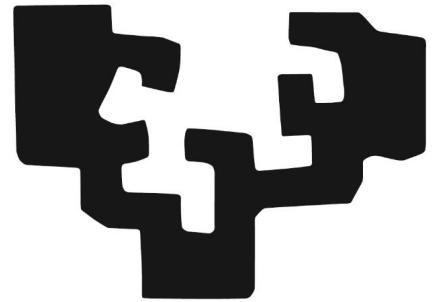


eman ta zabal zazu



Universidad  
del País Vasco

Euskal Herriko  
Unibertsitatea



**enigmedia**

**Carlos Tomás**  
CTO y Co-fundador

carlos@enigmedia.eu  
[www.enigmedia.eu](http://www.enigmedia.eu)

1. Introducción histórica a la criptografía
2. Criptografía Moderna
3. Retos de la criptografía en Internet of Things
4. Retos de la criptografía en Blockchain
5. Criptografía post-cuántica





# Qué no es criptografía

**Esteganografía:** Conjunto de técnicas que permiten ocultar un mensaje en otro medio



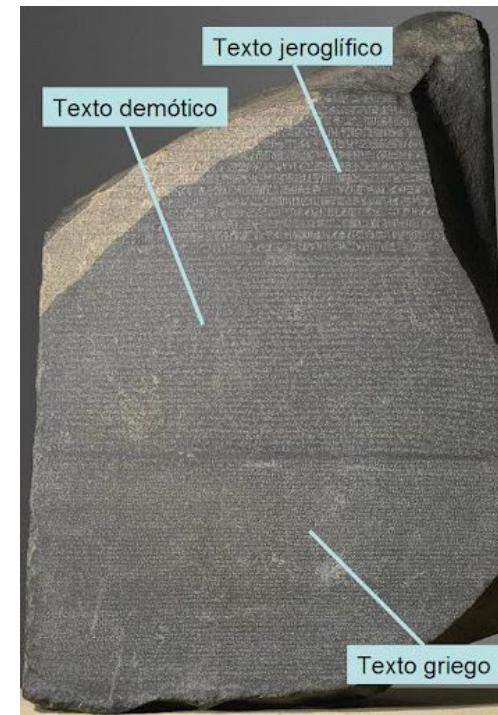
EL PERSONAJE DEL DÍA



**Julio Iglesias**  
Cantante

Julio Iglesias ha entrado en una polémica sin quererlo por la decisión de Ana Botella de investirle como hijo predilecto. O, por lo menos, la oposición es la que ha criticado este reconocimiento porque, dicen, es una decisión que ha llegado sin el acuerdo de los grupos. Estas propuestas, aseguran, las tienen que alcanzar los partidos en consenso, pues son unos «honores que la ciudad tiene que entregar y no otorgarlos sólo el Gobierno». Al margen de esto, se prevé que marzo sea el mes en que Madrid otorgue el premio al cantante.

**Código:** Establecer una correspondencia en la codificación entre el mensaje y el medio utilizado para transmitirlo (palabras, letras, etc...)





## ¿Para qué se puede usar la criptografía?

La criptografía actualmente se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican.

La criptografía se ocupa de dotar a la información de las siguientes propiedades:

- **Confidencialidad:** La información es accesible sólo para personas autorizadas
- **Integridad:** El mensaje recibido es el original
- **Autenticación:** El emisor y el receptor son quienes dicen ser
- **No-repudio:** El emisor puede demostrar que ha enviado el mensaje y el receptor que lo ha recibido



# HISTORIA DE LA CRIPTOGRAFÍA





## Primeros cifrados - Escítala

Se utiliza una vara de un diámetro para enrollar un papel sobre el que se escribe un texto. Para descifrar el mensaje el receptor necesita una vara del mismo diámetro



Grecia, 900 aC

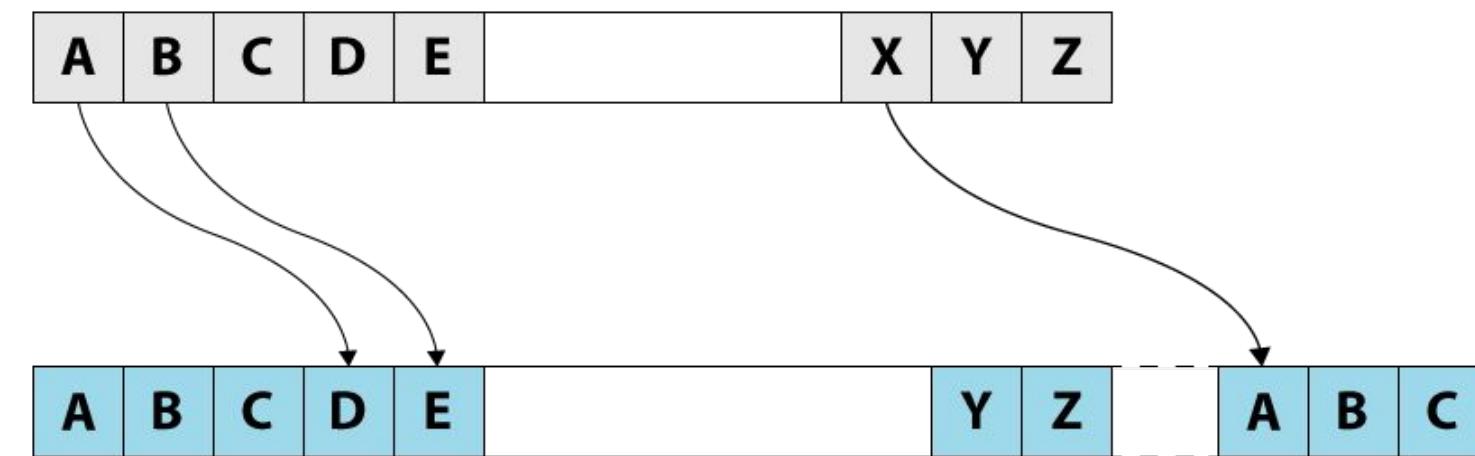




# Cifrado César



Julio César  
100 aC – 41 aC



Se sustituye cada letra por otra siguiendo una distancia fija entre letras, siendo esta distancia la clave de cifrado

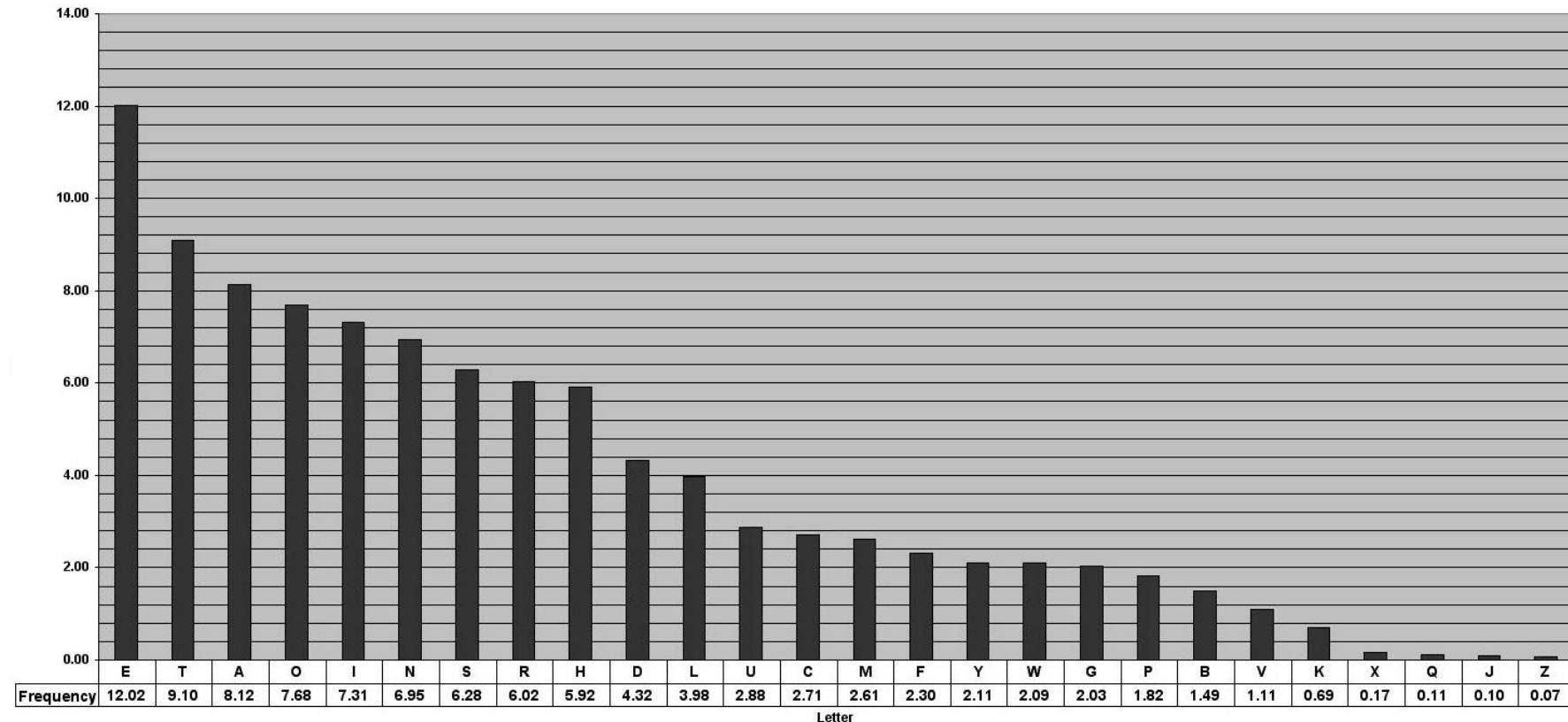




# Primer Criptoanálisis



Al-Kindi  
801 dC – 873 dC



Distribución letras en inglés



# Cifrados Homófonicos

Para reducir la probabilidad de este tipo de ataque estadístico, se busca que cada letra tenga más de un sustituto, de forma que reduzcamos la probabilidad de repetición en el texto cifrado



Ejemplo: Método de cinta móvil

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	X	Y	Z
X	Y	Z	E	U	F	O	R	I	C	A	S	B	D	G	H	J	K	L	M	N	Ñ	P	Q	T	V
									10	11	12	13	14	15	16	17	18	19	20						
21	22				23	24	25	26		27		28	29		30	31	32	33							
		34	35	36	37	38	39	40	41	42	43	44	45	46											
47	48			49	50	51	52	53	54	55	56	57	58	59											
		60	61		62	63	64	65	66	67	68	69	70	71											
72	73	74			75	76	77	78	79	80	81	82	83	84											
		85	86	87		88	89	90	91	92	93	94	95	96											
97	98	99																							

C	H	O	C	O	L	A	T	E	R	O
51	79	37	25	11	93	13	46	10	24	62





# Cifrado Vigenere

Entrada clave

Entrada texto

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



Blaise de Vigenere  
1523 - 1596





# Criptoanálisis Kasiski



Sistema Vigenere usado por los Confederados  
(1860 aprox)

En 1863, Friedich Kasiski publica:

*Escritura secreta y el arte de descifrarla*

Expone cómo romper el cifrado Vigenere





## Desiderata de Kerchoffs

1. El sistema tiene que ser indescifrable en la práctica, si no lo es matemáticamente.
2. **El método de cifrado no debería requerir secreto y no debería ser un problema que cayese en manos del enemigo.**
3. Deber ser posible comunicarse y recordar la clave sin usar notas escritas. Los usuarios pueden cambiar la clave a voluntad.
4. Debe ser aplicable a las comunicaciones telegráficas.
5. Debe ser portable y no tiene que requerir a muchas personas para operarlo.
6. El sistema debe ser fácil de usar y no debe requerir que los usuarios sepan una larga lista de reglas.





## Revolución WWII



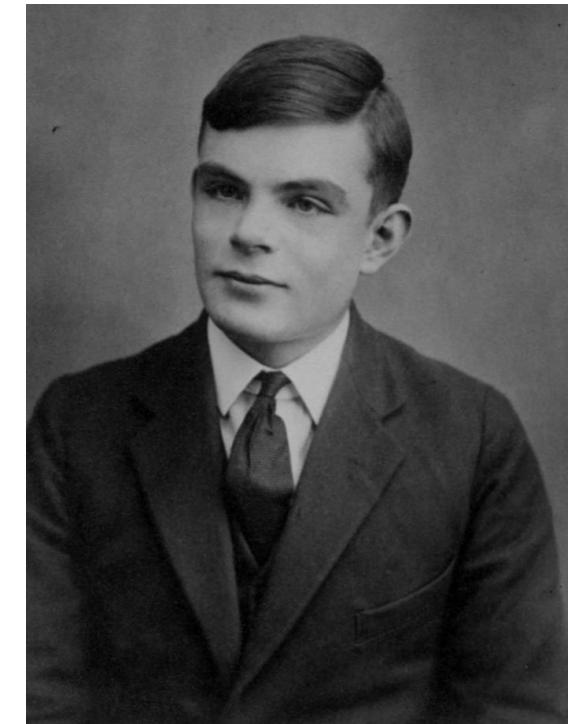
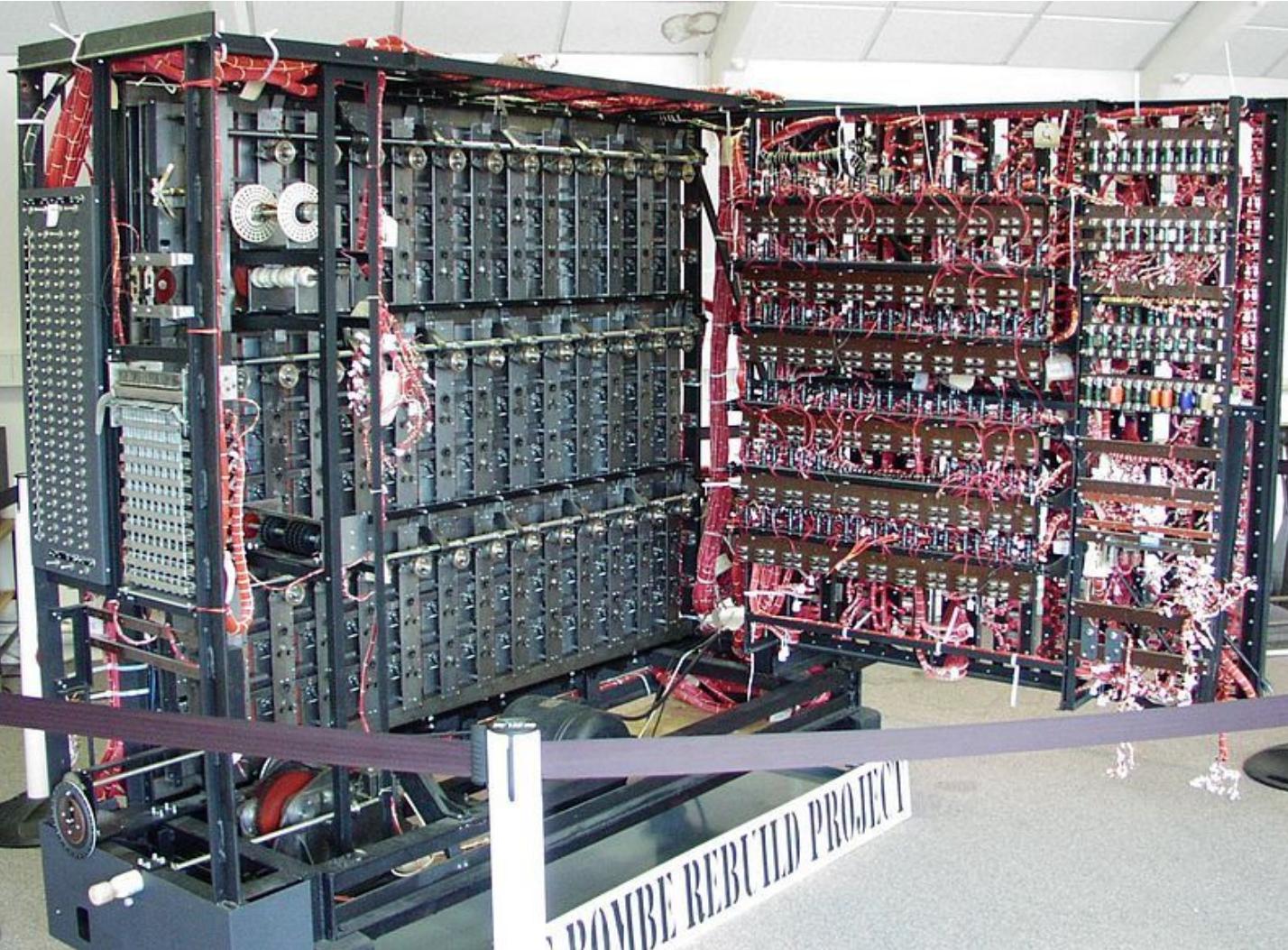
Los sistemas de cifrado se sofistican:  
Se introducen los sistemas de rotores.  
Se industrializan los métodos de  
gestión de claves.

Es humanamente imposible romper el  
cifrado.





# Máquina de Turing

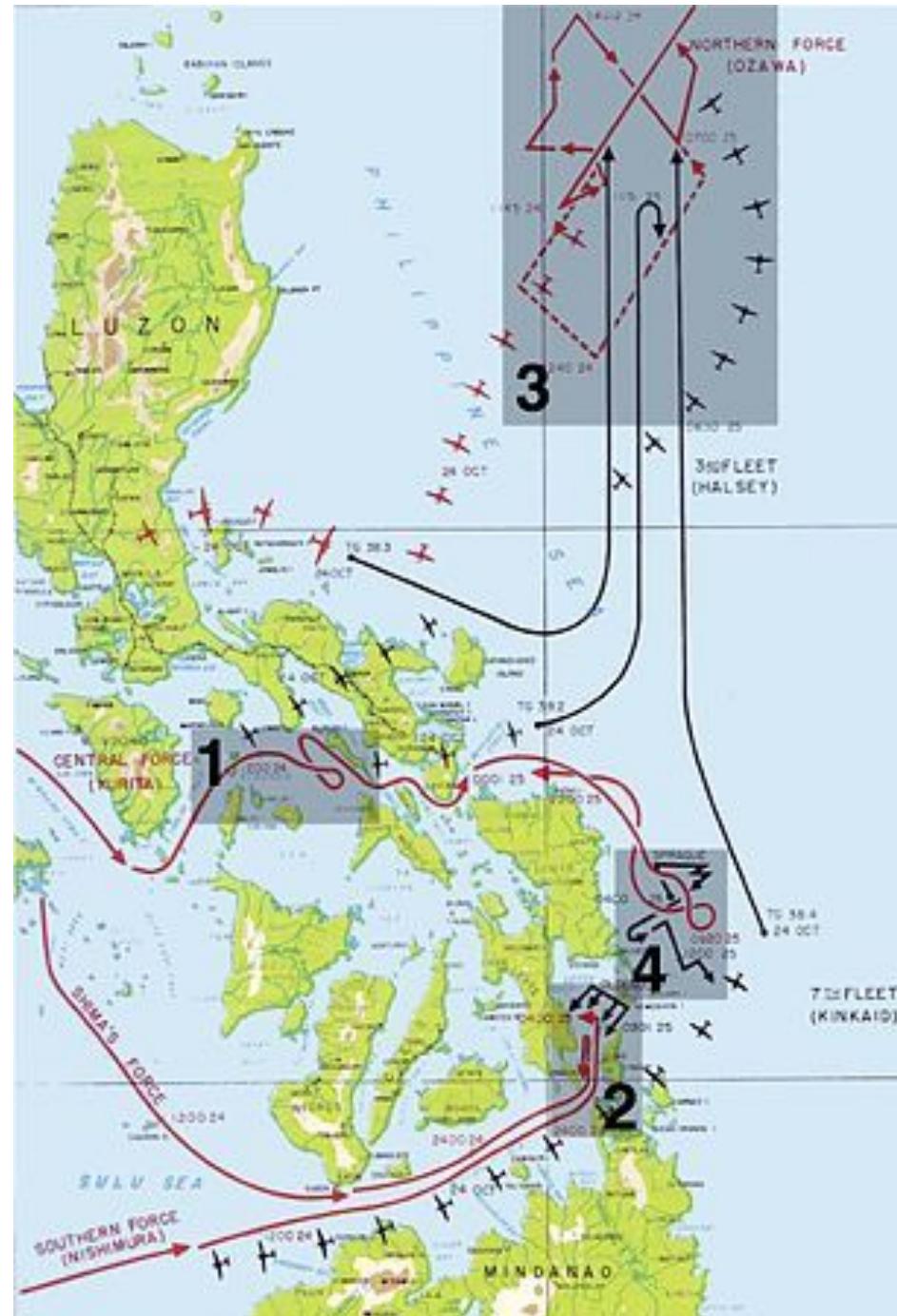


Alan Turing  
1912 - 1954

Descifrando Enigma, 2015



## Padding (relleno)



Para hacer menos predecible el texto plano se puede añadir texto aleatorio al principio y final del mensaje, haciendo más difícil encontrar patrones.

**TURKEY TROTS TO WATER GG FROM CINCPAC  
ACTION COM THIRD FLEET INFO COMINCH CTF  
SEVENTY-SEVEN X WHERE IS RPT WHERE IS TASK  
FORCE THIRTY FOUR RR THE WORLD WONDERS**

Del Almirante Nimitz al Almirante Harshey



# CRIPTOGRAFÍA MODERNA

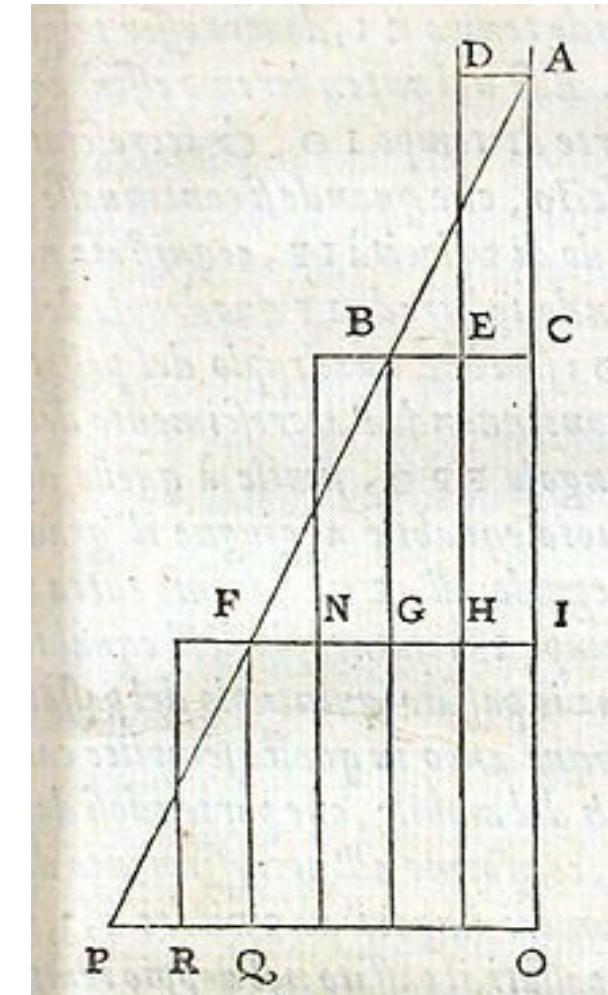




# Una nueva era...

Con la invención de los ordenadores, los cifrados de sustitución quedaban obsoletos porque cualquier complejidad añadida se resolvía añadiendo dicha complejidad al ordenador que lo iba a atacar (relación lineal).

**Comienza el desarrollo de cifrados basados en aritmética**



The derivative of  $f(x)$  with respect to  $x$  is the instantaneous rate of change (slope) of the function at any value of  $x$ .

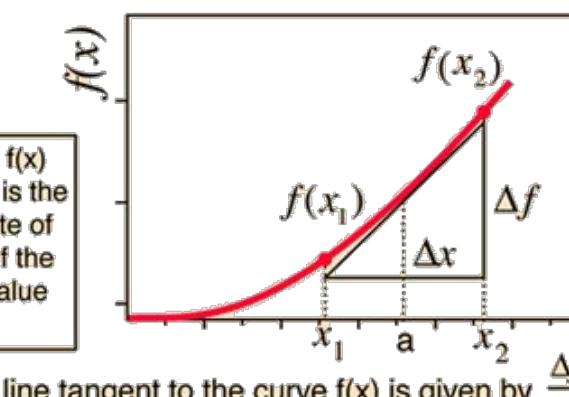
The slope of the line tangent to the curve  $f(x)$  is given by  $\frac{\Delta f}{\Delta x}$

That slope is also given approximately by  $\frac{f(x_2) - f(x_1)}{x_2 - x_1} = \frac{\Delta f}{\Delta x}$  and the approximation would be better if  $x_2 - x_1$  were smaller. The exact slope can be found by taking the limit as  $\Delta x \rightarrow 0$  and that limit is called the derivative of the function  $f(x)$  with respect to  $x$ .

The derivative gives the instantaneous rate of change of the function.

$$\frac{df(x)}{dx} = \lim_{\Delta x \rightarrow 0} \frac{\Delta f}{\Delta x}$$

The value of the derivative at  $x=a$  is equal to the slope to the line tangent to the curve  $f(x)$  at the point  $(a, f(a))$ .



The  $d$  in both numerator and denominator denotes the derivative.

$$\frac{df(x)}{dx} = \lim_{\Delta x \rightarrow 0} \frac{\Delta f}{\Delta x}$$

$x$  is the independent variable upon which the function  $f(x)$  depends.



Nicolás de Oresme 1323 - 1382



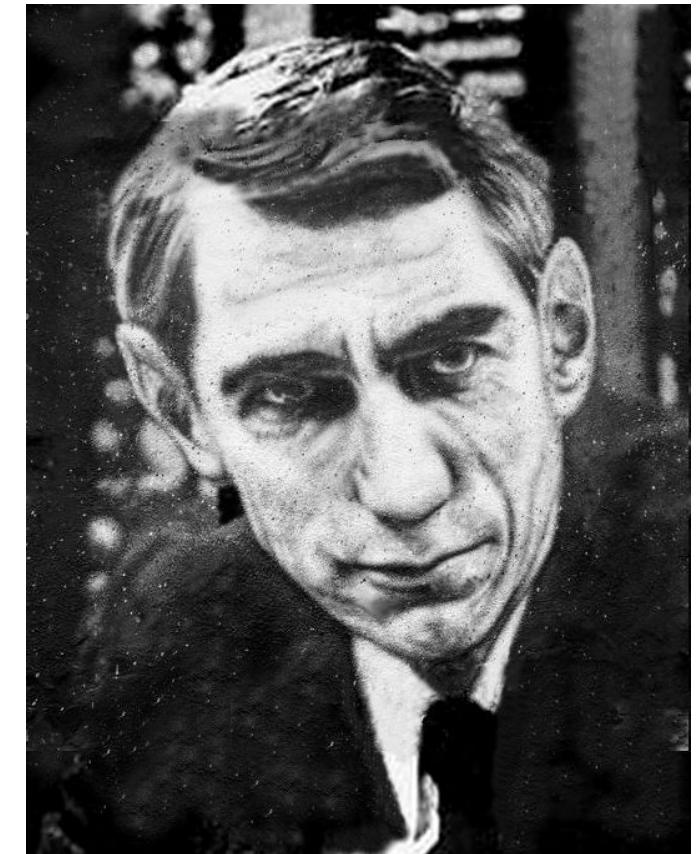
## Teoría de la Información

Durante la 2a Guerra Mundial Shannon creó las bases para los sistemas de comunicaciones actuales.

Se publicaron al acabar la Guerra.

A Mathematical Theory of **Communication**, Bell System Technical Journal 27, 1948

Communication Theory of **Secrecy Systems**, Bell System Technical Journal 28, 1949



Claude E. Shannon  
1916 - 2001





## Cifrados abiertos

Hasta los años 70, el cifrado era un asunto prácticamente exclusivo de gobiernos. Con el avance de las telecomunicaciones y la globalización, las grandes corporaciones comienzan a necesitar cifrado.

Para dar solución a este problema, en 1972 el US National Bureau of Standards empieza una convocatoria para definir un nuevo cifrado abierto.

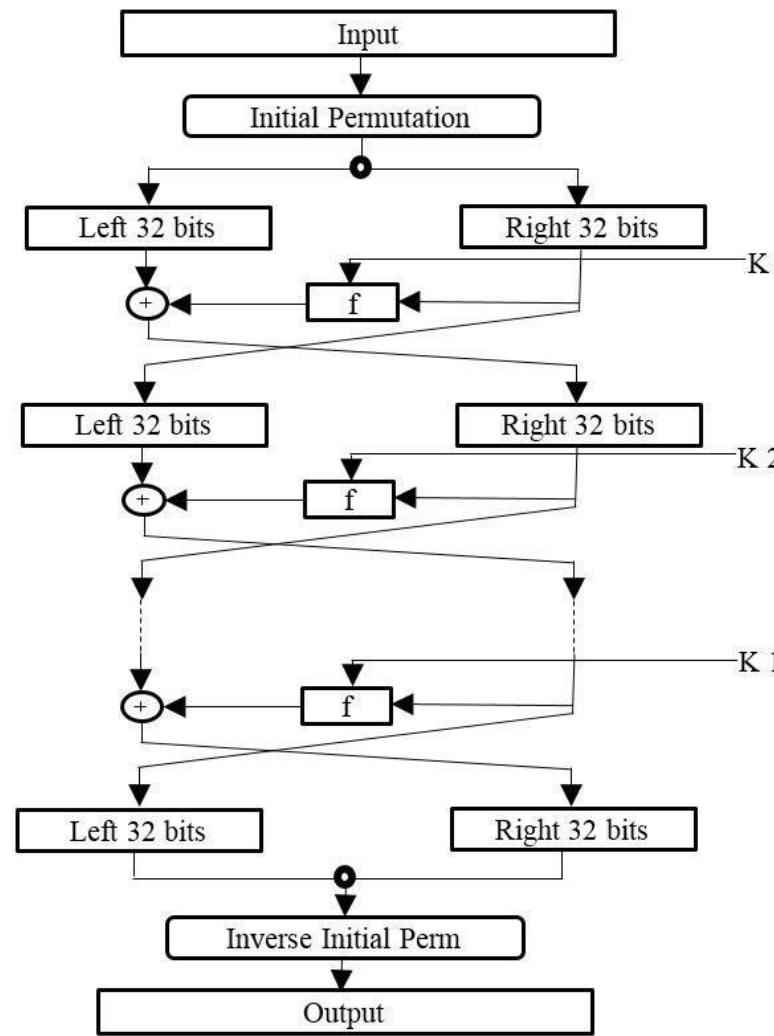
En el 1973 se selecciona la propuesta de IBM y la NSA aconseja hacer unas mejoras.

En 1977 se declara estándar el cifrado DES - Data Encryption Standard

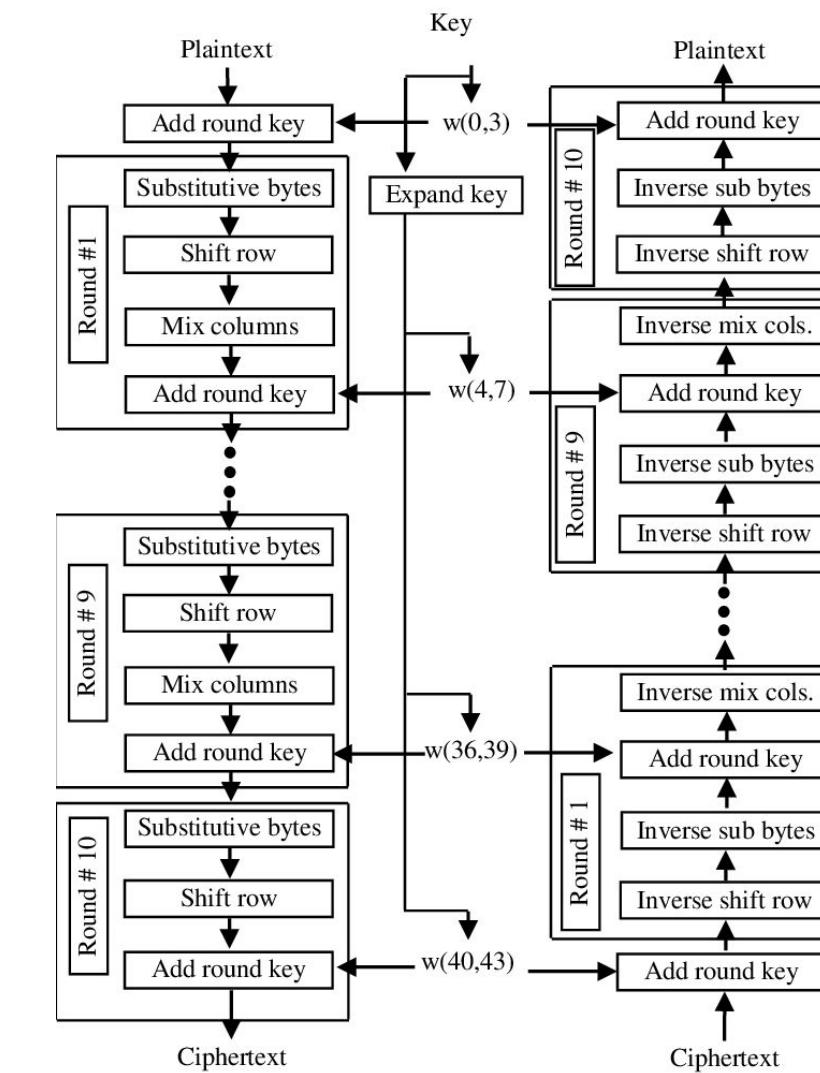
Se mantiene hasta el 2000, con la llegada del AES – Advanced Encryption Standard



# Cifrados avanzados



DES



AES



## El problema de la gestión de claves

En el momento que tenemos cifrados robustos y abiertos, la seguridad de nuestras comunicaciones depende exclusivamente de cómo de secretas son nuestras claves.

Cuando la criptografía era de uso exclusivamente militar, la gestión de estas contraseñas se hacía mediante libros de claves. Pero las organizaciones civiles no tienen los protocolos para custodiar de forma efectiva este tipo de información

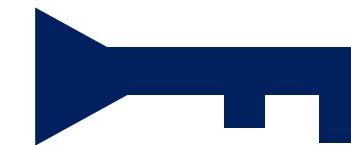




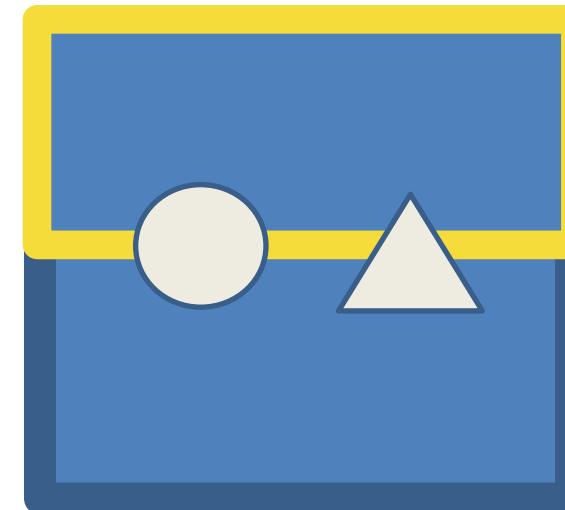
# Criptografía asimétrico o de Clave Pública



Clave  
Pública



Clave  
privada



La información que se cifra con la clave pública se descifra con la clave privada

La información que se cifra con la clave privada se descifra con la clave pública

W. Diffie, M. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory 22 (1976)

Rivest, Shamir, Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM 1978





## La importancia de los primos

Multiplicar dos números primos es una operación sencilla  $7 \times 11 = 77$

Descomponer un número en primos requiere muchas operaciones:

$$77 \div 2 = \text{no} \quad 77 \div 3 = \text{no} \quad 77 \div 4 = \text{no} \quad 77 \div 5 = \text{no}$$

$$77 \div 6 = \text{no} \quad 77 \div 7 = \text{sí}$$

$$11 \div 8 = \text{no} \quad 11 \div 9 = \text{no} \quad 11 \div 10 = \text{no} \quad 11 \div 11 = \text{sí}$$

Se usa el algoritmo de Euclides

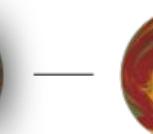




## Trap-door function



muy fácil



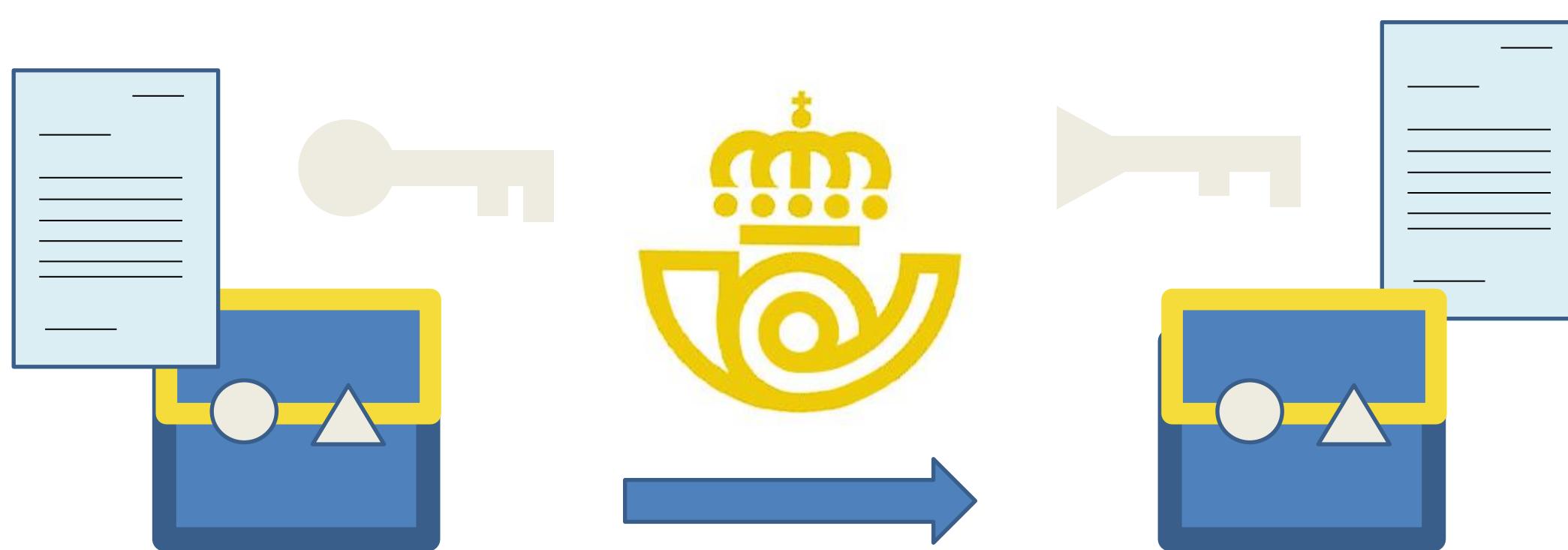
muy difícil

# Criptografía Clave Pública

A quiere hablar con B.

Cifra el mensaje con la pública de B.

B descifra con su privada.





# Firmas Digitales - Autenticación

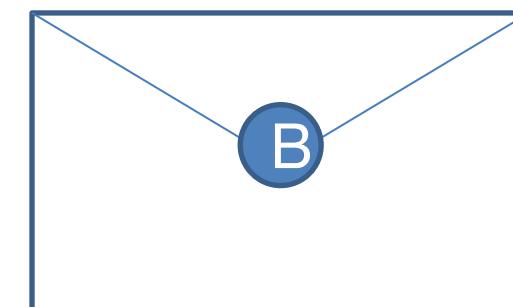
A quiere mandar un mensaje firmado a B

$$F = E(p_a(m))$$

Solo se puede descifrar usando la clave Pública de A. Solamente puede haberlo cifrado A.

Luego cifra con la Pública de B.  
Solamente B puede leer.

$$C^* = E(p_b(F)) = E(p_b(E(p_a(m))))$$



Mensaje claro = m firmado = F cifrado y autenticado =  $C^*$   
Pública =  $P_a, P_b$  Privada =  $p_a, p_b$



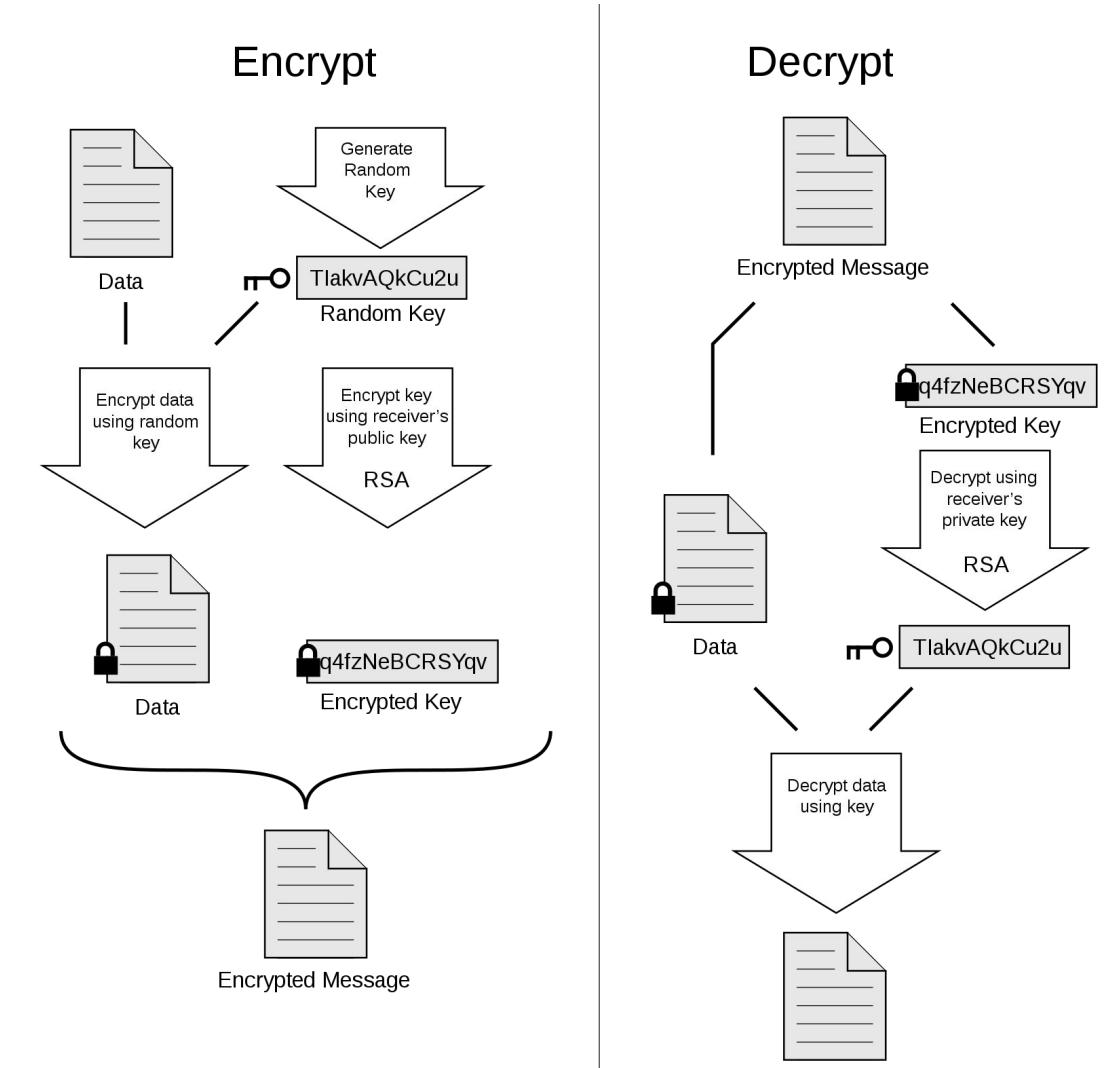


# Criptografía híbrida

La criptografía de clave pública o asimétrica es mucho menos eficiente (por el tipo de operaciones matemáticas que lleva a cabo) que la criptografía simétrica.

Para poder usar criptografía asimétrica de forma eficiente, puedo cifrar mi mensaje con una clave simétrica aleatoria y usar criptografía asimétrica para proteger la clave aleatoria

PGP: Pretty Good Privacy. Zimmermann, 1991



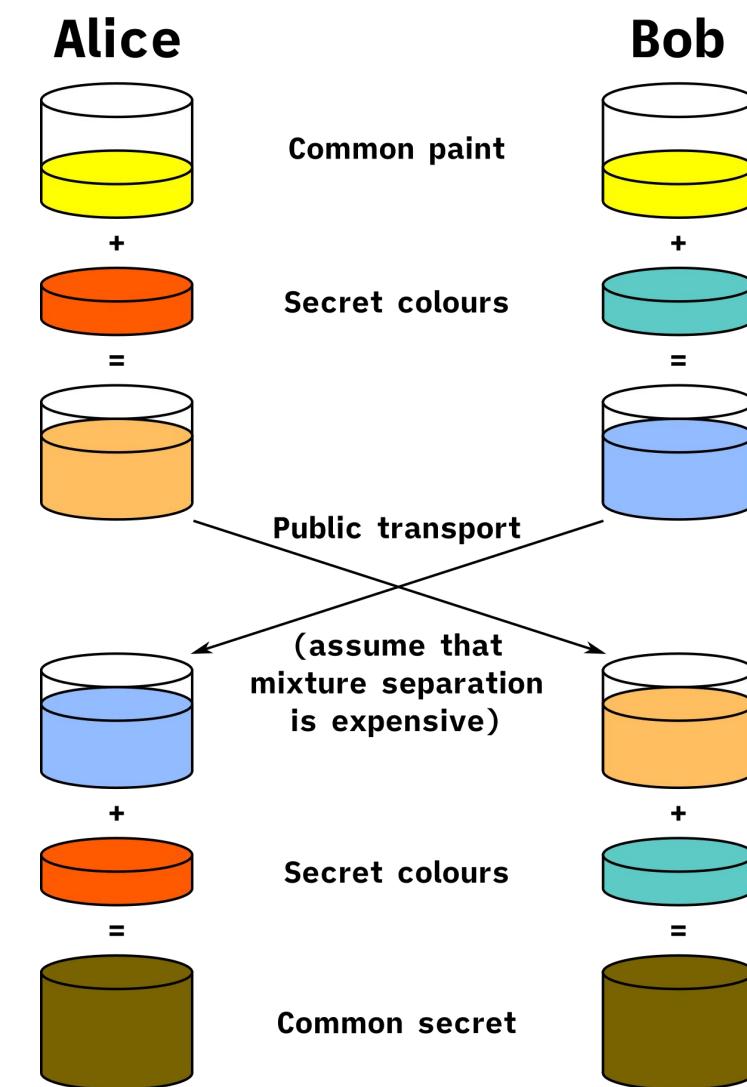


# Establecimiento de claves de sesión

Podemos usar criptografía de clave pública para poder intercambiar claves simétricas. Sin embargo si en algún momento se filtrase la clave privada, se podría recuperar la clave simétrica utilizada en todas mis comunicaciones pasadas.

Para evitar este riesgo existen los esquemas *Perfect Forward Secrecy* en la que la clave simétrica se establece mediante un método de claves asimétricas temporales.

## Diffie-Hellman





## Criptografía para verificación de integridad: Funciones hash

Las funciones hash o funciones resumen sirven para resumir un texto indefinidamente largo en un número fijo de letras.

Actualmente las funciones más seguras son las SHA (Secure Hash Algorithm)

Tienen que tener ciertas propiedades para que sean útiles. Como son funciones resumen, pueden tener colisiones donde diferentes textos pueden tener el mismo resultado.

En un lugar de la  
Mancha...

**ISBN-13:** 978-0307475411

Si cambia la tapa, editor... cambia ISBN





## Infraestructura de clave pública



Para que estos sistemas sean útiles deben de incorporar un interfaz de usuario, etc.

Llamamos a este interfaz sistema de gestión de claves o PKI.

Aparece el problema de quién guarda las claves... y quien las genera.

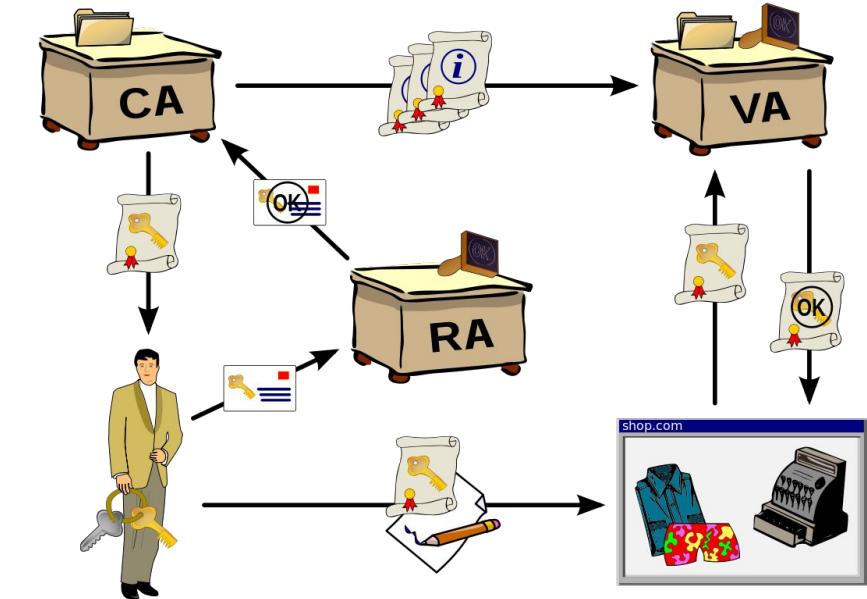


# Certificados Digitales

Todos los usuarios aceptan un tercero de confianza:

- Google
- Verisign
- Fábrica Nacional de Moneda y Timbre

...



Ese tercero firma todas las claves públicas del repositorio.

Los usuarios saben que esas claves son válidas, ya que pueden verificarlas con la clave pública del tercero.

A esas claves públicas firmadas las llamamos certificados.

Normalmente los navegadores de internet vienen con varias entidades pre-cargadas.





# Certificados Digitales

Para que un certificado sea confiable debe estar firmado por una Root of trust de confianza para el usuario

The screenshot shows a web browser window for <https://car.navarra.es/CAR/PreLoginCert.aspx?id=10005&referrer=https%3a%2f%2fhacienda.navarra.es%2fCertificadosEr>. The address bar includes icons for a lock and a warning sign. The main content area displays the Navarra.es logo and navigation menu (RÁMITES, TEMAS, GOBIERNO, ACTUALIDAD). A sidebar on the left contains a warning message: "car.navarra.es La conexión no es segura" and "Permisos: No ha concedido ningún permiso especial a este sitio." Below this, a red box highlights the "Certificado de Usuario" section, which states: "Utilice un certificado digital válido para acceder. Consulte las [certificaciones admitidas](#) para las tramitaciones on-line." A "Continuar" button is at the bottom of this section. To the right, another red box highlights the "Otros accesos" section, which includes a link to "DNI + PIN".





# Certificados Digitales

## ¿Podemos confiar en las Root of trust?

Security

### French gov used fake Google certificate to read its workers' traffic

Liberté, égalité ... invisibilité: Homme-dans-l'intermédiaire snooping at treasury dept

By John Leyden 10 Dec 2013 at 16:55

49 SHARE ▾



A French government agency has been caught signing SSL certificates and impersonating Google.

SC Media US > News > Gogo caught using fake Google SSL certificates



by Teri Robinson, Executive Editor

Follow @TeriRnNY

January 06, 2015

### Gogo caught using fake Google SSL certificates



Fliers who don't want their data intercepted by Gogo LLC, or unnecessarily fall into the hands of law enforcement, might want to reconsider using the inflight WiFi service after it was found to be using fake Google SSL certificates.

The practice, which essentially sets up a **man-in-the-middle** (MitM) attack of sorts, was discovered by Google engineer Adrienne Porter Felt, who logged into Gogo WiFi during a recent flight.

After seeing a telltale red "x" in her address bar, warning that the certificate for a site "was signed by an untrusted issuer," Felt realized that Gogo, not Google, had signed it.



Gogo caught using fake Google SSL certificates





## Esquema de seguridad para comunicaciones

Actualmente los sistemas de comunicaciones seguros en internet se basan en la combinación de varias tecnologías criptográficas:

- La autenticación del servidor se realiza mediante certificados de clave pública de tamaño suficiente firmados por una fuente de confianza
- La clave de sesión se establece en el inicio mediante un sistema de tipo Diffie-Hellman o equivalente
- La clave de sesión pactada se utiliza para cifrar la información con un cifrado robusto como AES
- A los mensajes se les añade una capa de verificación de integridad basada en funciones hash (HMAC) para evitar que sean manipulados durante el tránsito



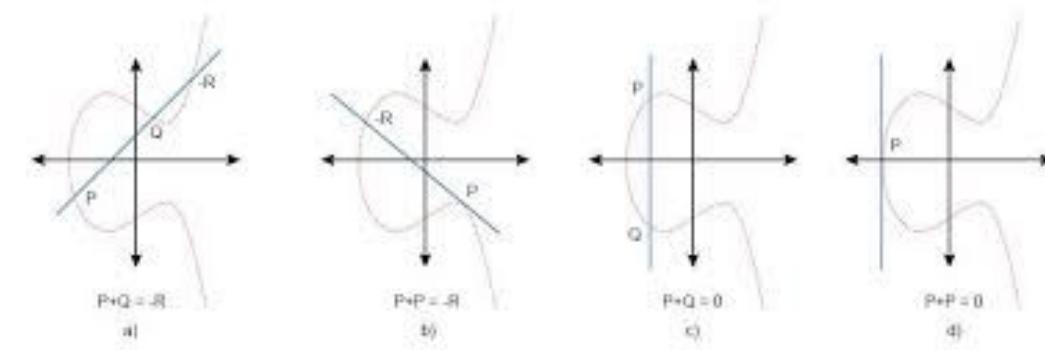
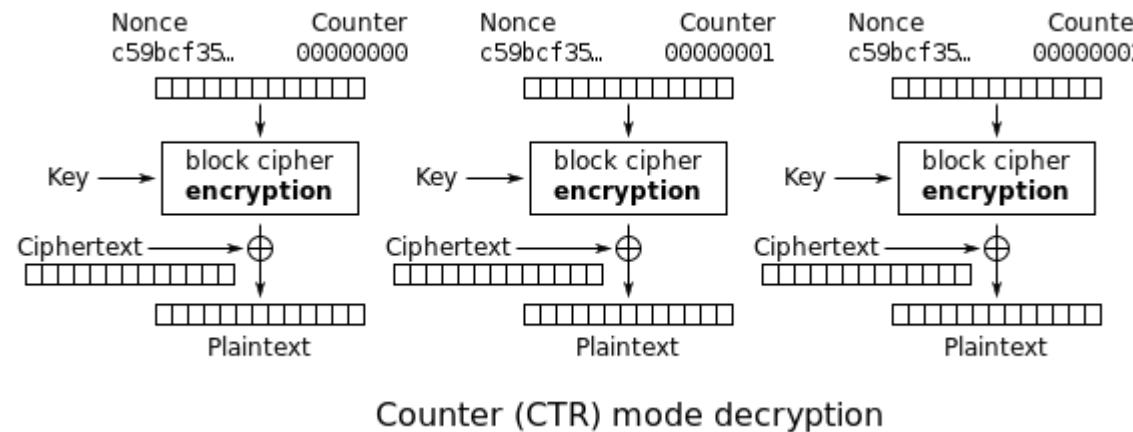


# Reduciendo costes: Cifrados de flujo y curvas elípticas

El esquema anterior es robusto pero tiene el problema de que tiene un coste computacional alto que crece al aumentar el volumen de información.

Para el cifrado simétrico de grandes volúmenes de información como voz o vídeo, se pueden usar cifrados de flujo, que a menudo son menos robustos pero con menor coste computacional

Para reducir el consumo de la criptografía asimétrica podemos usar curvas elípticas, que ofrecen un sistema casi igual de robusto por una fracción del coste computacional



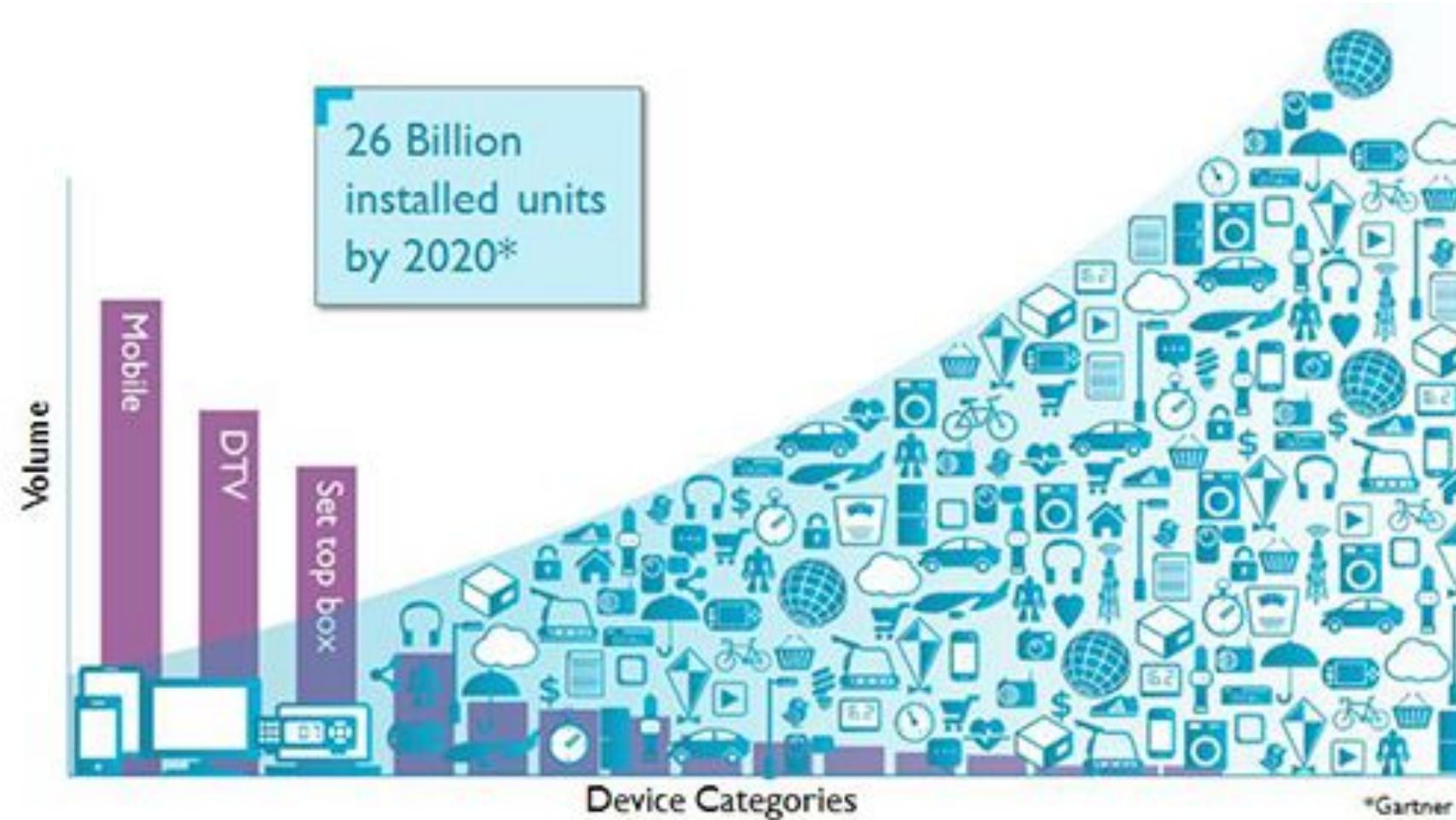
# INTERNET OF THINGS





## Efectos Colaterales

Más y más datos están siendo enviados...

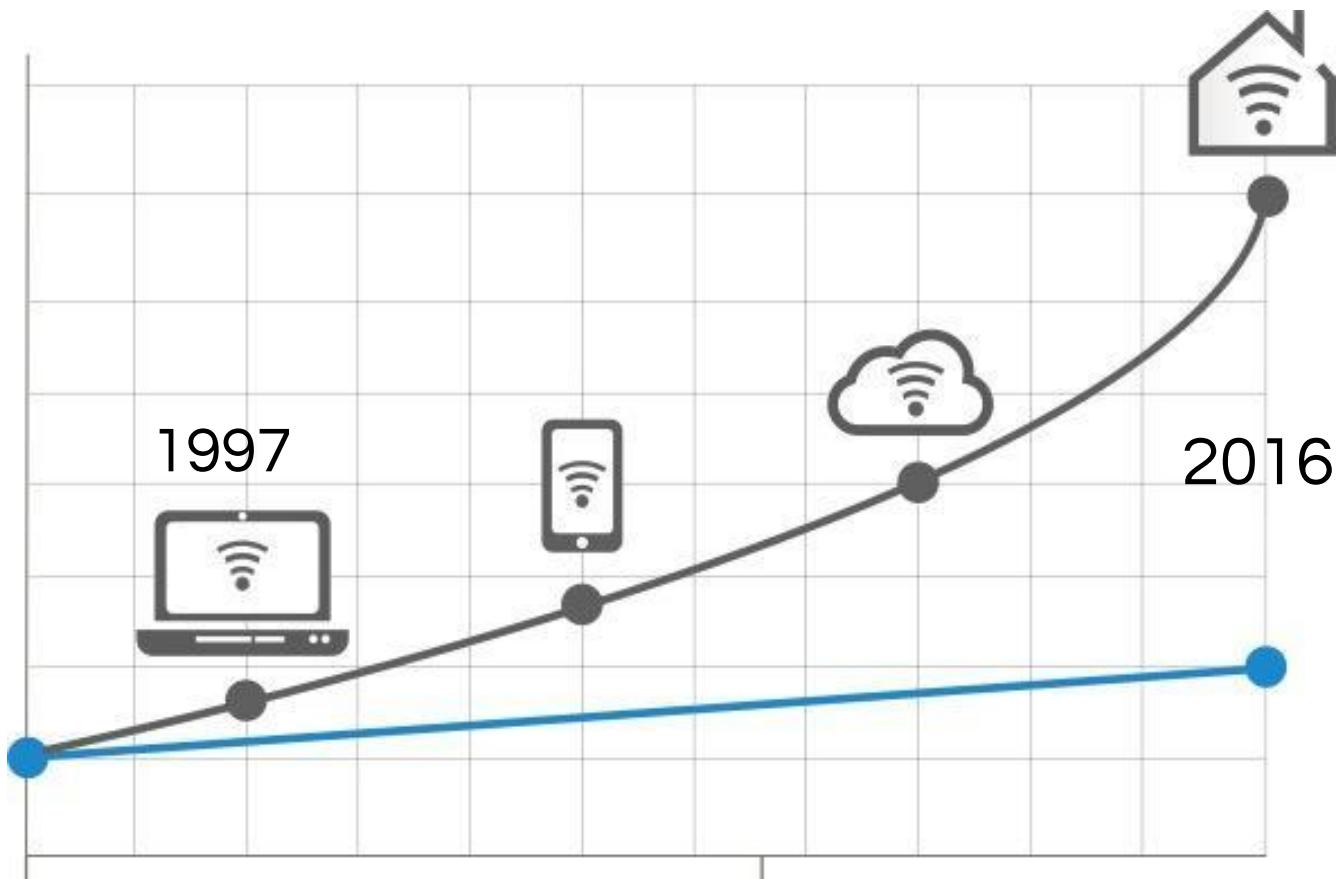


...y algunos canales de datos no son fáciles de proteger.





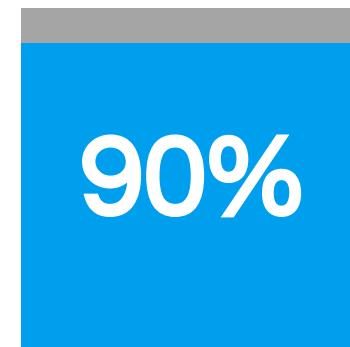
# ¿Por qué IoT es un desafío para la ciberseguridad?



- Tecnologías de la información
- Tecnologías de cifrado



## Dispositivos IoT



Envían datos personales

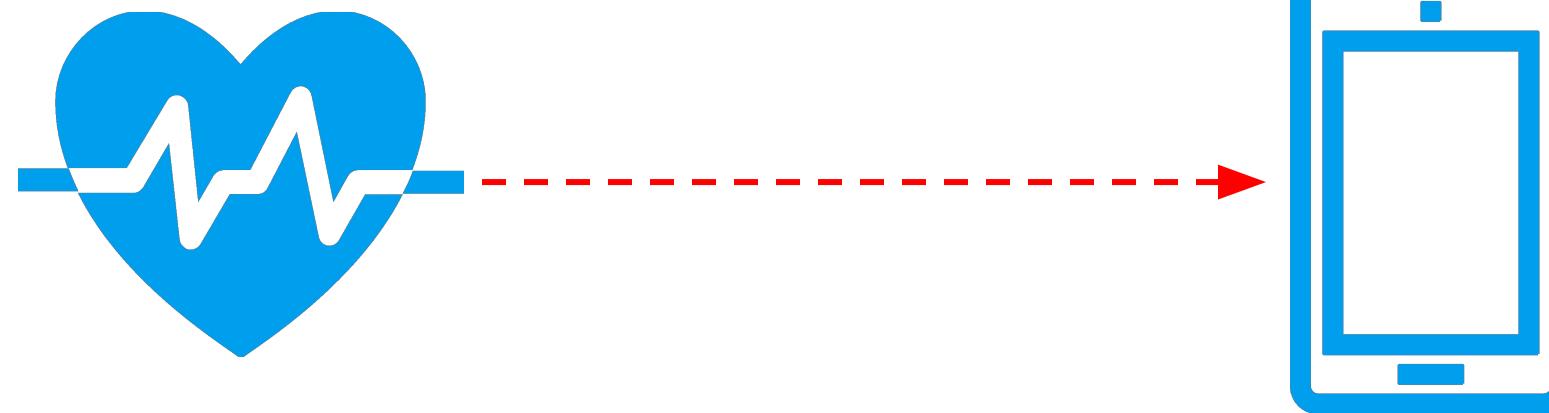


Usan cifrado





## Desafío: Capacidad del sensor para cifrar



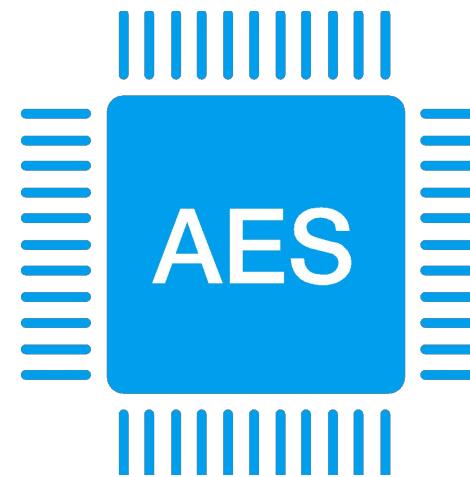
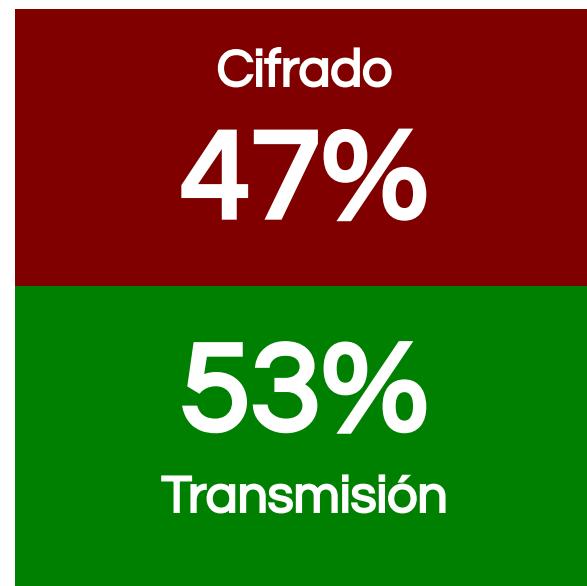
¿Viaja la información por  
un canal seguro?





# Actualmente, se utiliza el cifrado AES

## CONSUMO DE ENERGÍA



- AUMENTA EL TAMAÑO
- COSTE ADICIONAL

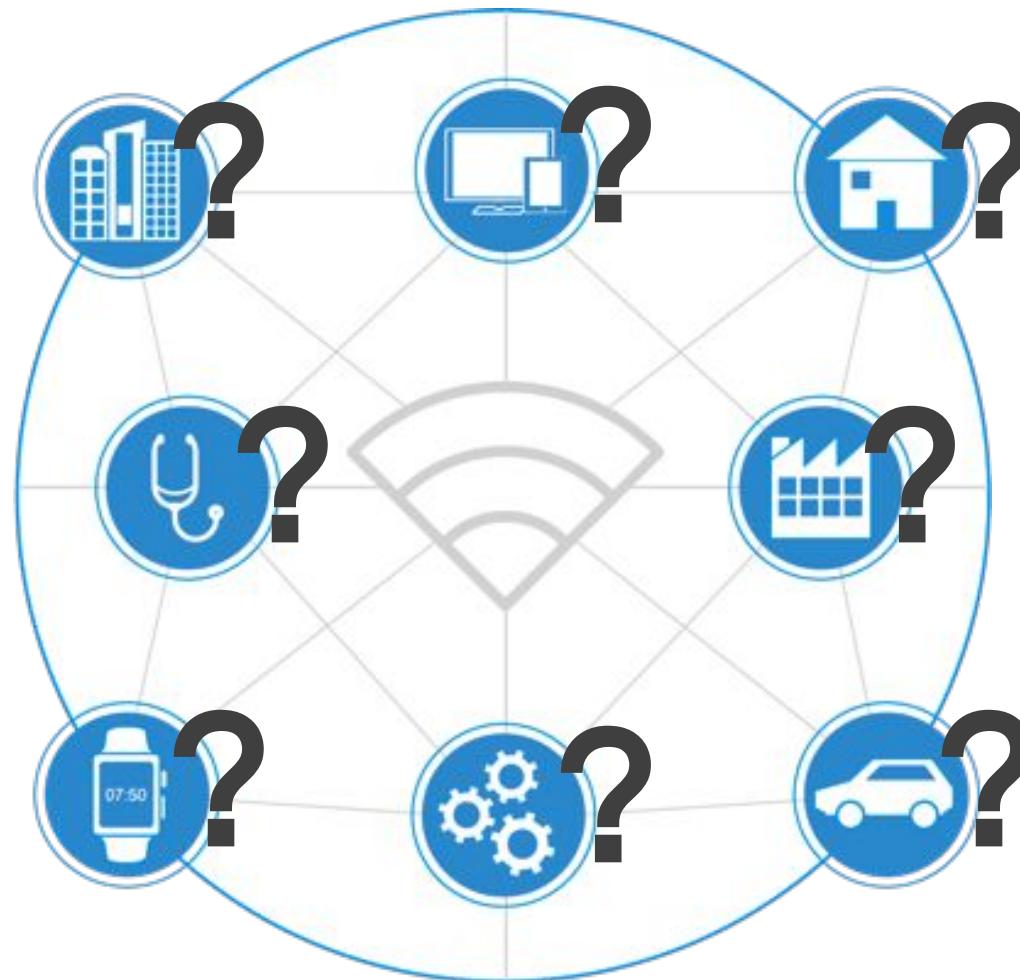
**Aceleradores AES mediante HW dedicado**  
son usados para garantizar la seguridad de  
los dispositivos IoT





# Autenticación de los dispositivos

¿Cómo sabes quién es quién?



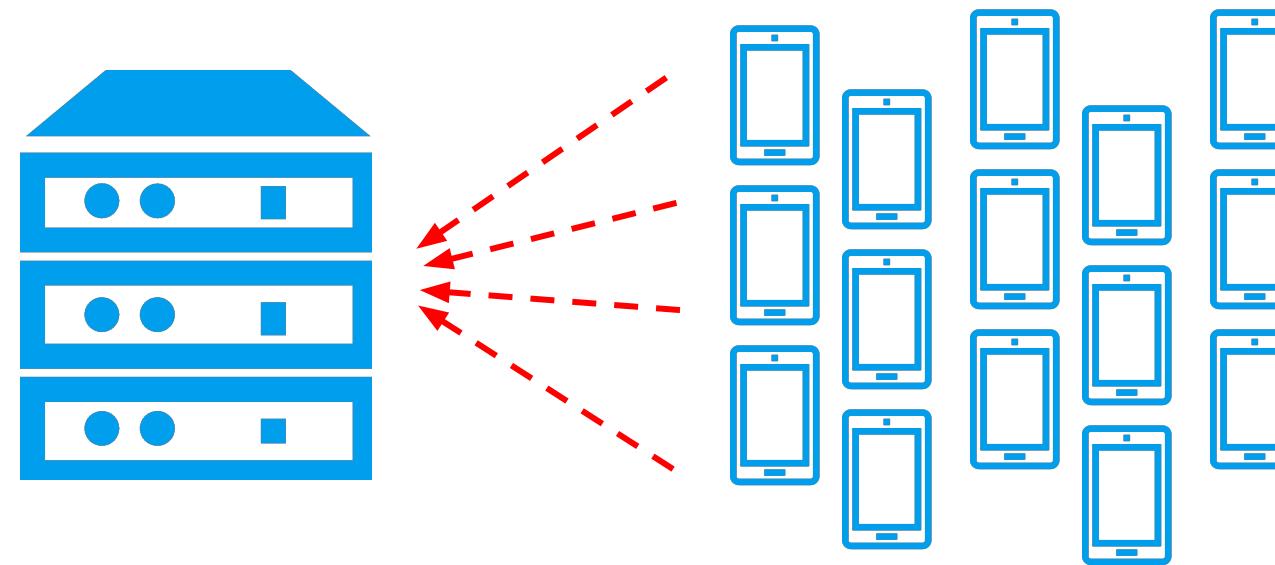
Imagina una llave maestra para 30 billones de dispositivos

Además, muchos de estos sistemas no tiene capacidad computacional para usar criptografía de clave pública





## Desafío 1: Autentificación

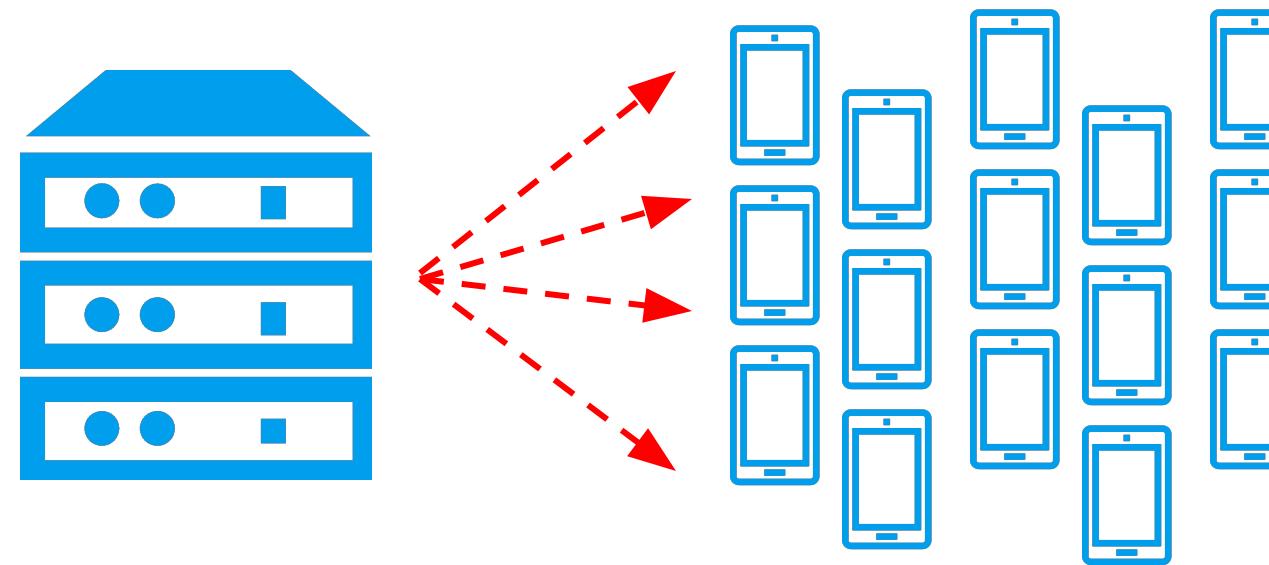


¿Cómo puedo identificar al  
receptor?





## Desafío 2: Escalabilidad



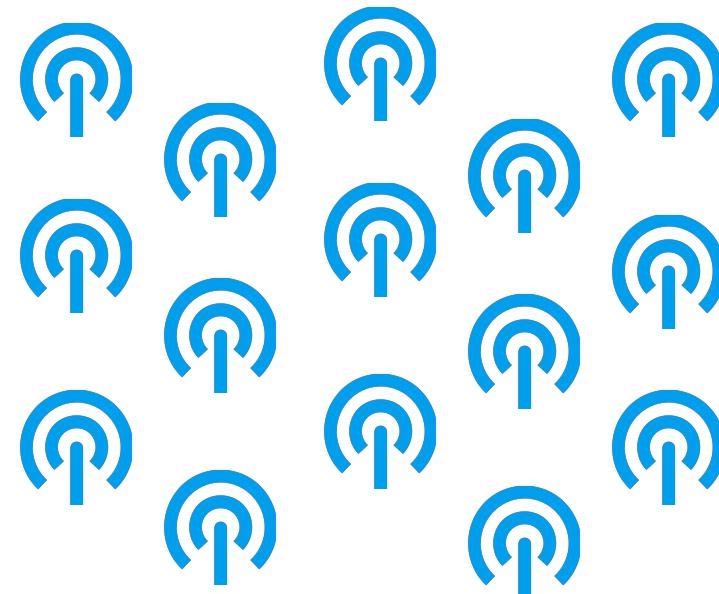
¿Cuántos dispositivos puede  
gestionar un servidor?





# El mundo real de las Infraestructuras Críticas

**10,000x**



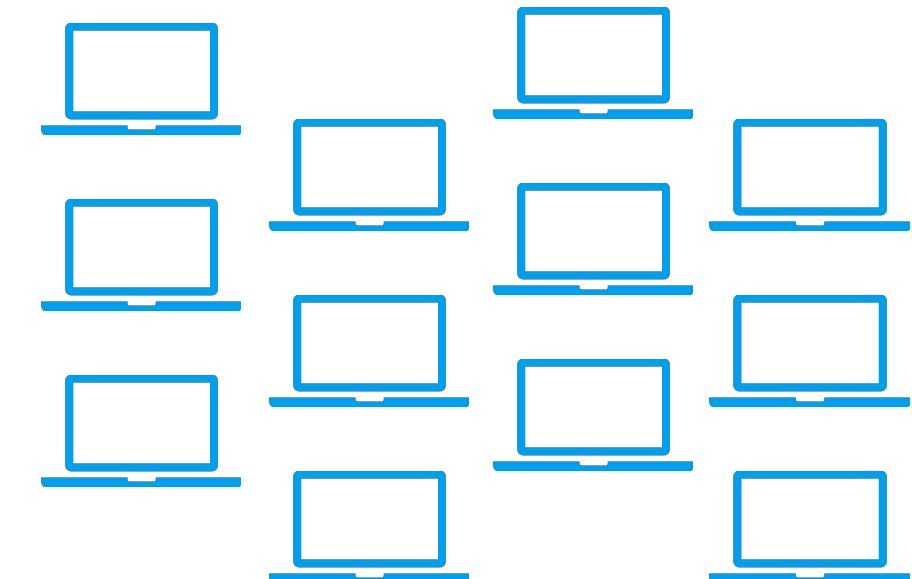
**Sensores**

**1x**



**Servidor**

**100x**

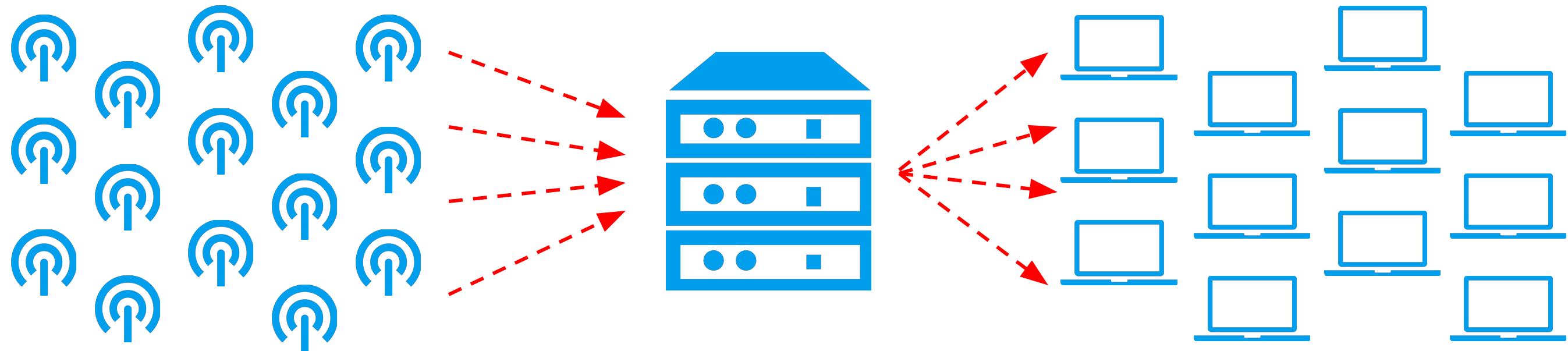


**Centro de control**





# Desafío: Todos los problemas juntos

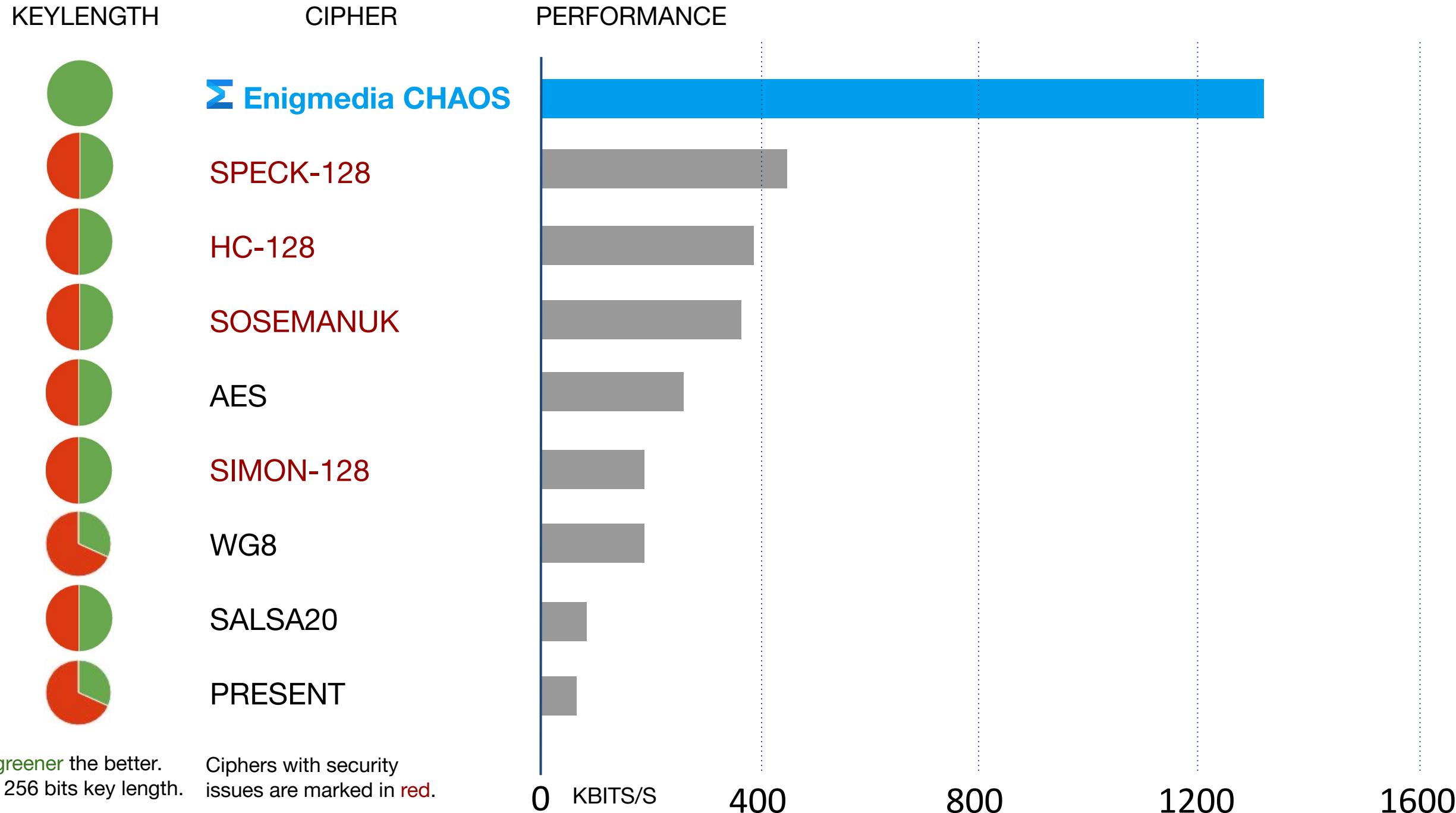


- Capacidad del sensor
- Propiedad
- Autentificación
- Escalabilidad





# Enigmedia encryption: Performance in TI MSP430



# BLOCKCHAIN





En 2008 se propone un método transacción monetaria digital sin intermediarios:

Descentralizado

Transparente

Anónimo

Seguro



# CRIPTOGRAFÍA

# Base de Datos Contable: Ledger

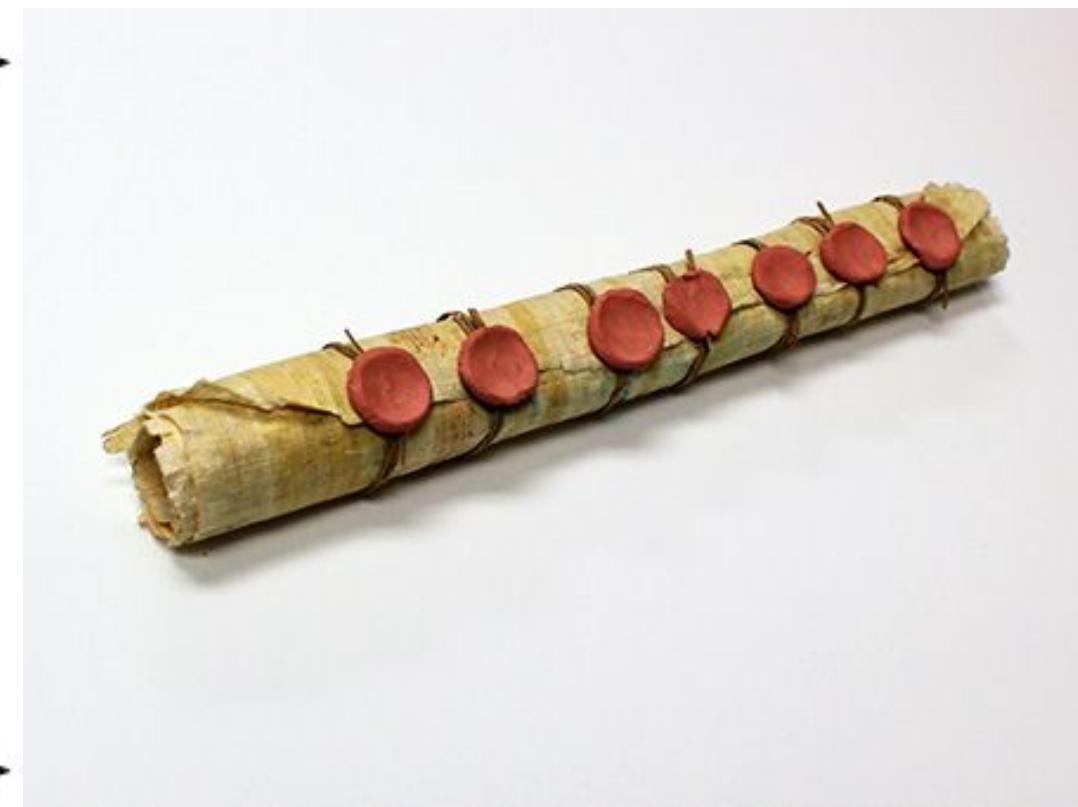
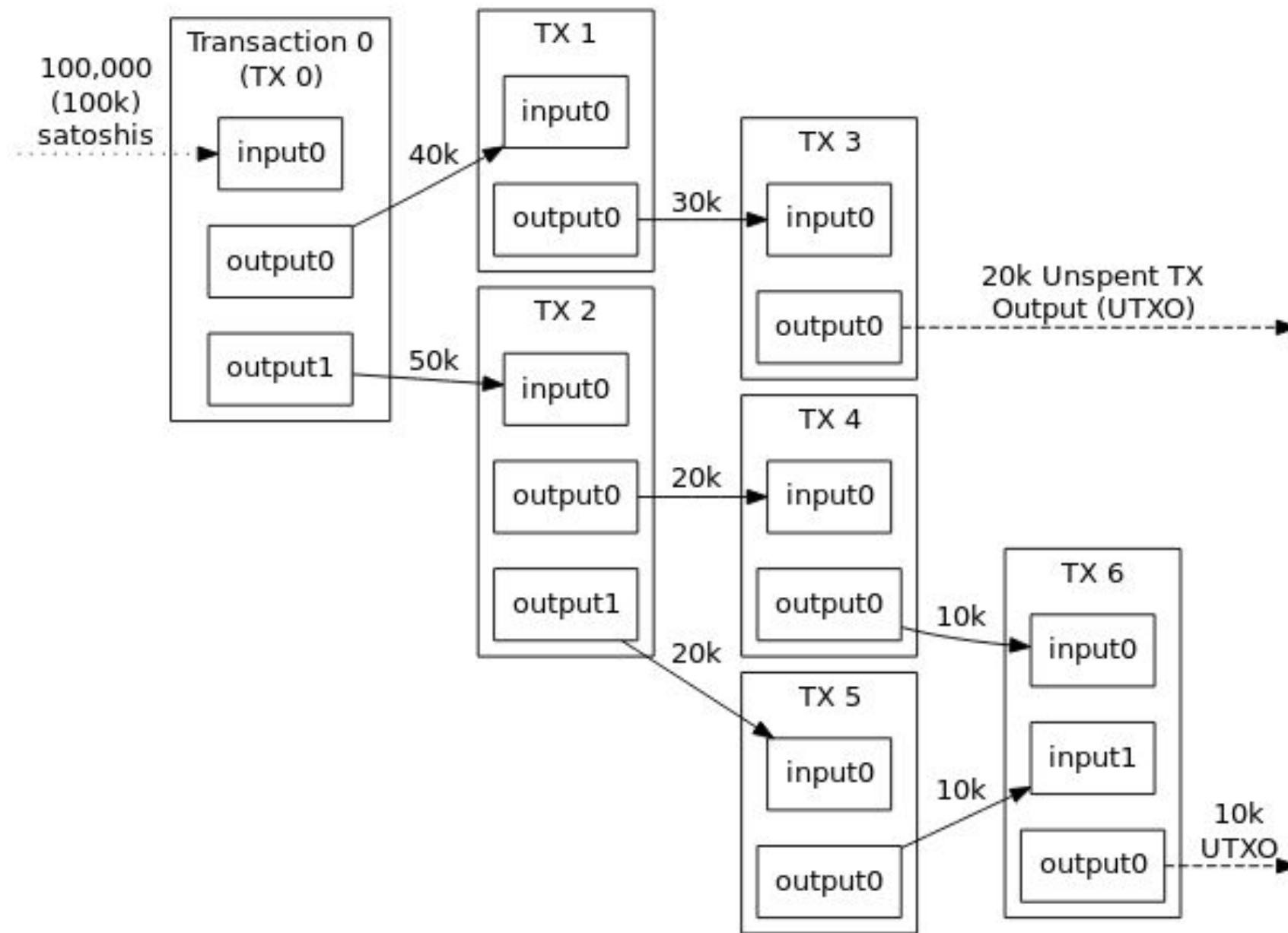
El ***ledger*** o **libro contable**, es un registro de todas las transacciones realizadas hasta la fecha.

Deben existir maneras de resumir este libro para que pueda ser factible no tener que revisar todas las transacciones pasadas.

Deben existir métodos para que haya consenso sobre el estado del libro contable



# ¿Como validamos el ledger?



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin



# Consenso, la vidilla de los sistemas distribuidos

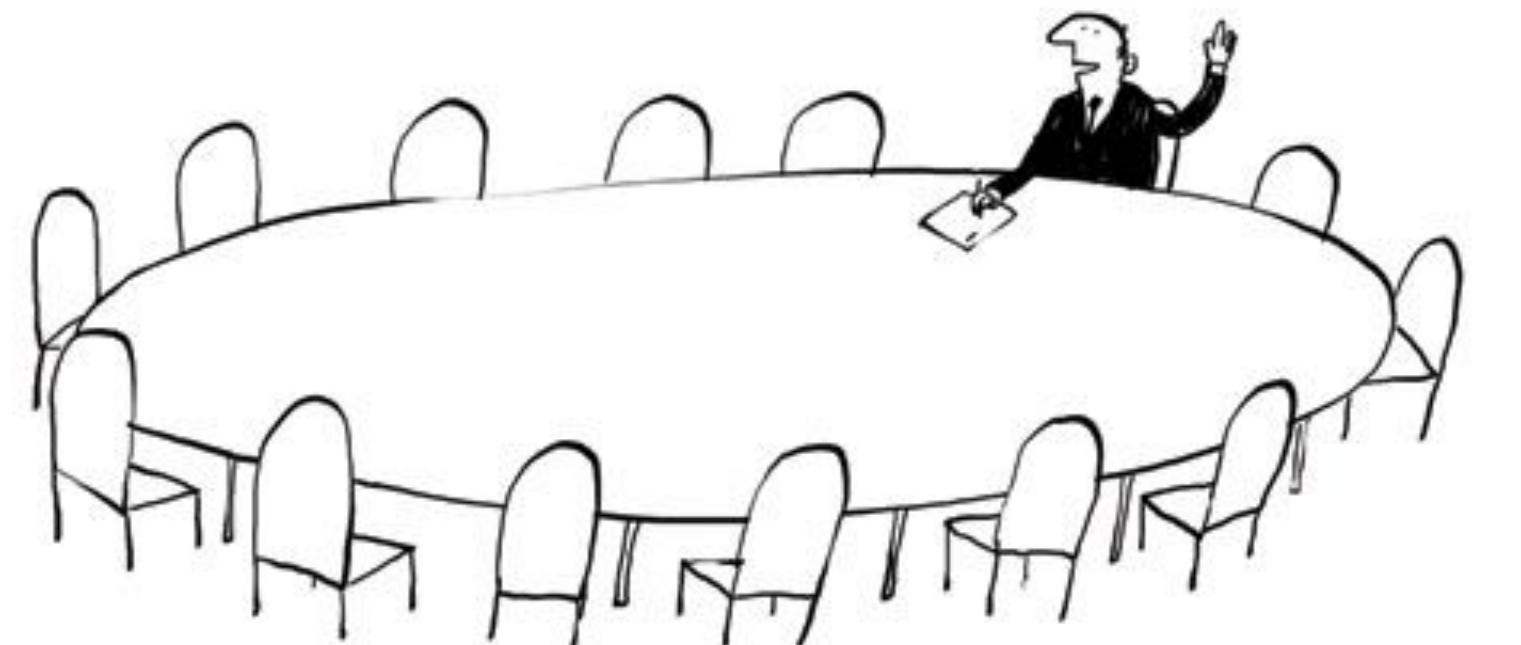
***¿Cómo sabemos que todas las partes están de acuerdo y han recibido la misma información?***

Enviar un acuse de recibo.

***¿Y si el acuse de recibo no llega?***

Aquí tenemos un problema típico de telecomunicaciones!

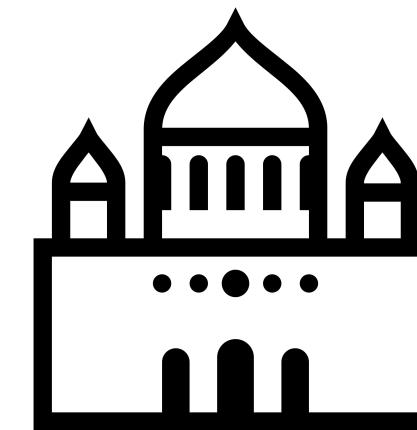
**ESTA ES LA DIFERENCIA ENTRE  
UNA BBDD Y BLOCKCHAIN**



**"It looks like we have a consensus."**



# Problema de los generales bizantinos - versión simple



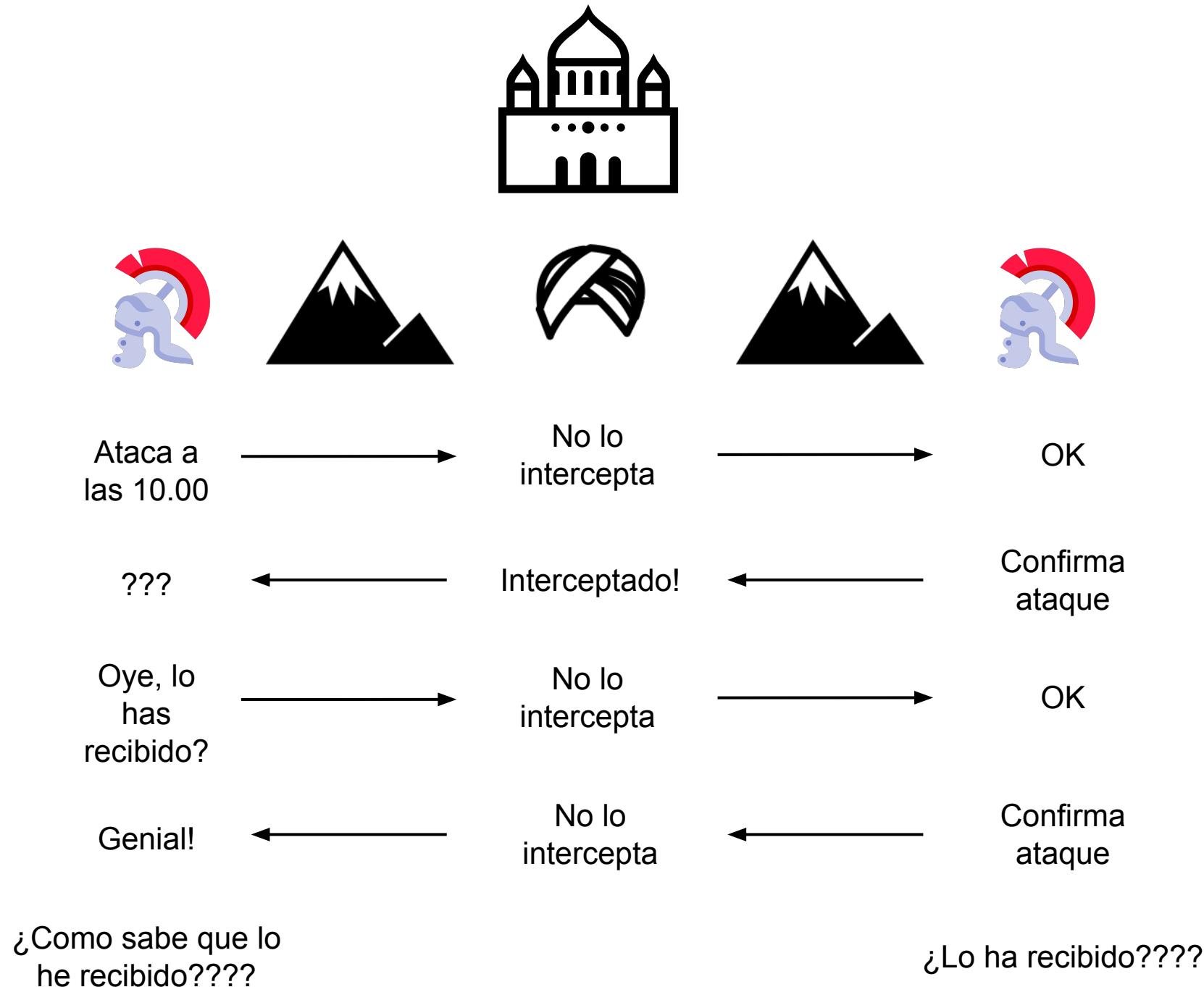
Los generales tienen que atacar la ciudad a la vez, de lo contrario morirán.

Tienen que coordinarse para poder atacar. Están separados por un valle ocupado por el enemigo.

Para simplificar el problema el enemigo no puede mandar información falsa. Tampoco es importa si lee el contenido de la información. Sólo puede interceptar el mensajero e impedir que llegue al otro general.



# Problema de los generales bizantinos - versión simple

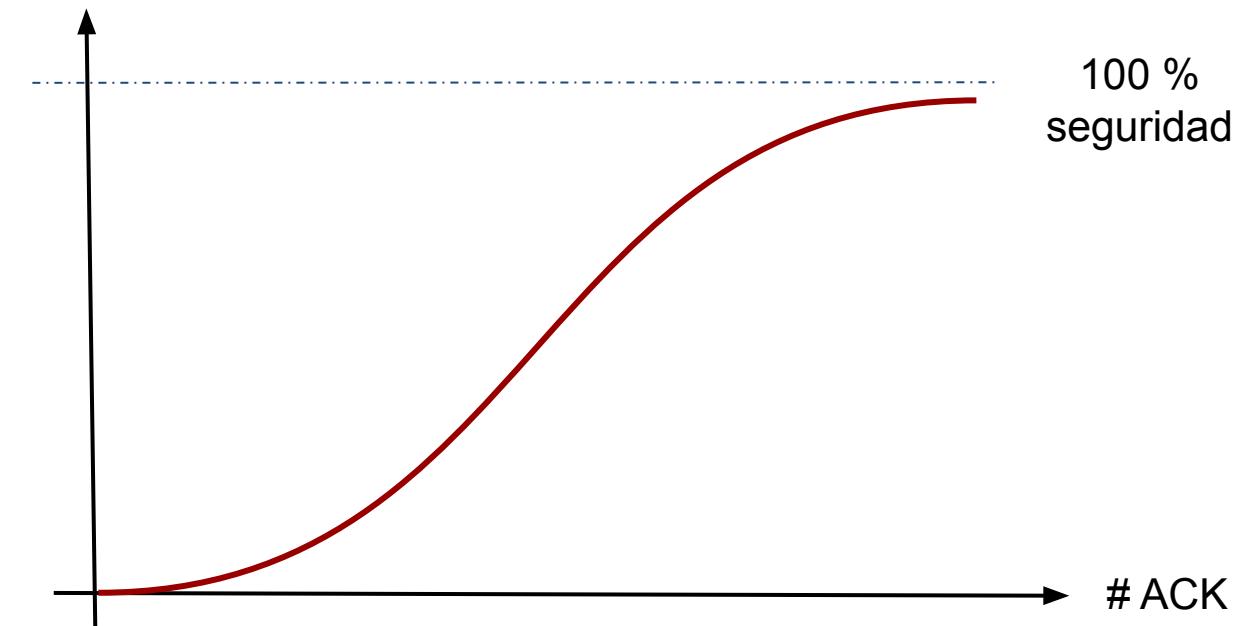




# Problema de los generales bizantinos - versión simple

Los generales quieren asegurarse de que están coordinados, pero NUNCA estarán al 100% seguros.

A medida que añadimos confirmaciones nos acercamos al 100% de seguridad, pero es imposible tener una certeza!



**Siempre hay una probabilidad de fallo.  
En blockchain se suele confiar con un consenso del 51%**

**Se usan funciones hash como mecanismo de Proof-of-Work a la hora de crear nuevos bloques**

**Se utilizan firmas digitales y hashes para resumir la cadena anterior**

**Los monederos se gestionan mediante criptografía de clave pública.**

**El identificador de un monedero es un hash de la clave pública del monedero**

**Se utilizan sistemas criptográficos de no repudio para establecer consenso**



**Ninguno de los elementos técnicos son nuevos, pero la combinación de todos ellos sí lo es.**

- **No es escalable**
- **Gran coste energético**
- **Baja velocidad de verificación**
- **Inmutable: no compatible con derecho al olvido**
- **No hay un marco regulatorio**
- **Brechas de seguridad en los smart contracts**



# Criptografía post-cuántica





A diferencia de los ordenadores clásicos que se basan en transistores, los ordenadores cuánticos se basan en Qubits

Los qubits se basan en el principio de superposición, una partícula puede estar en varios estados “a la vez”. Hasta que no haga una medida, no me quedaré con un único estado.

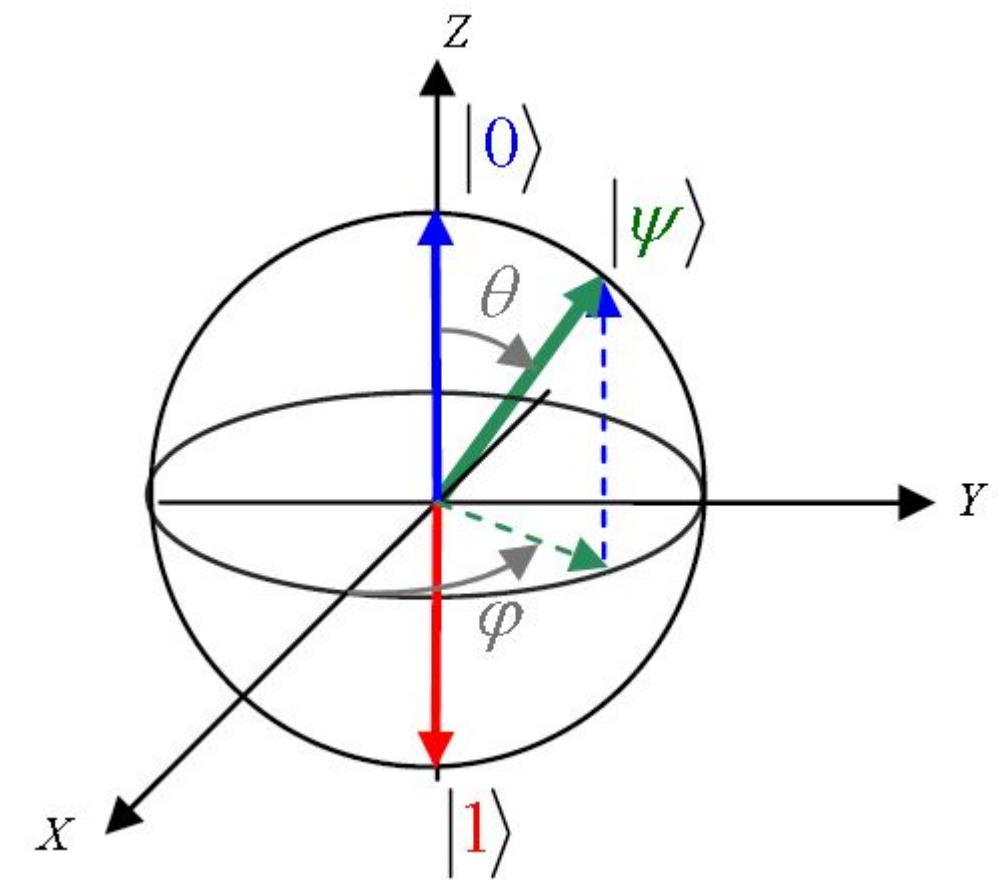
¡Las operaciones se convierten en probabilísticas!



Operadores de Pauli - son características de un sistema cuántico.

Puedo definir estados “a discreción”.

Para representar esa información se usa la Esfera de Bloch



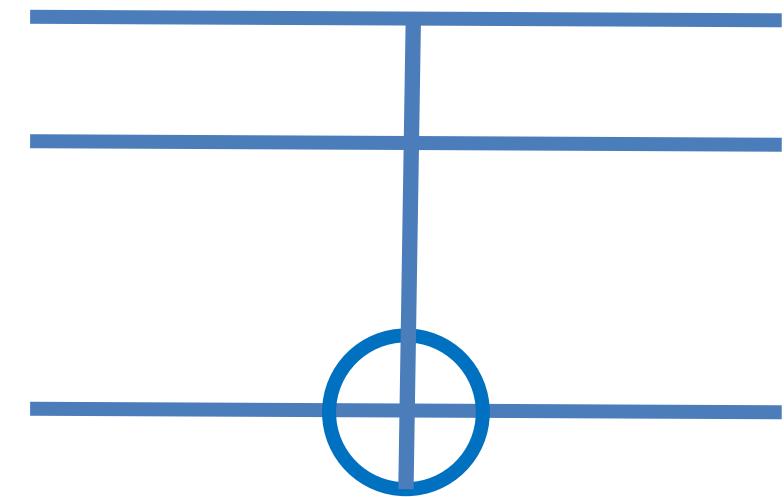


## Puertas Lógicas Cuánticas

Permiten hacer operaciones con qubits.

Son análogas a las puertas lógicas clásicas.

A diferencia de las clásicas, permiten operaciones con estados indeterminados.



Puerta de Toffoli  
CCNOT





## ¿En que afecta la computación cuántica a la criptografía?

- La criptografía de clave pública se basa en números primos
- Para romper la criptografía de clave pública necesito factorizar la clave en los números primos que he usado para crearla
- ¿Que necesitaría para factorizar una clave pública de 2000 bits usando un ordenador cuántico?
  - Número de qubits físicos necesarios = 500 M (disponible dentro de ~ 10 años)
  - Potencia requerida ~ una planta nuclear dedicada
  - Tiempo de procesado de un ordenador cuántico = **¡24 horas!**

**¡La computación cuántica tiene sobre la criptografía actual el mismo efecto que tuvo la computación clásica sobre los cífrados de sustitución!**

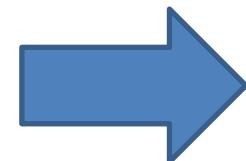




## Implicaciones cuánticas en la criptografía actual

Asimétrica - FIPS 186-4, SP 800-56A/56B

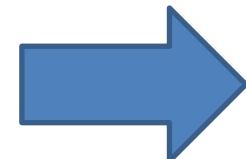
- RSA
- Elliptic Curve Cryptography (ECDSA)
- Finite Field Cryptography (DSA)
- Diffie-Hellman key Exchange



ROTO

Simétrico - FIPS 197, SP 800-57

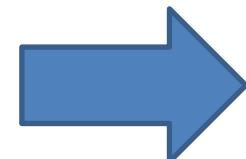
- AES
- Triple DES



X2 CLAVE

Hash - FIPS 180-4, FIPS 202

- SHA-1, SHA-2 and SHA-3



AUMENTAR  
CLAVE

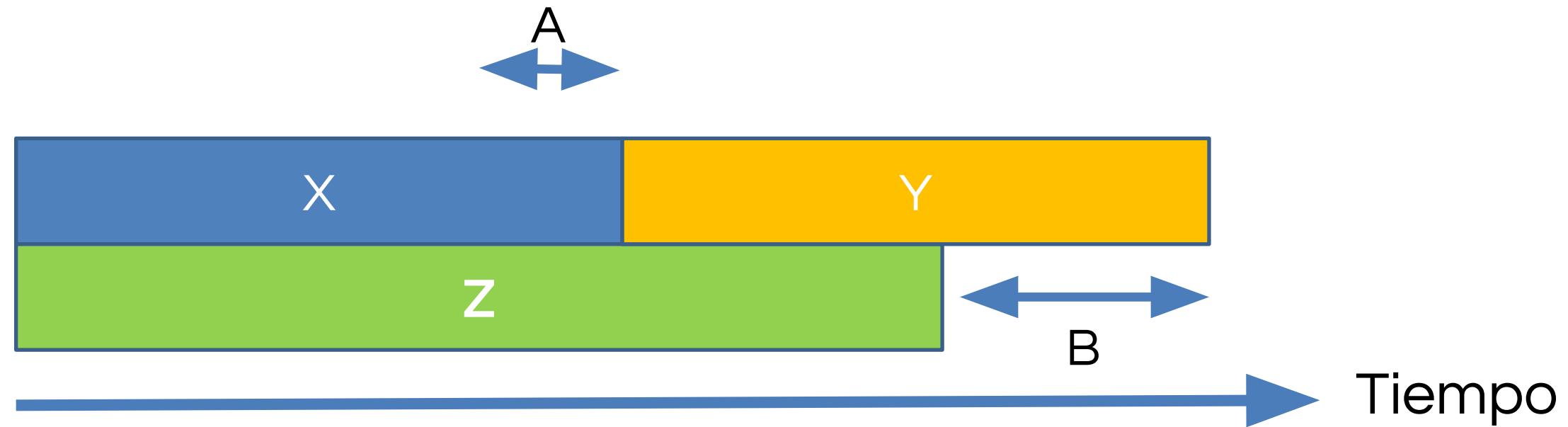




## Teorema de M.Mosca

A = Qué hacemos ahora?

B = Cuánto tiempo estamos al descubierto?



X = sustituir infraestructura

Y = necesidad de seguridad

Z = ordenador cuántico





## Iniciativas para definir criptografía “quantum safe”

NSA > nuevos programas e iniciativas

<https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm>

Europa > PQCrypto Project - WITDOM

ETSI > Nuevas iniciativas y workshops – Junio 2016

IETF > Preparando RFC sobre firmas basadas en funciones hash

ISO > Nueva iniciativa

NIST > report y nueva call para cifrados post-cuánticos





## Sistemas Clave Pública “quantum safe”

Funciones Hash > Sistemas de clave pública basados en firma – Merkle, 1979

Aleatorización > Códigos de Goppa binarios – McEliece, 1978

Lattices > NTRU – Hoffstein, Pipher, Silverman, 1998

Ecuaciones Cuadráticas Multivariadas > HFEv – Patarin, 1996





## ¿Por qué la matemática caótica es “quantum-safe”?

**Enigmedia ha desarrollado y patentado un sistema de criptografía basado en matemática caótica 20 veces más eficiente que los estándares actuales**

Sensitividad a las condiciones iniciales:

Una pequeña variación en las condiciones iniciales implica grandes cambios.

Impredicibilidad:

Es imposible de predecir el Sistema con precisión infinita.

Propagación del error:

Un pequeño error aumenta de forma exponencial.



# Preguntas

