

# Criptografía moderna para Aplicaciones Web

Protección de datos

# Prefacio

- ¿Quien es el presentador?
- ¿Para quién es este taller?
- Requisitos
- Organización
- ¿Que no cubriremos?



# Contacto

*Página web*

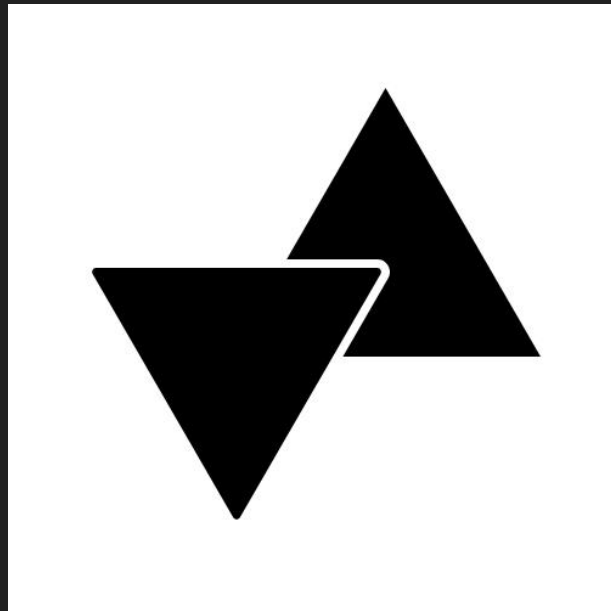
<https://www.liesware.com/>

*Twitter*

<https://twitter.com/liesware>

*Mail*

*liesware@liesware.com*



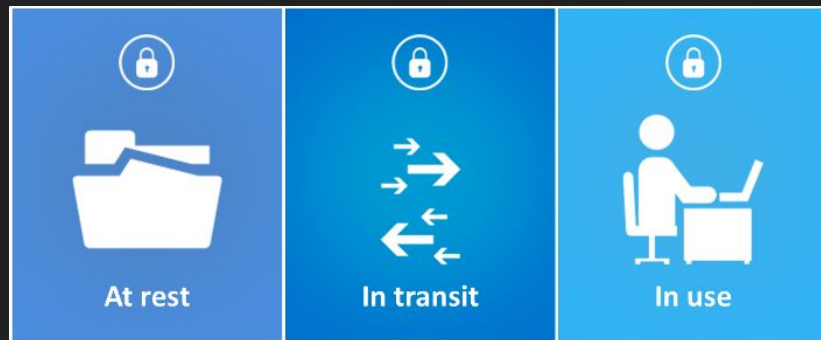
# Dia 1

- Fugas de información
- Datos en movimiento, en descanso y en uso
- Protección de datos
- Algoritmos criptográficos
- OpenSSL



# Día 2

- Técnicas de protección de datos en movimiento
- Técnicas de protección de datos en descanso
- Técnicas de protección de datos en uso



# Día 3

- Caso de estudio Telegram
- Implementación de propio protocolo criptográfico
- Sección de preguntas y respuestas
- Práctica



# Highlights

- Cinco de las seis principales empresas del mundo por valoración de mercado son empresas de datos.
- El impacto de la violación de datos
- Los datos son lo más valioso



# Las 100 empresas más grandes del mundo por valor de mercado en 2018.

- Apple
- Amazon.com
- Alphabet
- Microsoft
- Facebook
- Alibaba
- Berkshire Hathaway
- Tencent Holdings
- JPMorgan Chase
- ExxonMobil





# Impacto de una fuga de información



# Ashley Madison to Pay \$11.2 Million to Data Breach Victims



# Los datos son lo más valioso

- Basados en costos: el valor se determina en función del costo para producir los datos.
- Basados en el mercado: el valor se determina en función del precio de mercado de productos equivalentes o la disposición de los usuarios a pagar por los datos.
- Basados en los ingresos: el valor se define estimando los flujos de efectivo futuros que se pueden derivar de los datos.
- Monetización de beneficios: el valor se calcula definiendo los beneficios de productos de datos particulares, como un censo, y luego monetizando los beneficios.
- Basados en el impacto: el valor se determina evaluando el efecto causal de la disponibilidad de datos en los resultados económicos y sociales, o los costos en términos de ineficiencias o decisiones políticas deficientes debido a datos limitados o de mala calidad.

# Top 2018

## Aadhaar

- Cuentas de clientes afectadas: 1.1 mil millones (1 de cada 7 personas en el planeta!)
- Fecha de divulgación: 3 de enero de 2018.
- Aadhaar es un número de identidad único de 12 dígitos que pueden obtener los ciudadanos de la India



# TOP 2018

## Marriott Hotels

- Cuentas de clientes afectadas: 500 millones.
- Fecha de divulgación: 30 de noviembre de 2018.
- Marriott Hotels es una compañía que debido a una reciente adquisición ahora es propietaria de la cadena Starwood Hotels (Sheraton, St. Regis, Westin, W Hotels entre otros)



# TOP 2018

## Exactis

- Cuentas de clientes afectadas: 340 millones.
- Fecha de divulgación: 26 de junio de 2018.
- Exactis es un firma dedicada a la venta de datos



# TOP 2018

## Facebook

- Cuentas de clientes afectadas: un total de 257 millones en 3 incidentes separados.
- Cuentas de clientes afectadas: 87 millones.
- Fecha de divulgación: 17 de marzo de 2018.
- Cuentas de clientes afectadas: 120 millones.
- Fecha de divulgación: 27 de junio de 2018.
- Cuentas de clientes afectadas: 50 millones.
- Fecha de divulgación: 25 de septiembre de 2018.



# Top 2018

- Under Armour - 150 millones
- Quora - 100 millones
- MyHeritage - 92 millones
- Cathay Pacific - 9.4 millones
- SingHealth - 1.5 millones
- British Airways - 380 mil





# Resumen 2017 - 2018/2

Gemalto data breach report

# Aún más

- Collection #1
- <https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>
- <https://breachlevelindex.com/>

# Triada de la información

Enveil triad

# Datos en movimiento

- TLS
- TOR
- VPN
- Wireguard
- SSH



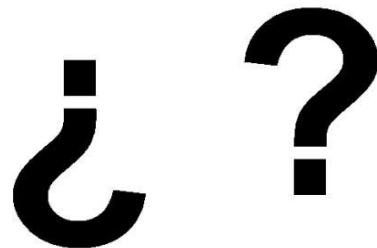
# Datos en descanso - Datos en uso

- Veracrypt
- Node.js - Javascript
- Coherence
- HSM
- Acra
- Enveil
- Vaultprotect
- SQLCipher



# ¿Por qué persiste?

1. Falta de conocimiento
2. Integración compleja
3. Falta de características



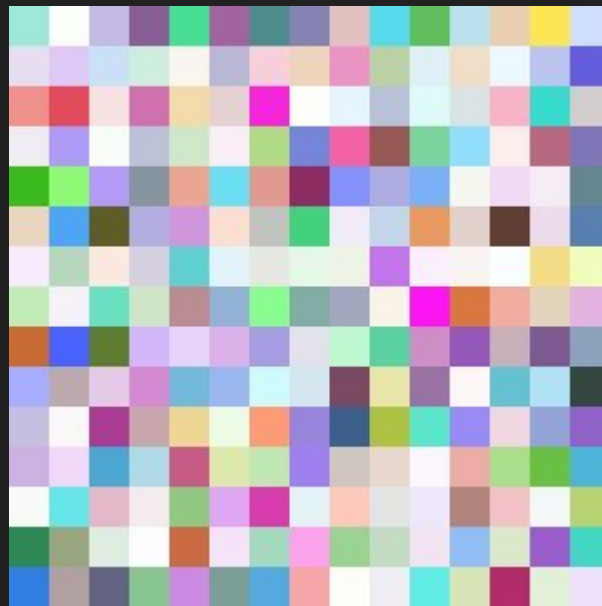
# Criptografía

- Confidencialidad
- Integridad
- Autenticidad
- Funciones hash
- Criptografía Simétrica
- Criptografía Asimétrica
- Números aleatorios


$$\begin{aligned} &^2(y f(x) + 20(x^2)y_1 + e_2(x)y_2 + e_3(x)y_3 \\ &(x+1)^2 = \left(\frac{x(x-2)}{2}\right)1 + (x(x-1))0 + \left(\frac{x(x-1)}{2}\right) \\ &= \left(\frac{(x-1)(x-2)}{2}\right)1 + (x(x-1))0 + \left(\frac{x(x-1)}{2}\right) \\ &f_P(x, y) \\ &)^2(y + 6x + 2)^4 - (y + 7x + 4)^4 + 8x)^2(y + 9x + 6)^4(x + 1) \\ &1)(x + 6)^4(x + 9)^4 - x(x + 8)^4(x + 2)^4 \\ &-9b + \sqrt{3}\sqrt[3]{4a^3 + 27b^2})^{1/3} 6x)^2(y + 10x + 8)^4x + 1 \\ &\frac{2^{1/3}3^{2/3}}{x(x+6)^2} \frac{(y+8x)^2}{(y+9x+} \\ &\frac{(1-i\sqrt{3})(-9b+\sqrt{3}\sqrt[3]{4a^3+27b^2})^{1/3}}{2^{1/3}3^{2/3}x+9} \frac{(y+8x+} \\ &\frac{(y+8x)^2(y+7x+4)^4(y+} \end{aligned}$$

# Números aleatorios

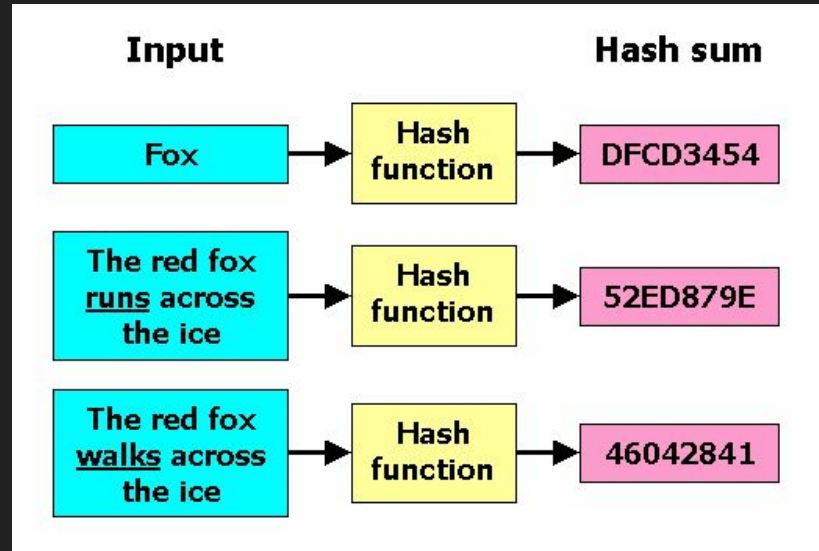
- Entropía
- Semillas
- RNGs (PRNGs, TRNGs)
- /dev/random
- /dev/urandom
- RDRAND





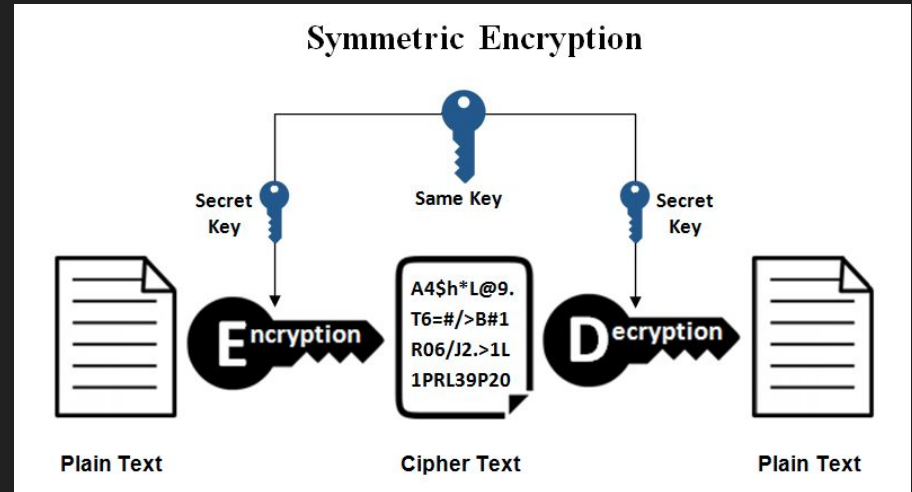
# Funciones hash

- One-way function
  - Huella digital
  - Integridad
- 
- SHA1, SHA2, SHA3
  - md5sum



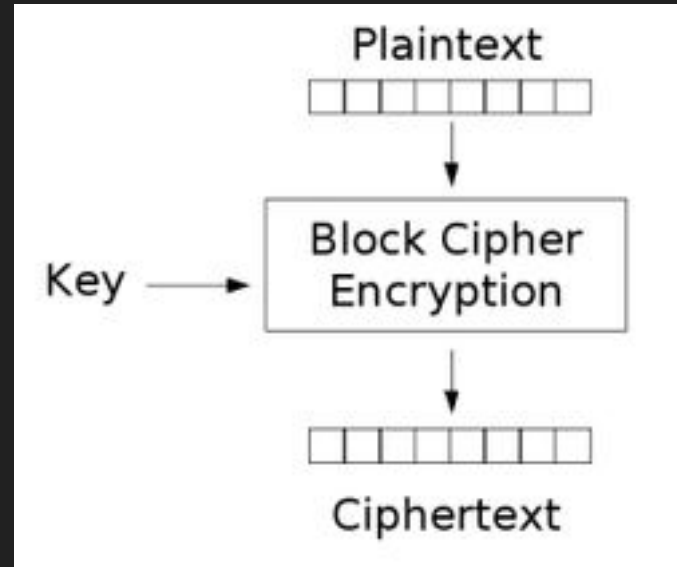
# Criptografía simétrica

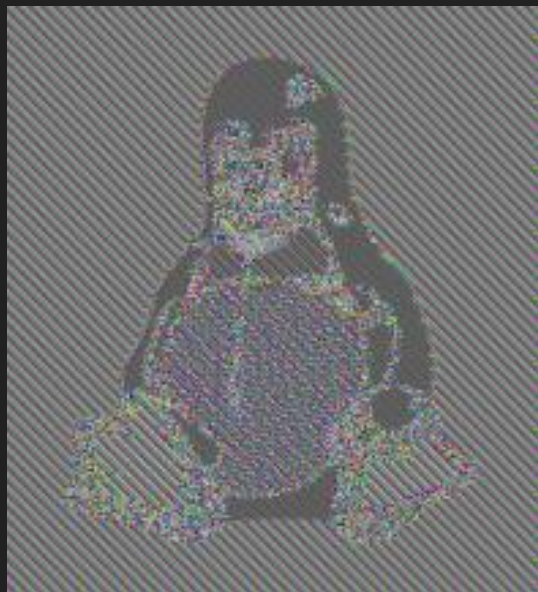
- Clave
- Vector de inicialización
- Algoritmo
- Compartir claves



# Algoritmos de bloque

- Bloque
  - Clave
  - Algoritmo
  - Texto
  - Modos de operación
- 
- DES
  - AES





# Algoritmos de flujo

- PRNG
- XOR
- Byte por byte

## XOR LOGIC

0 XOR 0 = 0 Same Bits  
1 XOR 1 = 0 Same Bits  
1 XOR 0 = 1 Different Bits  
0 XOR 1 = 1 Different Bits

XOR Symbol  
 $\oplus$

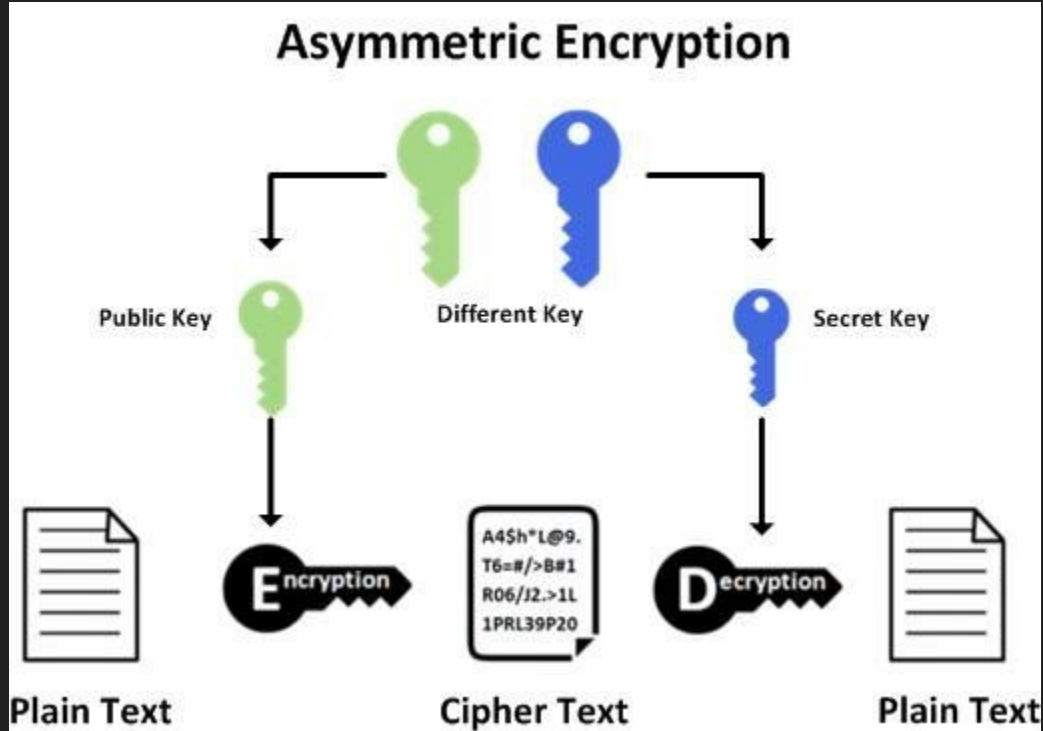
## ENCRYPT

$\oplus$   
0 0 1 1 0 1 0 1 Plaintext  
1 1 1 0 0 0 1 1 Secret Key  
= 1 1 0 1 0 1 1 0 Ciphertext

## DECRYPT

$\oplus$   
1 1 0 1 0 1 1 0 Ciphertext  
1 1 1 0 0 0 1 1 Secret Key  
= 0 0 1 1 0 1 0 1 Plaintext

# Criptografía asimétrica



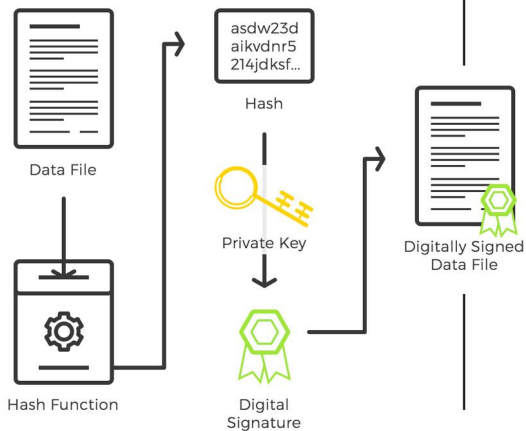
# Intercambio de claves

- Alice y Bob acuerdan usar el número primo  $p=23$  y la base  $g=5$ .
- Alice elige un número secreto  $a=6$ , luego envía a Bob  $(g^a \bmod p)$   
 $5^6 \bmod 23 = 8$ .
- Bob elige un número secreto  $b=15$ , luego envía a Alice  $(g^b \bmod p)$   
 $5^{15} \bmod 23 = 19$ .
- Alice calcula  $(g^b \bmod p)^a \bmod p$   
 $19^6 \bmod 23 = 2$ .
- Bob calcula  $(g^a \bmod p)^b \bmod p$   
 $8^{15} \bmod 23 = 2$ .

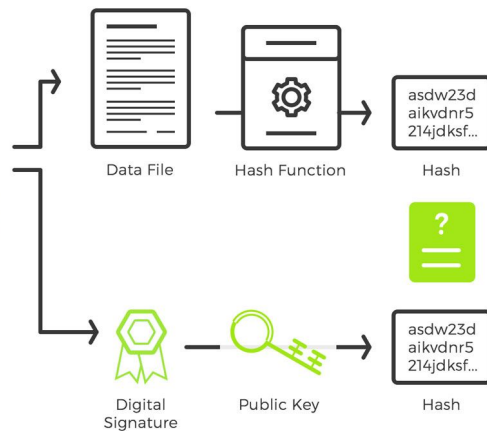
# Firma digital

## Common Public Key Digital Signature

### Signing



### Verification





# Algoritmos

- DH (intercambio de claves)
- RSA (cifrado, firmas digitales)
- DSA (firmas digitales)

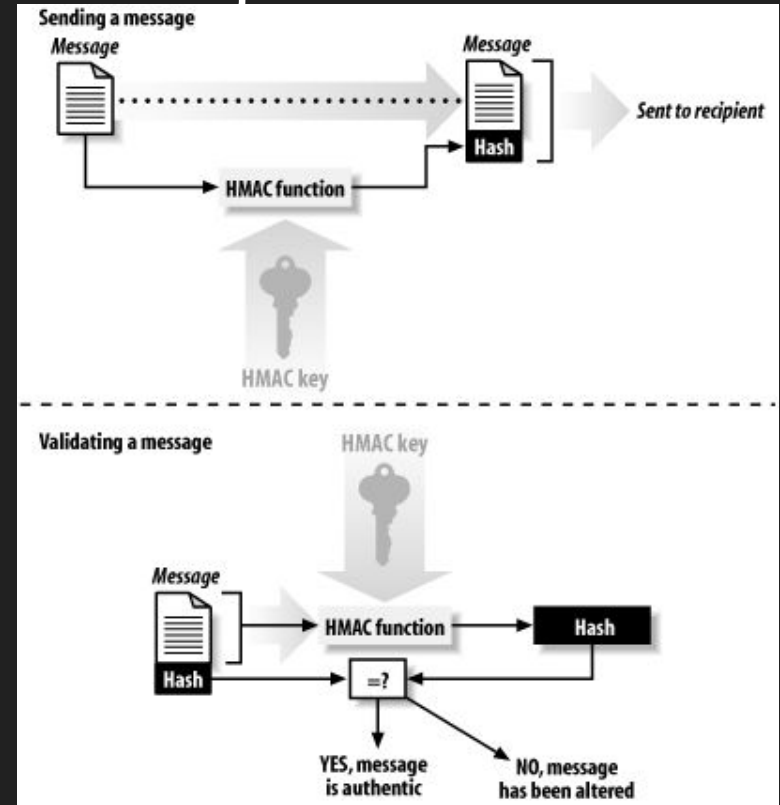
## EC

- ECDH (intercambio de claves)
- ECIES (cifrado)
- ECDSA (firmas digitales)



# Códigos de autenticación de mensaje

- Integridad
- Autenticidad



# Seguridad

## Comparable Key Sizes for Equivalent Security

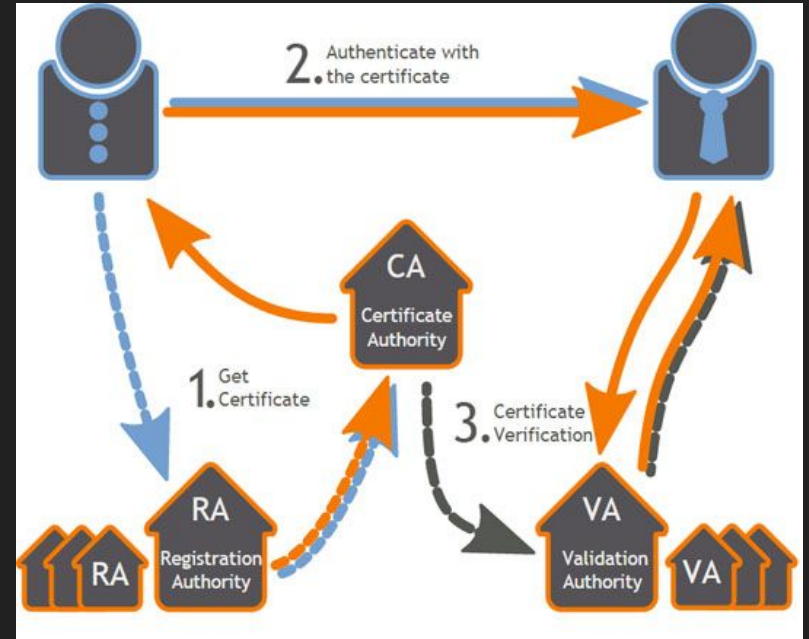
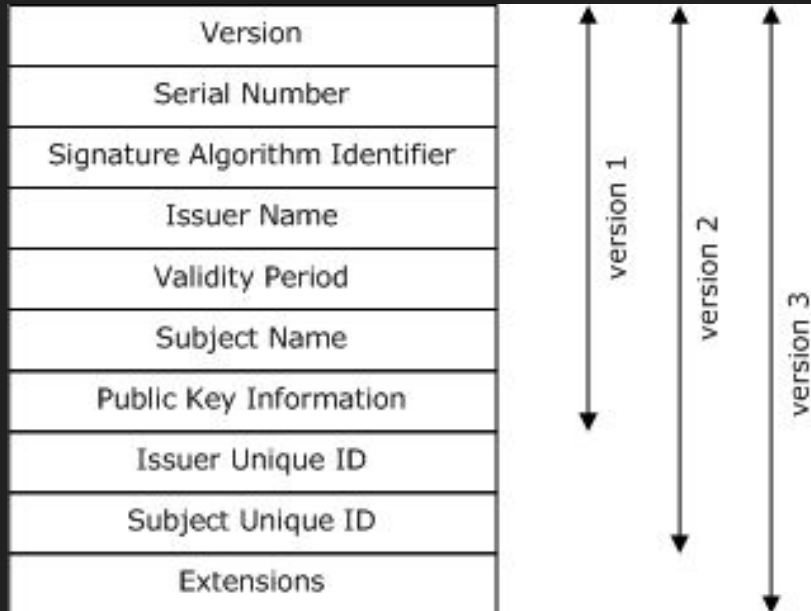
<b>Symmetric scheme (key size in bits)</b>	<b>ECC-based scheme (size of <math>n</math> in bits)</b>	<b>RSA/DSA (modulus size in bits)</b>
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

# OpenSSL

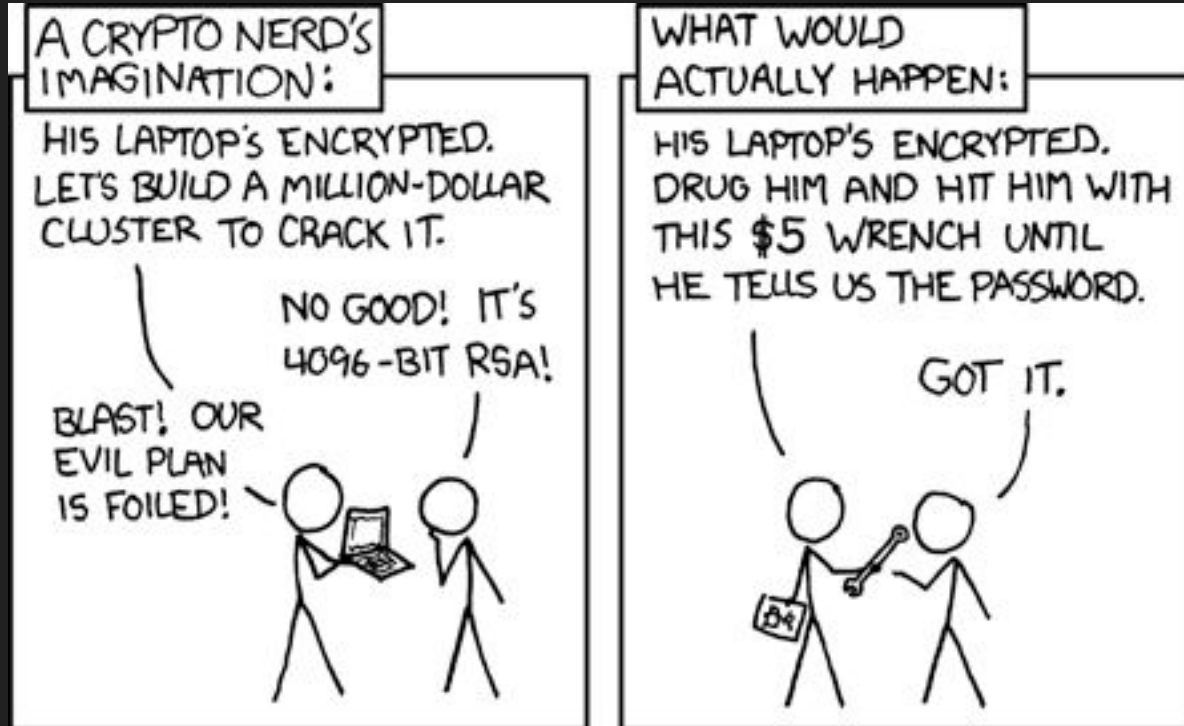
- TLS/SSL
- Librería
- Programa Bash
- FIPS 140-2



# X.509

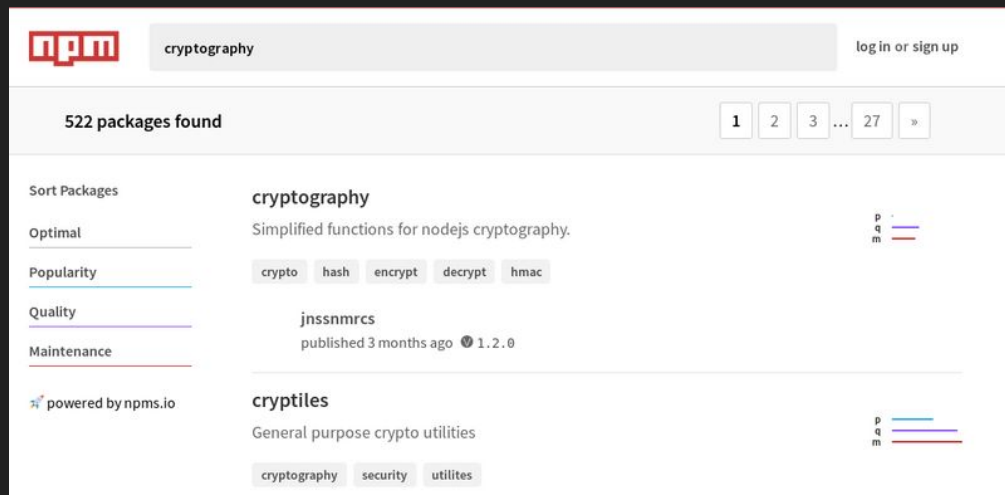


# Aclaración



# Criptografía en L7 - libs

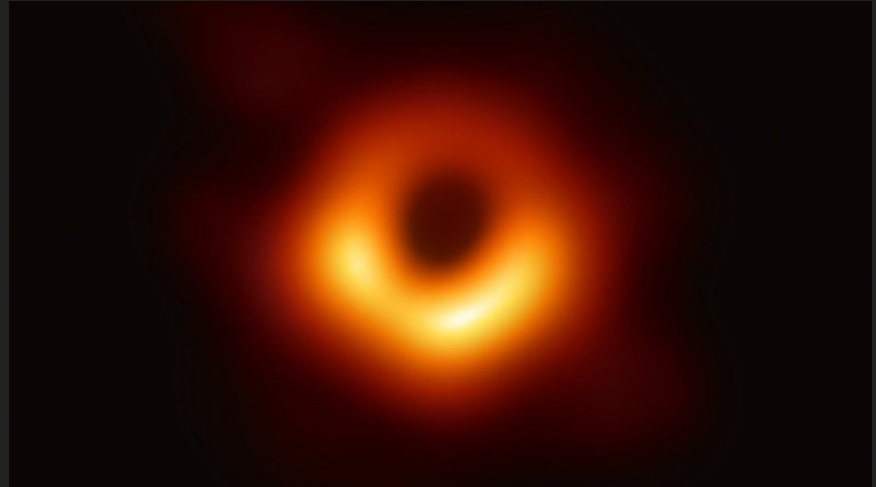
- ¿Cual?
- Características
- Documentación
- Dependencias



The screenshot shows the NPM search results for the term 'cryptography'. At the top, the NPM logo is on the left, the search term 'cryptography' is in the center, and a 'log in or sign up' link is on the right. Below the search bar, it states '522 packages found' and shows pagination controls with numbers 1, 2, 3, ..., 27, and a '»' button. On the left side, there is a 'Sort Packages' section with five options: 'Optimal' (selected), 'Popularity', 'Quality', and 'Maintenance'. Below this is a 'powered by npms.io' logo. The main content area displays two packages. The first package is 'cryptography' by 'jnsnmrcs', described as 'Simplified functions for nodejs cryptography.' It has tags for 'crypto', 'hash', 'encrypt', 'decrypt', and 'hmac'. It was published 3 months ago and has version 1.2.0. To its right is a small bar chart showing popularity trends for packages 'p', 'q', and 'm'. The second package is 'cryptiles' by 'jnsnmrcs', described as 'General purpose crypto utilities'. It has tags for 'cryptography', 'security', and 'utilites'. To its right is another small bar chart showing popularity trends for packages 'p', 'q', and 'm'.

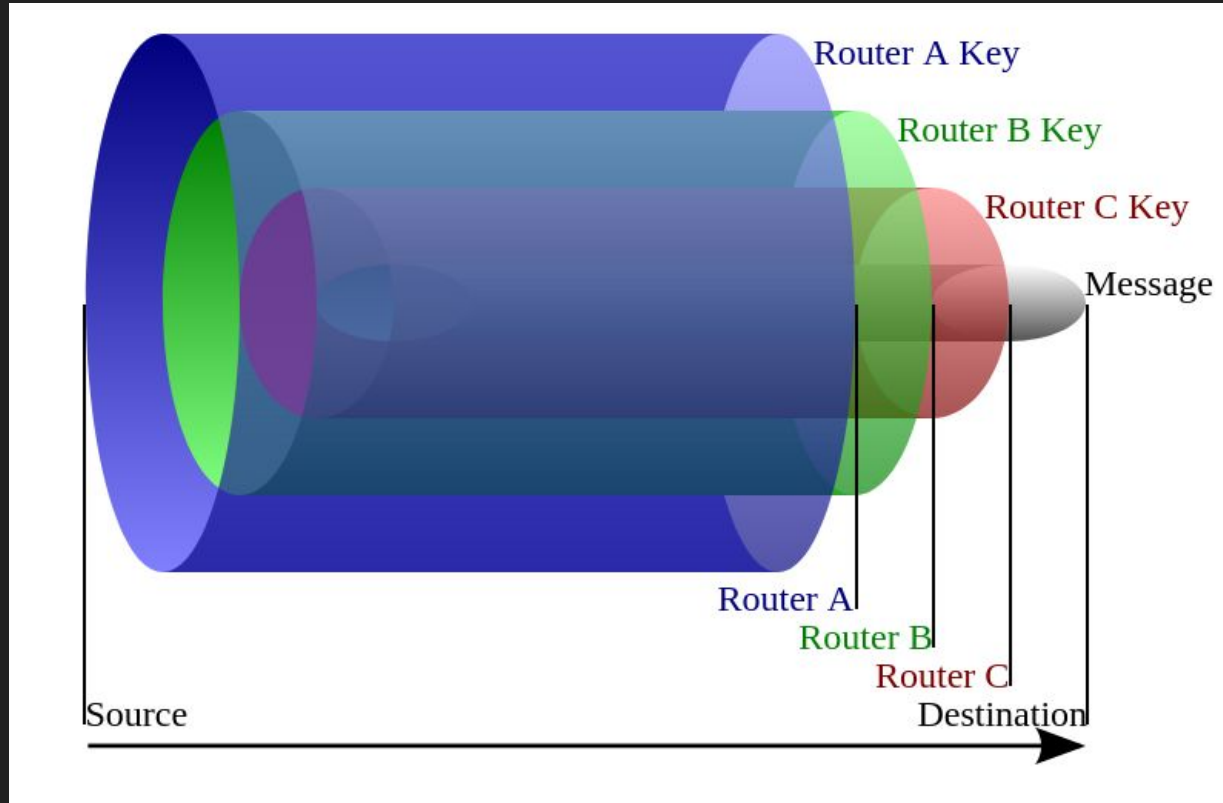
# Criptografía en L7 - PCKS#11

- HSM (precio)
- ¿SoftHSM?





# Onion protocol

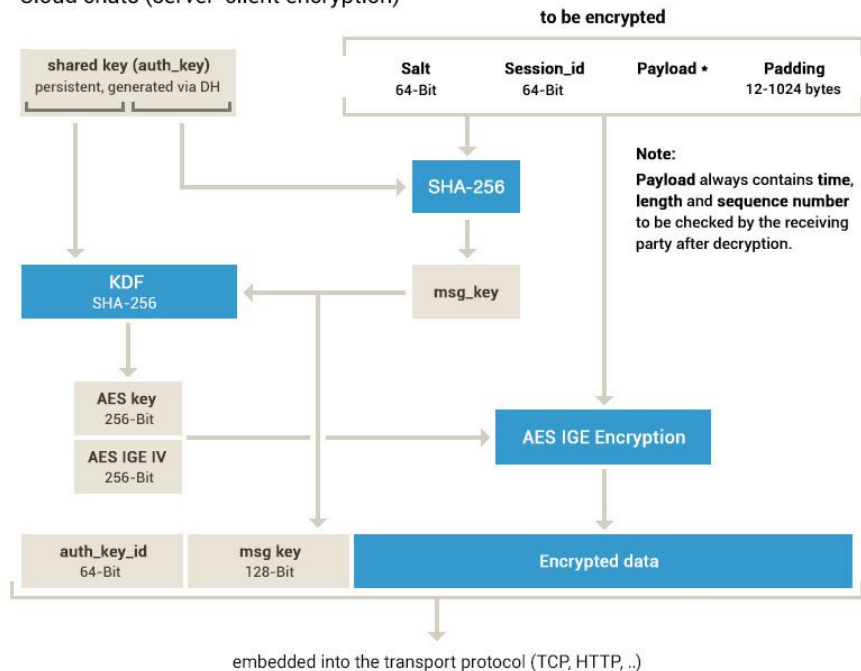


# MTPROTO

- HTTP, HTTPS, TCP, UDP

## MTPROTO 2.0, part I

Cloud chats (server-client encryption)



**Important:** After decryption, the receiver must check that  
 $\text{msg\_key} = \text{SHA-256}(\text{fragment of auth\_key} + \text{decrypted data})$

# Coherence

Coherence proporciona una interfaz para los algoritmos criptográficos modernos que se inspira en las API web, pero sin ser HTTP, se implementa como un servidor TCP sin bloqueo con una interfaz JSON para poder ser utilizada por cualquier idioma, es decir, Coherence minimiza el tiempo desarrollo y complejidad del código para aplicaciones criptográficas. Algunos de los algoritmos ofrecidos por Coherence son candidatos AES y AES, Sosemanuk, familia SHA \*, HMAC, DH, RSA, DSA, ECC, NTRU.

# Características - 1

- Hash functions: SHA3, SHA2, SHA1, WHIRLPOOL, Blake2b, SipHash.
- Password-hashing function: Argon2
- Stream ciphers: Sosemanuk, Salsa20/20.
- Block ciphers: AES, RC6, MARS, Twofish, Serpent, CAST-256, Camellia, SPECK, SIMECK .
- Block ciphers modes: CTR, GCM.
- Message authentication codes: HMAC(SHA3, SHA2, SHA1, WHIRLPOOL), CMAC(AES, RC6, MARS, Twofish, Serpent, CAST-256, Camellia), VMAC(AES, RC6, MARS, Twofish, Serpent, CAST-256, Camellia), Poly1305.

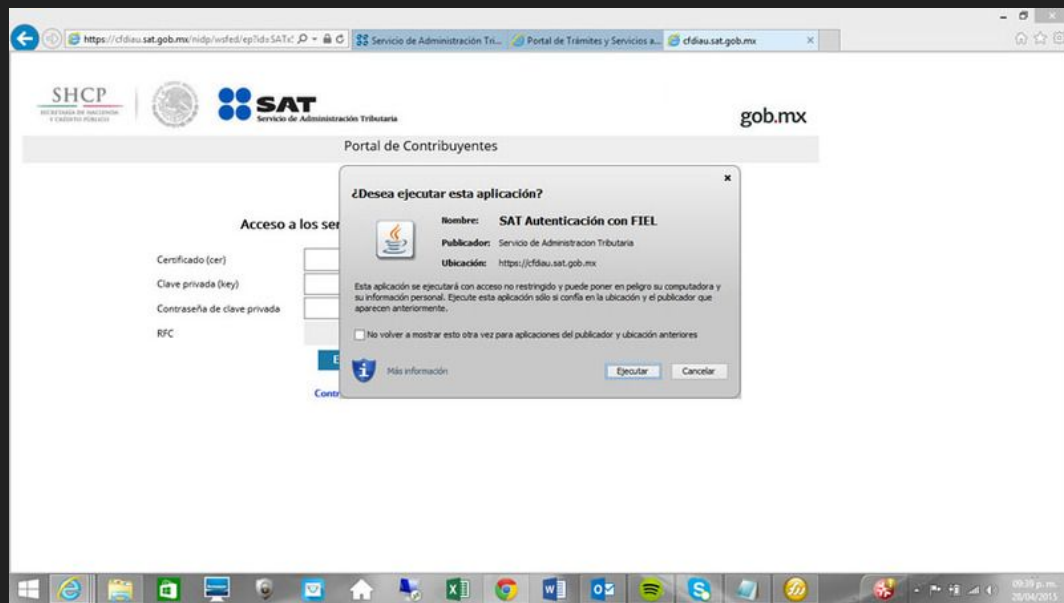
# Características - 2

- RSA: Key generation, digital signature, encryption.
- DSA: Key generation, digital signature.
- DH: Key generation, key exchange (rfc and custom parameters).
- ECC: Key generation, ECIES, ECDSA, ECDH, Curve25519, ECNR.
- Rand numbers: Randpool, AutoSeededRandomPool, Rdrand.
- Post-Quantum Cryptography: NTRU, Qtesla.
- Json-log format output, so elasticsearch ready

# Casos de uso - offload

- Internet explorer
- JAVA
- Miedo de instalar Java

Y después de 6 meses deja de funcionar



# Casos de uso - autenticación

- GPU
- PHC
- Fugas de datos

id	username	password	passwordHint
1	admin	7E7274BAC45E467C5AB832170F12E418	k3wl dud
2	pumpkin22	5377DBF76D995CC213ED76924A31CB13	my favorite holiday
3	johndoe	512239D9AE0C3B5567DE188739F689F2	Freddie Mercury's band
4	alexa45	2FE5421E49061F8225C2FB7CB81980FD	password
5	guy	ABE35E2827DDA834C9612FE9E9C92CE0	NULL
6	maryjane	198670893B2781C83F3DA5D45150123D	I'm one!
7	dudson123	59E2113217E65B9885F9DA73FDC5697B	scary movie!