hashing

Hashing protege tus datos contra posibles alteraciones

03

Ofuscar

Hacer que el código fuente sea ininteligible, difícil de comprender e interpretar

04

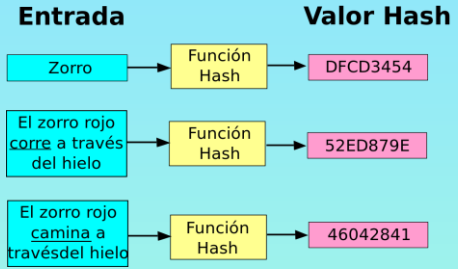
01.Diferencias

Y funciones:

01 Codificar

02 Cifrar

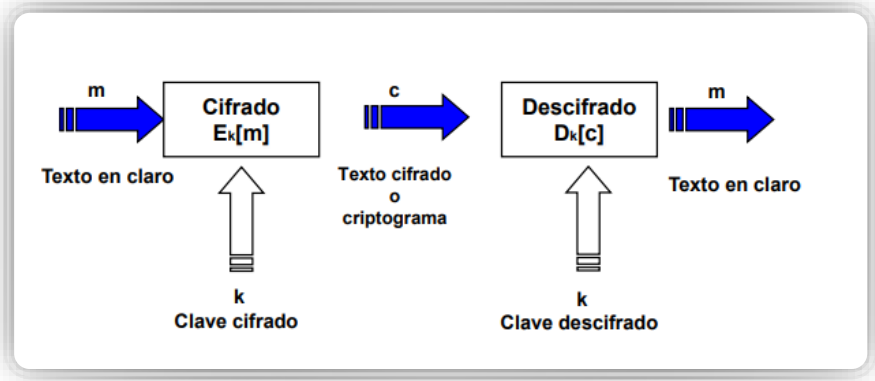
03 Hashing



04 Ofuscar

0.2 CriptograFía

- CRIPTOGRAFÍA: DEL GRIEGO KRYPTOS (OCULTO) + GRAPHOS (ESCRITURA)
- CIENCIA DE CODIFICAR Y DECODIFICAR INFORMACIÓN PARA QUE SOLO LAS PERSONAS AUTORIZADAS PUEDAN ACCEDER A ELLA



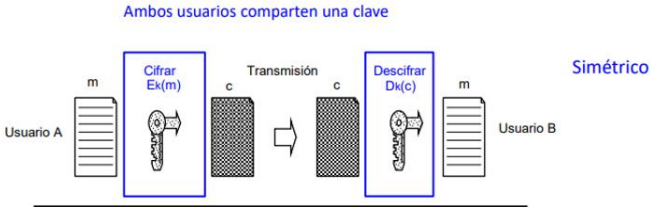
03. Aplicaciones

- Comunicaciones seguras
  - Tráfico web: HTTPS (SSL/TLS)
  - Tráfico wireless: 802.11 WPA2 (WPA,WEP), GSM, Bluetooth
- Cifrar ficheros almacenados en un disco duro
- Protección de contenido (p.ej. Amazon Prime, NetFlix, Spotify)
- Firma digital
- Votaciones electrónicas
- Moneda digital anónima
- (Bitcoin, Ethereum...)
- ...

04.
Tipos de Cifrado

Cifrado simétrico y cifrado asimetrico

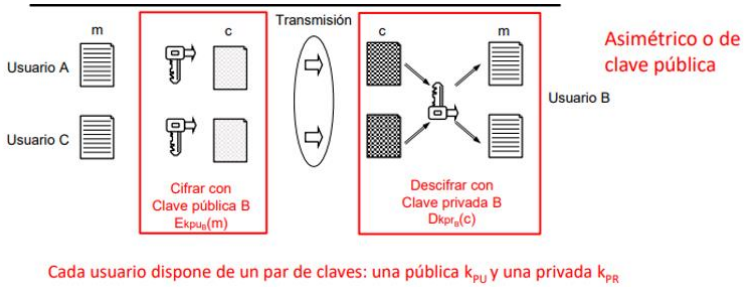
Simétrico vs Asimétrico



Simétrico

Misma clave para cifrar y descifrar.

Desventaja: La clave secreta debe ser compartida entre las partes que intercambian información



Asimétrico

Claves distintas. (Clave Privada y Clave pública).

Muy seguro y eficaz para proteger la información confidencial ya que no se necesita compartir la clave privada

Ejemplo

Cifrado Asimétrico

Para ello Luis cifra el mensaje con la clave pública de María.

María descifra el mensaje cifrado con su clave privada.

Cifrado Simétrico

Se intercambia la clave de cifrado y descifrado utilizando protocolos de intercambios de clav como por ejemplo DIFFIE-HELLMAN o utilizando un canal de comunicación seguro como por ejemplo una VPN.

05. Modo de cifrado

Se cifra el mensaje

Modo de cifrado

Criptografía asimetrica:

Algoritmo	Función unidireccional
Diffie-Hellman	Logaritmo discreto
Elgamal	Logaritmo discreto
RSA	Factorización
ECC (Elliptic Curve Cryptography)	Logaritmo discreto (sobre curvas elípticas)
Probabilísticos	Residuosidad cuadrática

1. Escoger 2 primos: $p = 431$ y $q = 313$
2. Calcular $n = p \cdot q = 134903$ y $\phi(n) = (p-1)(q-1) = 134160$
3. Escoger $e = 101$ (cumple $\text{mcd}(\phi(n), e) = 1$
4. Calcular d tal que $1 \equiv e \cdot d \ mod\ \phi(n)$
   $d = 54461$

Parámetros públicos: (e, n)
Parámetros privados: $(d, p, q, \phi(n))$
Clave pública: $K_{pub} = (e, n)$
Clave privada: $K_{priv} = (d, n)$

- Clave pública: $K_{pub} = (e, n)$ (exponente público)
- Clave privada: $K_{priv} = (d, n)$ (exponente privado)

$e \cdot d \equiv 1 \mod \phi(n)$

$m_i < n$ — cifrado → $c_i = m_i^e \mod n$

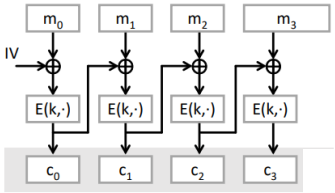
$c_i < n$ — descifrado → $m_i = c_i^d \mod n$

- Como $e \cdot d \equiv 1 \mod \phi(n)$, por el teorema de Euler:

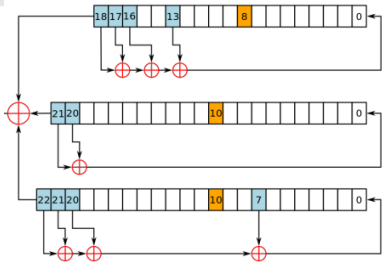
$$c_i^d \mod n = m_i^{e \cdot d} \mod n = m_i^{1 \mod \phi(n)} \mod n \equiv m_i \mod n$$
$$m_i^e \mod n = c_i^{d \cdot e} \mod n = c_i^{1 \mod \phi(n)} \mod n \equiv c_i \mod n$$

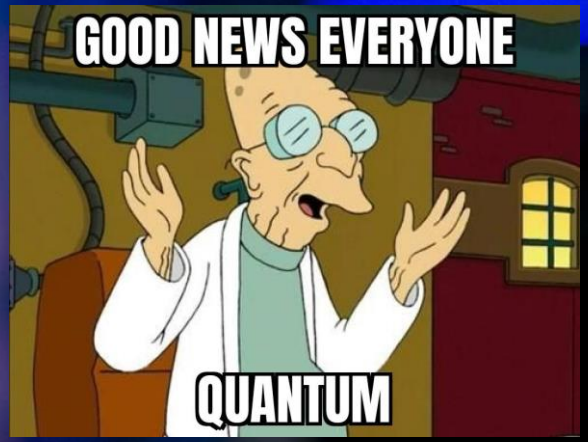
Criptografía asimetrica:

Cifradores en flujo o en bloque



Cifrado: $c_i = E_K\{m_i \oplus c_{i-1}\}$
Descifrado: $m_i = D_K\{c_i\} \oplus c_{i-1}$



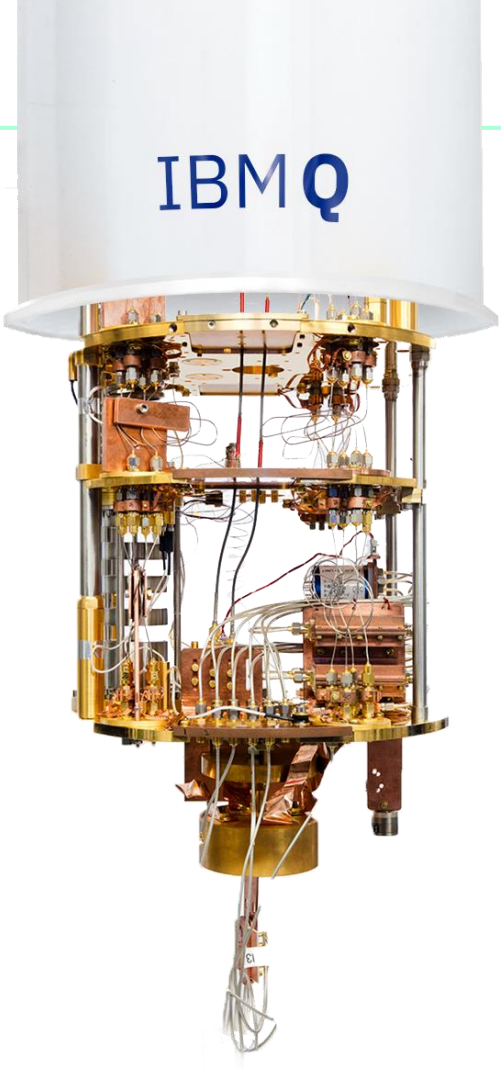


Ordenadores Cuánticos

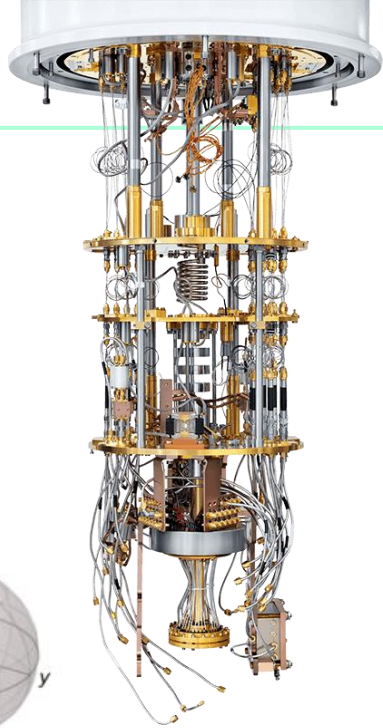
SCRM INTERNATIONAL HUB

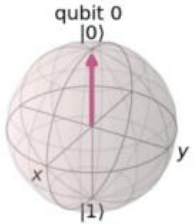
¿Para qué sirven?

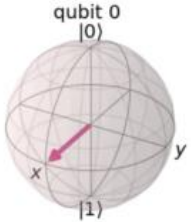
- Nueva comprensión de la física y de nuestro universo
- Resolver matemáticas complicadas con rapidez
- Mayor precisión (militar, meteorológica, gestión del tráfico)
- Nuevos medicamentos, mejores células solares, nuevos productos químicos.
- Cosas que ahora no podemos imaginar



¿Qué son los ordenadores cuánticos?







- Los ordenadores tradicionales son binarios.
- Cada bit puede ser 1 o 0, carga positiva o carga negativa.
- Un bit solo puede ser una cosa a la vez.

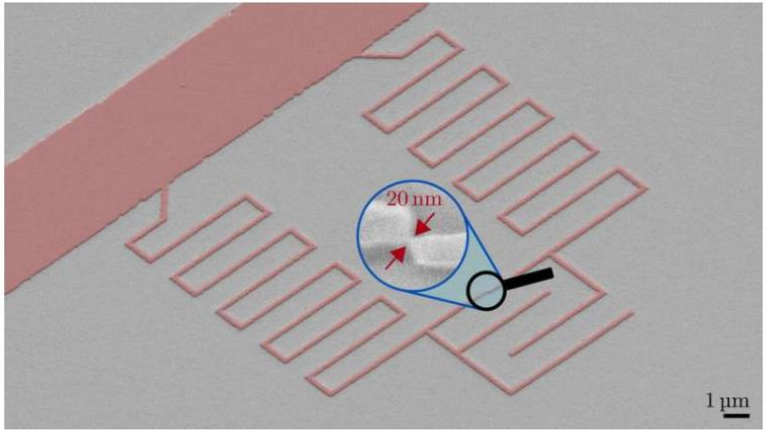
- Los Ordenadores Cuánticos usan Qubits.
- Un Qubit puede tener los dos estados simultáneamente.

Hay un problema

- Es muy difícil hacer Qubits estables.
- La gran mayoría de Qubits necesitan “estabilización” o “QEC” para funcionar.
- 1 error cada 200 acciones.

A new qubit approach for more stable states for quantum computers

by Karlsruhe Institute of Technology



The properties of gralmonium qubits are determined by a small junction of 20 nanometers only, which a…

Quantum computers can more rapidly process large amounts of data, because they carry out many computation steps in parallel. The information carrier of the quantum computer is a qubit. Qubits do not only possess the information of "0" and "1," but also values in between. However, the difficulty consists in producing qubits that are small enough and can be switched quickly enough to execute quantum calculations.

Timeline

2018

max. 72 Qubits

2022

433 Qubits

2025

Se esperan procesadores de 4000+ Qubits

Ordenadores Cuánticos Comercializables

2 Qubit

3 Qubit

IBM Q™

Cloud

Development Roadmap

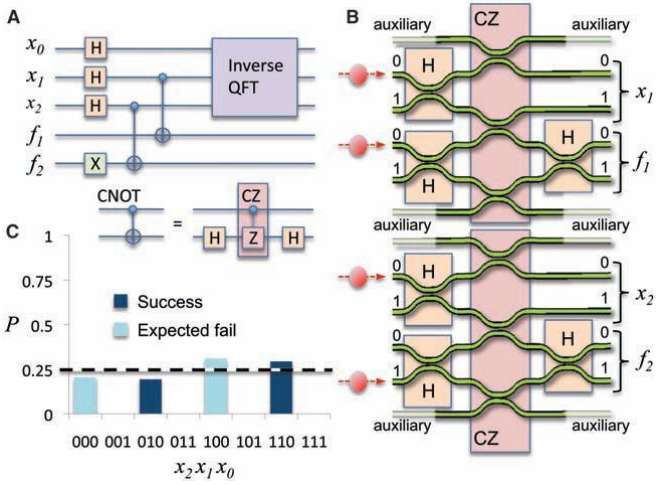
Executed by IBM
On target

IBM **Quantum**

	2019	2020	2021	2022	2023	2024	2025	Beyond 2026
Model Developers					Prototype quantum software applications → Quantum software applications			
						Machine Learning | Optimization | Natural Science | Finance		
Algorithm Developers		Quantum algorithm and application modules			Quantum Serverless			
		Machine Learning | Natural science | Optimization | Finance				Intelligent orchestration	Circuit Knitting Toolbox	Circuit Libraries
Kernel Developers	Circuits			Qiskit Runtime				
					Dynamic Circuits	Threaded Primitives	Error suppression and mitigation	Error correction
System Modularity	Falcon 27 qubits	Hummingbird 65 qubits	Eagle 127 qubits	Osprey 433 qubits	Condor 1,121 qubits	Flamingo 1,386+ qubits	Kookaburra 4,158+ qubits	
					Heron 133 qubits x p	Crossbill 408 qubits		

Algoritmo de Shor

- Requiere 20 qubits para funcionar decentemente.
- Un ordenador cuántico de 4099 Qubits, podría romper una clave de 2048-bits en 100 segundos.



¿Estaremos preparados?

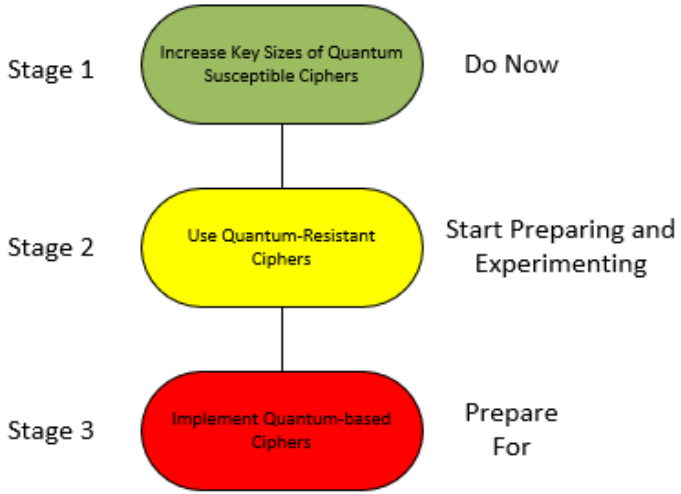
Commercial National Security Algorithm Suite and Quantum Computing FAQ

Q: Why is now the right time to make an announcement?

A: Choosing the right time to champion the development of quantum resistant standards is based on 3 points: forecasts on the future development of a large quantum computer, maturity of quantum resistant algorithms, and an analysis of costs and benefits to NSS owners and stakeholders. NSA believes the time is now right—consistent advances in quantum computing are being made, there are many more proposals for potentially useful quantum resistant

¿Cómo nos podemos preparar?

- Educando.
- Datos Inventariados.
- Empezar a usar quantum-resistant crypto.
- Evitar las escuchas de datos de gran valor.



Round 3 Finalists: Public-key Encryption and Key-establishment Algorithms

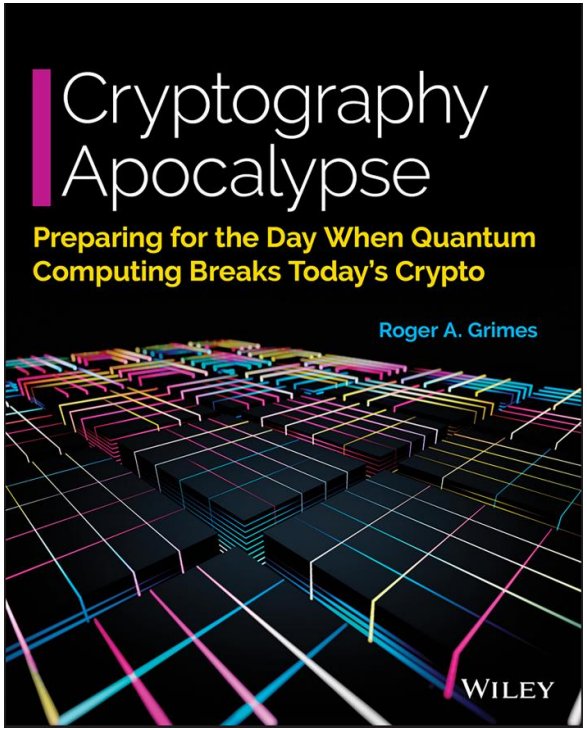
Algorithm	Algorithm Information	Submitters	Comments
Classic McEliece *(merger of Classic McEliece and NTS-KEM*	Zip File (97MB) IP Statements Website	Martin R. Albrecht Daniel J. Bernstein Tung Chou Carlos Cid Jan Gilcher Tanja Lange Varun Maram Ingo von Maurich Rafael Misoczki Ruben Niederhagen Kenneth G. Paterson Edoardo Persichetti Christiane Peters Peter Schwabe Nicolas Sendrier Jakub Szefer Cen Jung Tjhai Martin Tomlinson Wen Wang	Submit Comment View Comments
CRYSTALS-KYBER	Zip File (7MB) Website	Peter Schwabe Roberto Avanzi Joppe Bos Leo Ducas Eike Kiltz Tancrede Lepoint Vadim Lyubashevsky John M. Schanck Gregor Seiler Damien Stehle Jintai Ding	Submit Comment View Comments
NTRU	Zip File (6MB) IP Statements Website	Cong Chen Oussama Danba Jeffrey Hoffstein Andreas Hulsing Joost Rijneveld John M. Schanck Peter Schwabe William Whyte Zhenfei Zhang Tsunekazu Saito Takashi Yamakawa Keita Xagawa	Submit Comment View Comments
SABER	Zip File (5MB) IP Statements Website	Jan-Pieter D'Anvers Angshuman Karmakar Sujoy Sinha Roy	Submit Comment View Comments

Round 3 Finalists: Digital Signature Algorithms

Algorithm	Algorithm Information	Submitters	Comments
CRYSTALS-DILITHIUM	Zip File (11MB) IP Statements Website	Vadim Lyubashevsky Leo Ducas Eike Kiltz Tancrede Lepoint Peter Schwabe Gregor Seiler Damien Stehle Shi Bai	Submit Comment View Comments
FALCON	Zip File (4MB) Website	Thomas Prest Pierre-Alain Fouque Jeffrey Hoffstein Paul Kirchner Vadim Lyubashevsky Thomas Pornin Thomas Ricosset Gregor Seiler William Whyte Zhenfei Zhang	Submit Comment View Comments
Rainbow	Zip File (595MB) Website	Jintai Ding Ming-Shing Chen Albrecht Petzoldt Dieter Schmidt Bo-Yin Yang Matthias Kannwischer Jacques Patarin	Submit Comment View Comments

Fuentes y formación.

- https://quantum-computing.ibm.com/composer/docs/iqx/guide
- https://study-online.sussex.ac.uk/cmp/msc-quantum-technology
- https://www.developerro.com/2019/05/29/introduccion-quatum-development-iii/
- https://quantum-explore.com/master/
- Udemy
- https://keepcoding.io/blog
- https://www.adictosaltrabajo.com/2016/11/10/criptografia-y-seguridad
- https://blog.thedojo.mx/2021/12/12/tipos-de-algoritmos-criptograficos-cifrados-de-flujo.html



Conclusiones

- La mayor parte de la criptografía que hoy es computacionalmente imposible de descifrar, se podrá romper en menos de 2 minutos.
- La computación cuántica ha venido para cambiarnos la vida.
- Hay que empezar a proteger toda información sensible para evitar captura de datos y la desencriptación en la era cuántica.
- Seguir formándonos y mantenernos “up to date” para aplicar los estándares que marque la NIST.