Organiza:

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Partners Estratégicos:

GOVERTIS Advisory Services

Telefónica

"Taller práctico
El cifrado en la protección de datos: cuándo y para qué"

Carlos Bachmaier Johanning

https://es.linkedin.com/in/carlosbachmaier
ABaPllc.aec+ClubDPD@gmail.com
https://t.me/PersonalisNotitiaSemperParatus


WE HAD A MASSIVE DATA BREACH. HACKERS GOT INTO THE PRIVATE DATA OF ALL OF OUR CUSTOMERS.
DILBERT.COM @SCOTTADAMSSAYS
NO PROBLEM. WE'LL ISSUE A PRESS RELEASE THAT SAYS WE'RE SORRY AND IT WILL NEVER HAPPEN AGAIN.
5-7-18 ©2018 Scott Adams, Inc./Dist. by Andrews McMeel
THAT'S WHAT WE SAID THE LAST THREE TIMES IT HAPPENED.
OUR STRATEGY IS TO WEAR THEM DOWN.

Trama

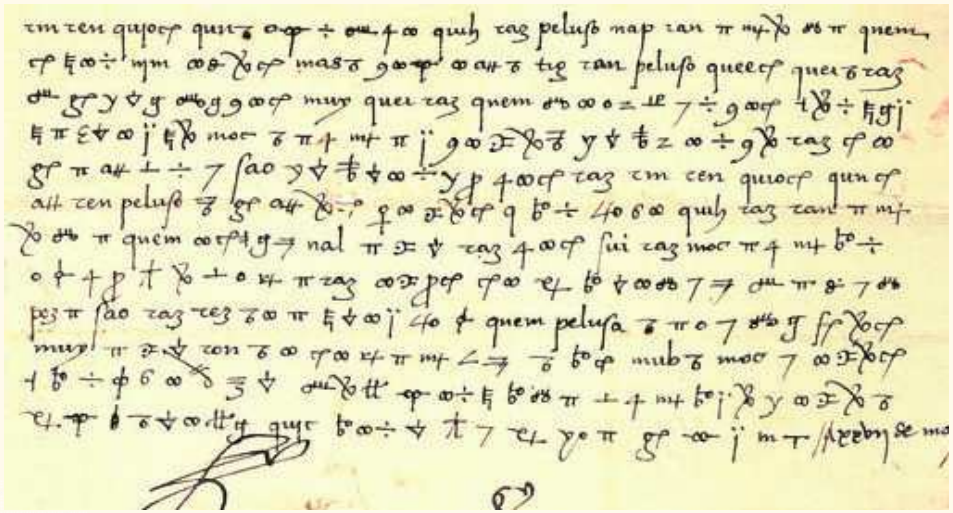
Toma de contacto y relevancia

(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

¿Qué es cifrar?

¿Qué se persigue al cifrar?

Conozca en el vídeo por qué el Rey Católico enviaba las cartas cifradas al Gran Capitán



Text to Encrypt

En un lugar de la Mancha, de cuyo nombre no quiero acordarme, no ha mucho tiempo que vivía un hidalgo de los de lanza en astillero, adarga antigua, rocín flaco y galgo corredor. Una olla de algo más vaca que carnero, salpicón las más noches, duelos y quebrantos los sábados, lantejas los viernes, algún palomino de añadidura los domingos, consumían las tres partes de su hacienda.

Encrypt

Encrypted Text

```
7j/O7SooEhJ6+5KyPXmL0esEYhVDrHoEmoPaQhtChayM6lUucDuXkEucQEzJvodrBnwLVbi
IvlJFgJAo++wyHzfQF0gLfH4y1rtEuLj8i9aUTGRjfe25lBb0A0N
/k0iZw9liLRgrxjMCf4w3xMz9ay+bn6ONBzQU/JPCx7kdc/iYISDbby8sMPzLmN2QquCK
/I+/iABQHAZe
/YeeVnuAniJVU1Ks38DpvYKWBSzZPVCbPHd8Rp2N7CIJr0SGYVTxp+tNg3O1lmoksRhg1iW
mHn56osdMYaE5uLKB2Gn
/ydnh948N5X9nDhFApjGEXLogQynXvfxuouhaLchavK9ePSafBLbpsLvOg+RU1INj+3IUor
qYu9gM2lsLv3LFqYtwzrkaDTdwfIApxP27tktOdWF+hpMMOOMEtFw0yOb7vSvyWw6HtjW7r
1lsxz2kmi8b8HIY5IbFAFN8hroXh57D3yOdT++qaV2rC+FjtrJcP3vI1lmZE2ChHbMhEvo2
xILUm9UiN/Cf8utJlUwxYiLU9HY6JnIMWXUTt0aa5VNotlg=
```

¿Qué es cifrar?

- RAE:

  Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger

- CNSS [CNSS-4009:2006] (CCN)

  Convert plain text to cipher text by means of a cryptographic system.

  Un tratamiento sobre información (**texto en claro**) que la transforma en algo ininteligible (**texto cifrado/criptograma**) por medio de un medio de cifrado (**sistema criptográfico) (algoritmo/método+clave)**

¿Qué se persigue al cifrar?

Preservar la confidencialidad / secreto de la información

Confidencial

- RAE

  Que se hace o se dice en la confianza de que se mantendrá la **reserva** de lo hecho o lo dicho. (*prevención o cautela para no **descubrir** algo que se sabe o piensa*) (*manifestar, hacer patente*)

Secreto

- RAE:

  Cosa que cuidadosamente se tiene reservada y oculta.

  Reserva, sigilo. (*revelar: descubrir o manifestar lo ignorado o secreto)*

  …

  Pieza aplanada del cerdo posterior a la paleta.

Confidencialidad

- Magerit:

  Que la información llegue solamente **a las personas autorizadas**. Contra la confidencialidad o secreto nos encontraremos con *fugas y filtraciones* de información, así como con accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación

- ISO 27mil

  Propiedad por la que la información no se pone a disposición o se divulga a ***personas, entidades o procesos*** no autorizados

(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

Seguridad de los datos personales

Artículo 32

Seguridad del tratamiento

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

Artículo 33

Notificación de una violación de la seguridad de los datos personales a la autoridad de control

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

TÍTULO X

Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio

[Bloque 289: #ci-8]

CAPÍTULO I

Del descubrimiento y revelación de secretos

[Bloque 290: #a197]

Artículo 197.

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

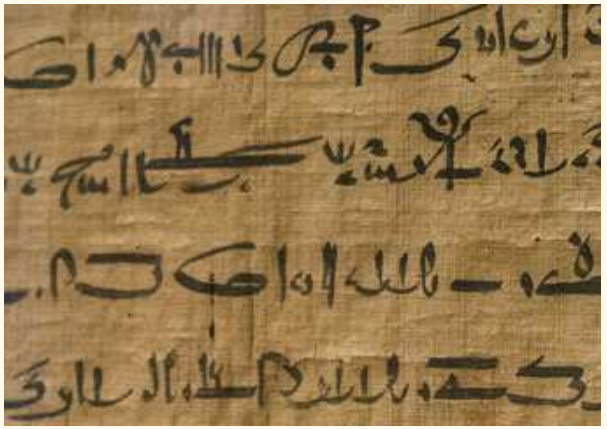
2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

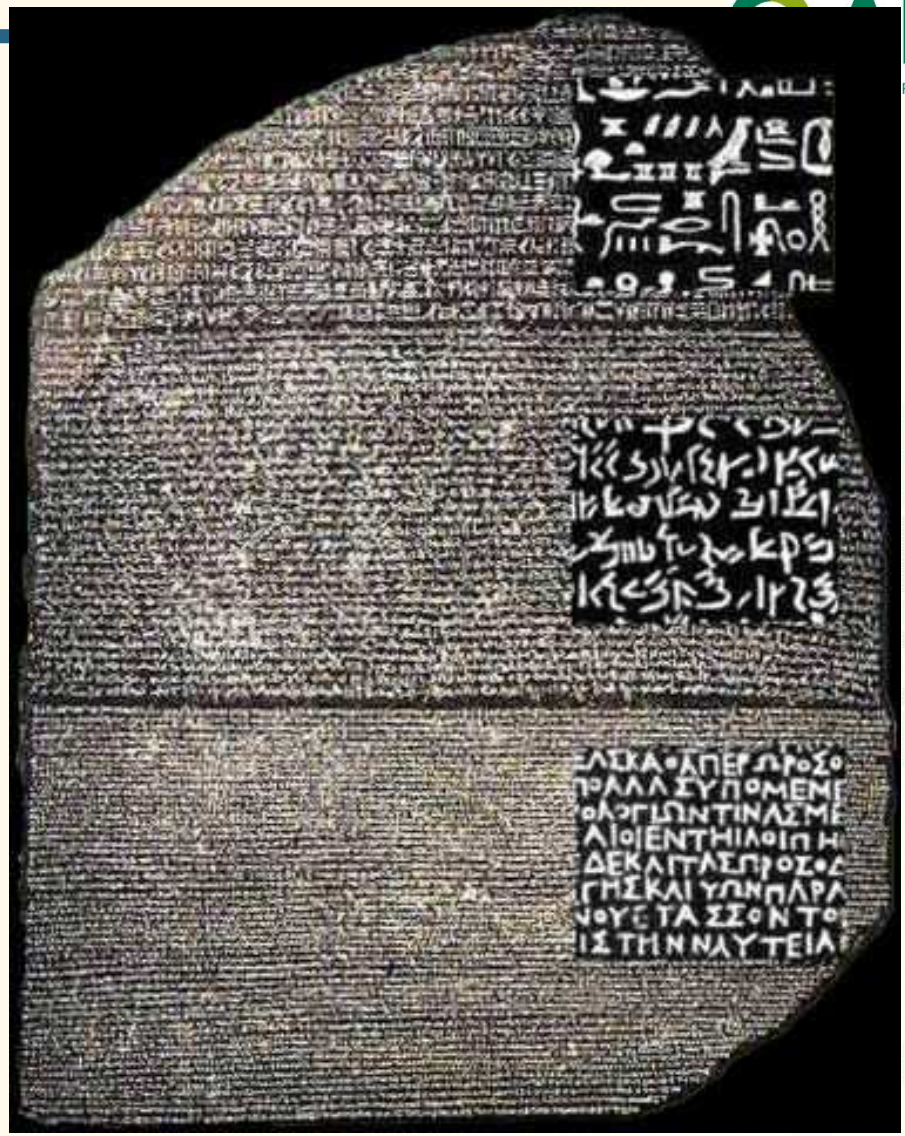
Qué es cifrar y qué no es…
(cómo se hace)

(comprensión básica)

¿Es un texto cifrado?



¿Es un texto cifrado?



¿Es un mensaje cifrado?

¿Es un mensaje cifrado?

Locutor de claves

Locutor de claves es el término empleado para referirse a personas que se comunican utilizando lenguajes codificados. Generalmente es usado para nombrar a nativos americanos que sirvieron en el Cuerpo de Marines de los Estados Unidos y cuya principal ocupación era la de transmitir mensajes militares secretos.

Estos mensajes eran transmitidos, generalmente, por teléfono o radio, usando códigos construidos sobre sus propios lenguajes, conocidos por pequeños grupos, en ocasiones decenas de personas en todo el mundo, lo que suponía una gran ventaja estratégica. Dicha ventaja reside

Locutores de claves navajos, Saipán, junio de 1944

En la Segunda Guerra Mundial se usaron códigos en idioma navajo para identificar mensajes militares. Por ejemplo «chai-da-gahy-nail-tsaidi» (literalmente "asesino de tortugas") quería decir «armas antitanque».


Covadonga 722 A.C.

¿Es un mensaje cifrado?

Mayday Mayday

…

Roger

¿Es un mensaje cifrado?

Ad nutum

…

Habeas corpus

…

Logaritmo

Código/Lenguaje

Código (criptografía)

Un código, en criptografía, consiste en sustituir unidades textuales con importancia semántica, habitualmente palabras o frases, para ocultar el mensaje. Por ejemplo, «cielo azul» podría significar «atacar al amanecer». Cuando se usan códigos, la documentación secreta que relaciona cada código con la información que representa se recopila en un diccionario o **libro de códigos**.

En la actualidad no se suelen usar salvo para denominar operaciones encubiertas. Por ejemplo: Operación Tormenta del desierto para denominar a la operación de inicio del ataque a Irak en 1991.

Códigos vs Cifrado

Confusión con cifrado [editar]

En el lenguaje cotidiano, y de forma incorrecta, es habitual el uso de la palabra *cifra* para incluir tanto a **códigos** como a procesos de cifrado.[6] Tanto los códigos como los cifrados son métodos para alterar las representaciones de los mensajes para hacerlos ininteligibles a intrusos y así mantener la confidencialidad. Esencialmente un código es una sustitución de palabras o frases por otros. Sin embargo un cifrado consiste en una transformación carácter por carácter o bit por bit, según el caso, sin importar la estructura lingüística ni el significado del mensaje.[1] Sin embargo, el concepto de código y sistemas de cifra se pueden aplicar de forma conjunta. Ese puede ser el origen del uso inadecuado de la palabra *cifra*. Por ejemplo:

- Un sistema de cifra puede ser usado para cifrar los símbolos de un código.
- Se pueden usar códigos para algunas partes del mensaje, y el resto, para las que no existen códigos asociados, se pueden cifrar. A esta forma de operar se le llama **nomenclátor** (véase en Sustitución homófona).

Si llevamos las consideraciones al límite, un código puede ser considerado como un sistema de cifra con un alfabeto muy grande.

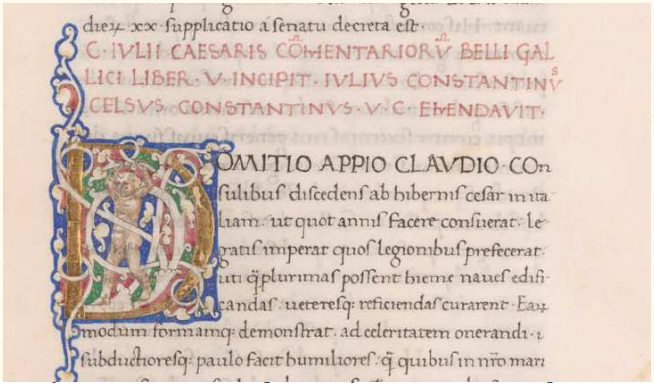
Ocultación

Esteganografía

La **esteganografía** (del griego στεγανος *steganos*, "cubierto" u "oculto", y γραφος *graphos*, "escritura") trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados *portadores*, para ser enviados y de modo que no se perciba el hecho. Es decir, procura ocultar mensajes dentro de otros objetos y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase *inadvertido* para observadores que tienen acceso a ese canal.

Con esteganografía y criptografía, en ambas, se intenta ocultar un mensaje para ser enviado, pero ellas son fundamentalmente diferentes, ya que la criptografía solo cifra los mensajes, manteniéndolos visibles pero indistinguibles de basura, aparecen como una secuencia de bit aleatorios; para ver su contenido original es necesario conocer una clave. En la esteganografía, el archivo u objeto que contiene el mensaje oculto se observará idéntico al original, y para conocer su mensaje contenido será necesario conocer la clave y el algoritmo (software) con el que se ocultó.

Historia

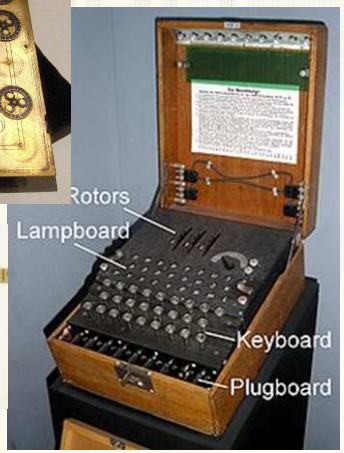


adoptó y que Suetonio en De Vita Caesarum describe como sigue:

"*... si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet*"

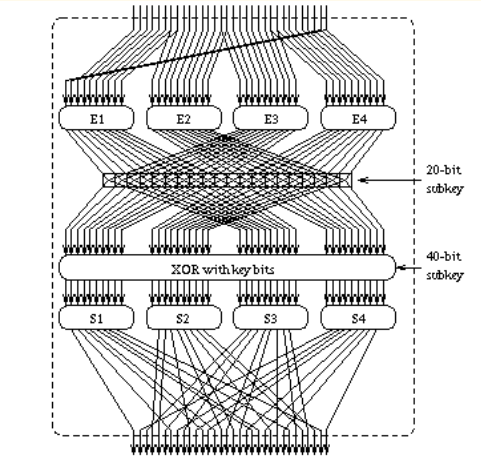
Julio César sustituìa cada letra de su mensaje con la letra que se encontró tres posiciones más adelante en el alfabeto; por lo que cada una A se convirtía en D, cada B se hacía ed E, y así sucesivamente; las tres últimas letras del alfabeto fueron reemplazados por las tres primeras.
Por ejemplo, usando el **cifrado César**:

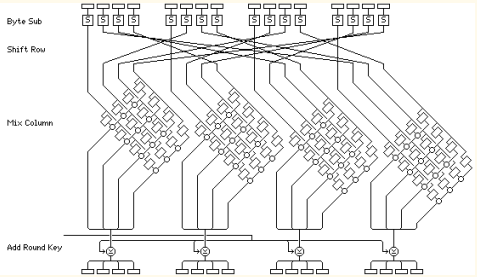
"*Omnia Gallia est divisa in partes tres*"
RPQND LDOOND HVZ GNBNVD NQ SDUZHV ZUHV

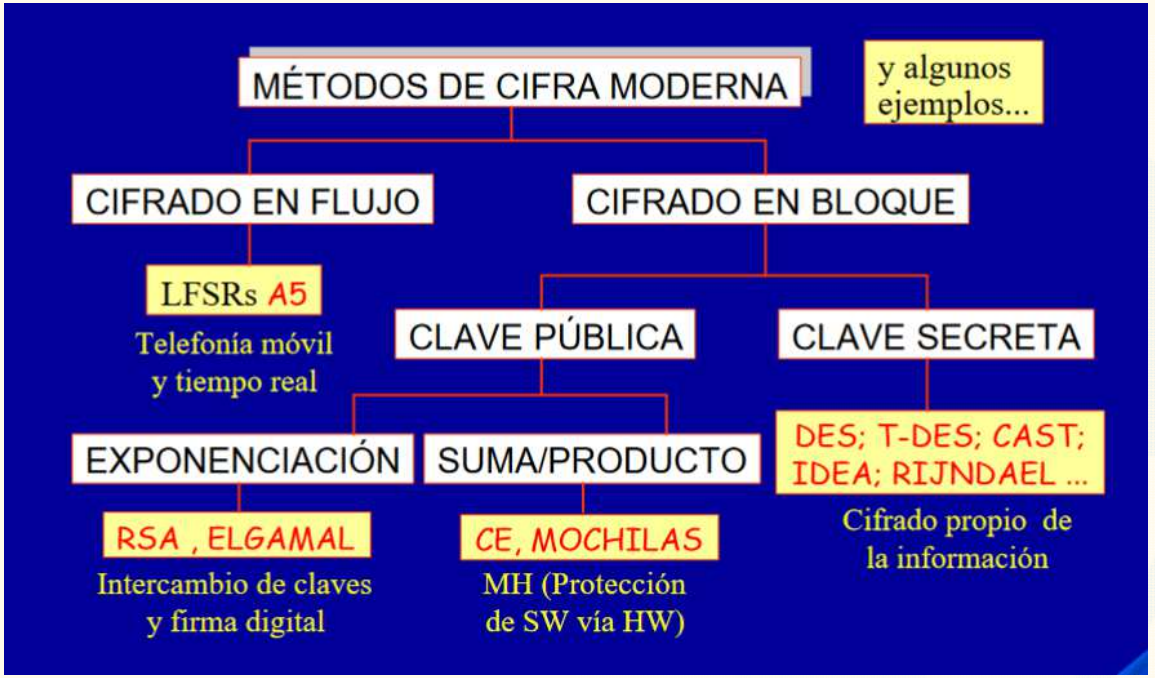


Permutación y Sustitución

Historia


E1
E2
E3
E4
20-bit subkey
XOR with key bits
40-bit subkey
S1
S2
S3
S4


Byte Sub
Shift Row
Mix Column
Add Round Key


MÉTODOS DE CIFRA MODERNA
y algunos ejemplos...
CIFRADO EN FLUJO
CIFRADO EN BLOQUE
LFSRs A5
Telefonía móvil y tiempo real
CLAVE PÚBLICA
CLAVE SECRETA
EXPONENCIACIÓN
SUMA/PRODUCTO
DES; T-DES; CAST; IDEA; RIJNDAEL ...
Cifrado propio de la información
RSA , ELGAMAL
Intercambio de claves y firma digital
CE, MOCHILAS
MH (Protección de SW vía HW)

Algoritmos modernos

Clave secreta /Simétricos

clave única/compartida, 1 clave

AES Blowfish DES (internal mechanics, Triple DES) Serpent Twofish

Clave Pública / Asimétricos

claves pública/privada (secreta)

Diffie–Hellman – DSS – ElGamal - **RSA**

[**S/MIME** – **PGP** - **TLP-SSL** (web) – SSH]

(usan internamente simétricos)

Block ciphers (security summary)	
Common algorithms	AES · Blowfish · DES (internal mechanics, Triple DES) · Serpent · Twofish
Less common algorithms	Camellia · CAST-128 · GOST · IDEA · RC2 · RC5 · RC6 · SEED · ARIA · Skipjack · TEA · XTEA
Other algorithms	3-Way · Akelarre · Anubis · BaseKing · BassOmatic · BATON · BEAR and LION · CAST-256 · Chiasmus · CIKS-1 · CIPHERUNICORN-A · CIPHERUNICORN-E · CLEFIA · CMEA · Cobra · COCONUT98 · Crab · Cryptomeria/C2 · CRYPTON · CS-Cipher · DEAL · DES-X · DFC · E2 · FEAL · FEA-M · FROG · G-DES · Grand Cru · Hasty Pudding cipher · Hierocrypt · ICE · IDEA NXT · Intel Cascade Cipher · Iraqi · Kalyna · KASUMI · KeeLoq · KHAZAD · Khufu and Khafre · KN-Cipher · Kuznyechik · Ladder-DES · Libelle · LOKI (97, 89/91) · Lucifer · M6 · M8 · MacGuffin · Madryga · MAGENTA · MARS · Mercy · MESH · MISTY1 · MMB · MULTI2 · MultiSwap · New Data Seal · NewDES · Nimbus · NOEKEON · NUSH · PRESENT · Prince · Q · RC6 · REDOC · Red Pike · S-1 · SAFER · SAVILLE · SC2000 · SHACAL · SHARK · Simon · SM4 · Speck · Spectr-H64 · Square · SXAL/MBAL · Threefish · Treyfer · UES · xmx · XXTEA · Zodiac
Design	Feistel network · Key schedule · Lai–Massey scheme · Product cipher · S-box · P-box · SPN · Confusion and diffusion · Avalanche effect · Block size · Key size · Key whitening (Whitening transformation)
Attack (cryptanalysis)	Brute-force (EFF DES cracker) · MITM (Biclique attack · 3-subset MITM attack) · Linear (Piling-up lemma) · Differential (Impossible · Truncated · Higher-order) · Differential-linear · Distinguishing (Known-key) · Integral/Square · Boomerang · Mod *n* · Related-key · Slide · Rotational · Side-channel (Timing · Power-monitoring · Electromagnetic · Acoustic · Differential-fault) · XSL · Interpolation · Partitioning · Rubber-hose · Black-bag · Davies · Rebound · Weak key · Tau · Chi-square · Time/memory/data tradeoff
Standardization	AES process · CRYPTREC · NESSIE
Utilization	Initialization vector · Mode of operation · Padding
Stream ciphers	
Widely used ciphers	RC4 · block ciphers in stream mode · ChaCha
eSTREAM Portfolio	Software: HC-256 · Rabbit · Salsa20 · SOSEMANUK Hardware: Grain · MICKEY · Trivium
Other ciphers	A5/1 · A5/2 · Achterbahn · E0 · F-FCSR · FISH · ISAAC · MUGI · ORYX · Panama · Phelix · Pike · Py · QUAD · Scream · SEAL · SNOW · SOBER · SOBER-128 · VEST · VMPC · WAKE
Theory	shift register · LFSR · NLFSR · shrinking generator · T-function · IV
Attacks	correlation attack · correlation immunity · stream cipher attacks
Cryptography	[show]

Public-key cryptography		
Algorithms	Integer factorization	Benaloh · Blum–Goldwasser · Cayley–Purser · Damgård–Jurik · GMR · Goldwasser–Micali · Naccache–Stern · Paillier · Rabin · RSA · Okamoto–Uchiyama · Schmidt–Samoa
	Discrete logarithm	BLS · Cramer–Shoup · DH · DSA · ECDH · ECDSA · EdDSA · EKE · ElGamal (signature scheme) · MQV · Schnorr · SPEKE · SRP · STS
	Lattice/SVP/CVP/LWE/SIS	NTRUEncrypt · NTRUSign · RLWE-KEX · RLWE-SIG · BLISS · NewHope
	Others	AE · CEILIDH · EPOC · HFE · IES · Lamport · McEliece · Merkle–Hellman · Naccache–Stern knapsack cryptosystem · Three-pass protocol · XTR
Theory	Discrete logarithm · Elliptic-curve cryptography · Non-commutative cryptography · RSA problem · Trapdoor function	
Standardization	CRYPTREC · IEEE P1363 · NESSIE · NSA Suite B · Post-Quantum Cryptography Standardization	
Topics	Digital signature · OAEP · Fingerprint · PKI · Web of trust · Key size · Post-quantum cryptography	

Nudo

¿Cómo se cifra (modernamente)?

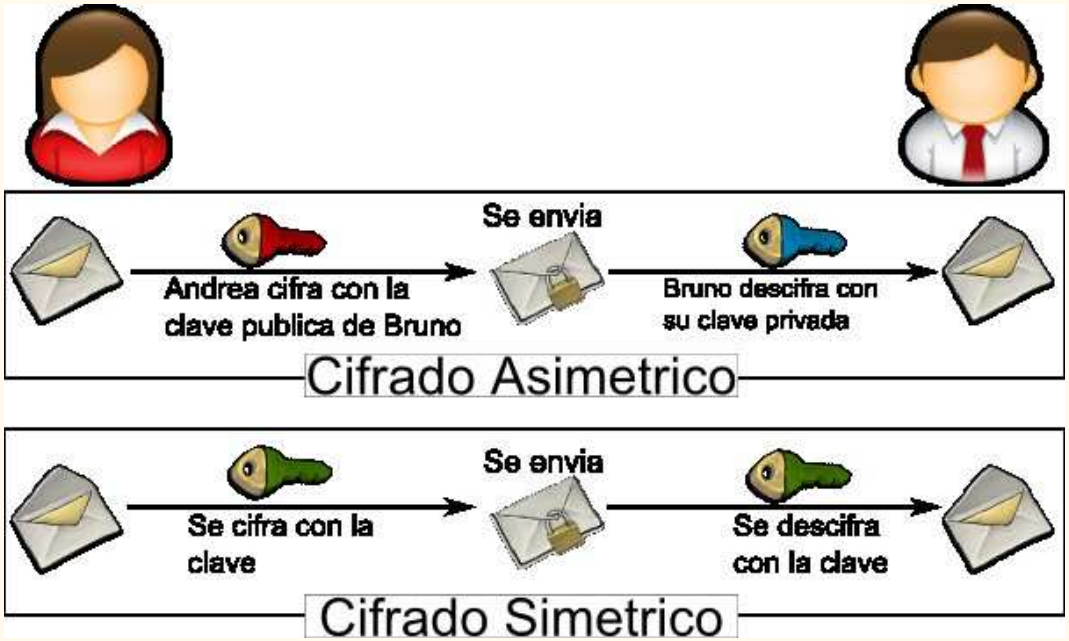
Mediante un **criptosistema**

Texto en claro

Algoritmo y Mecanismo + Claves

Texto cifrado (criptograma)

Algoritmos modernos / Simétricos - Asimétricos



Requisitos esenciales de un criptosistema y su operación

- Algoritmo/matemáticas “sólidas” (puertas traseras)
- Implementación sin fisuras (errores de implementación)
- **Claves: fortaleza, intercambio, custodia** y su **reemplazo** “frecuente”

Fallan si:

- Se pierde el secreto de la(s) clave(s)
- Ataques de fuerza bruta (si algoritmo o/y clave débiles)

> At present, there is no known practical attack that would allow someone without knowledge of the key to read data encrypted by AES when correctly implemented.

Open Source and Security

- Kerckhoffs' principle
  - Auguste Kerckhoffs: 19th Century Dutch linguist and cryptographer
  - Made an important realization:

> "The security of any cryptographic system does not rest in its secrecy, it must be able to fall into the enemy's hands without inconvenience."

The adversary knows the system
(Claude Shannon)

  - As opposed to "security through obscurity"

- **El sistema debe ser irrompible al menos en la práctica, si es que fuera matemáticamente rompible.**

- **La efectividad del sistema no debe depender de que su diseño permanezca en secreto, y no debe ser un problema que caiga en manos del enemigo.**

- La clave debe ser fácilmente memorizable de manera que no haya que recurrir a notas escritas.
- Los criptogramas deberán dar resultados alfanuméricos.
- El sistema debe ser operable por una única persona.
- El sistema debe ser fácil de utilizar.

Claves

Fortaleza

Diccionario, relacionadas con el usuario, fechas, nombres, duplicaciones, cortas, escasos signos, rehusadas para objetos distintos, …

Frases largas

bajoelmar_rielaba20veces#la#perestroika

Sintéticas

u/rLAbj0pdZQxCxtQFoeHcUhsF6lQEFMow/RKsFQsPqiMB/BkC==Q3GXs8r

Intercambio

Presencial, por carta/fax/telegrama, en containers cifrados, remoto?

Canales alternativos: telegram, signal, whatsapp, llamada de voz, SMS

Clave pública/privada: “autoridad” de certificación / “quedadas” (no vayas a mandar secretos a la persona equivocada…)

Custodia

Memoria, agenda, archivos, …

Clavijeros – locales (Keepass) en la nube (lastpass) / una contraseña para guardarlas todas!

Custodio

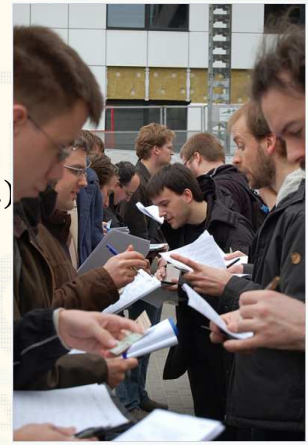
Claveros

Uso

Infraestructura corporativa

Depósito/Scrow

Que hacer si perdemos al clavero



Fiesta de firmado de claves en frente del FOSDEM 2008.

Problemas

No se puede tratar información cifrada

¿cómo sumar hj809 + jik332 ?
¿cómo enviar un correo electrónico a nuestro cliente Fkko#gim56?
¿búsquedas entre la información?

Manejo de las claves

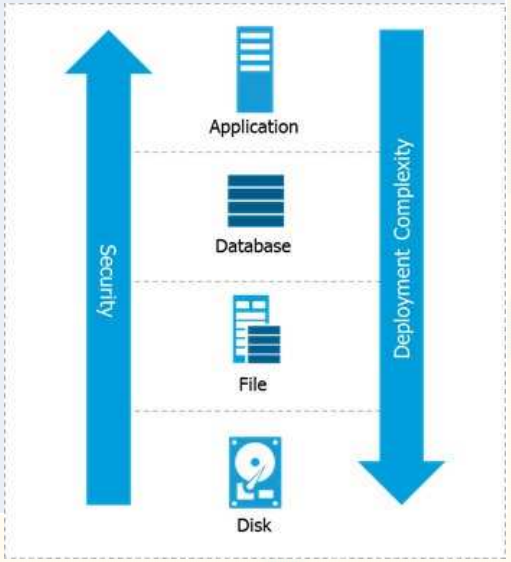
¿Quién las conoce? ¿Qué haces cuando esta de vacaciones? ¿Cómo operan los sistemas de información?
¿Quién descifra la base de datos?
¿Pérdida de claves? (móvil del finés; huella en móvil de fallecido)

Sistemas de información

¿Acceso a texto en claro en procesos de cifrado/descifrado?
¿Integridad de la plataforma?
¿Tienen los de TI las claves de las nóminas?

¿Qué podemos cifrar?

Información en reposo	Información en tránsito	Información en tratamiento
Protegida cifrando la información (no se implementa por defecto)	Protegida enviando información cifrada (capsulas cifradas) o cifrando el canal de envío (de información en claro o cifrada)	Protección compleja Atención on/premises (local) off/premises (nube)
• Ficheros “sueltos” en nuestro disco (USB, CD, etc.) • Todo una carpeta de nuestro PC • Cifrado completo de PCs, tabletas, móviles (protege la información si la plataforma es integra, aunque los perdamos) • Ficheros “sueltos” en nuestro disco en la nube (protege la información si los subimos cifrados) • Dockers/MV • Almacenes de claves de usuario • **Bases de datos** • **Backups**	Correo electrónico - Cuerpo y/o adjuntos (no se implementa por defecto) Información subida/bajada por web (solo si “candado on”) Intercambios de correos electrónicos (canal cifrado) (no se implementa por defecto) Cloud-gateways	**SANDBOXING**



Nube y cifrado

- Datos cifrados en la nube no son datos personales, ¿o sí?
- Si no lo son,
  - No hay encargados
  - No hay terceros países

Desenlace

¿Cuándo cifrar?

- La naturaleza de los datos y su tratamiento conlleve un riesgo elevado para los derechos y libertades (categorías especiales; datos sensibles como información financiera) (High Wins)
- Limitar riesgos innecesarios (transmisiones por correo electrónico, dispositivos móviles, soportes USB/CD, Back-ups) (Quick Wins)
- BBDD ¿?
- Almacenamiento en la nube
  - Reducción de riesgo
  - Evitar encargos de tratamiento

EE UU amenaza a España con no compartir información si no excluye a Huawei de sus redes 5G

Cifrado, ¿para qué?

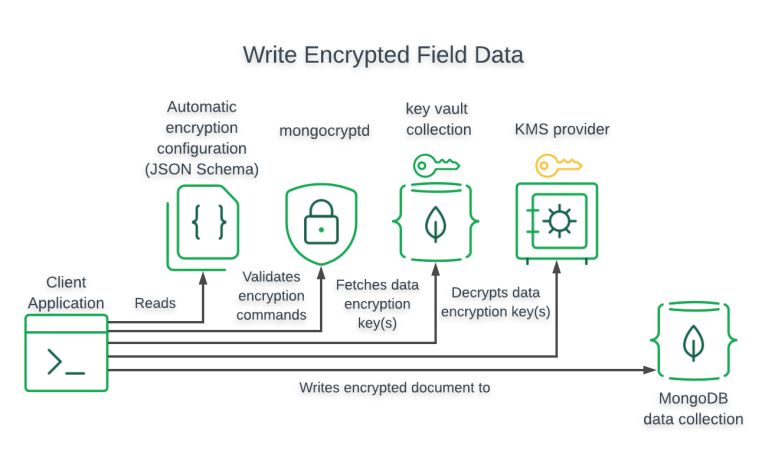
- Accountability/proactividad-diligencia y prevención (reducción de incidentes) (medida de seguridad)
- Evitar la necesidad de notificar en casos de brechas de seguridad
- Evitar encargos de tratamiento (datos cifrados en la nube no son datos personales, ¿o sí?)

Implicaciones

Transformación de TI por el RGPD

- **Pseudonimización**
- **Estrategia de empleo de cifrado**
  - **Almacenamiento cifrado y transmisión cifrada**
  - **Refactorizado de aplicaciones corporativas**
    - Guardar información cifrada
    - Gestión integral de claves
    - Segregación de funciones (ni administrador ni aplicación tienen la clave; fin de aplicaciones-usuarias genéricas; el encargado funcional/seguridad interna responsable(s) de “su” clave)

    - Cifrado como **estrategia organizativa** y no como parches individuales
    - Control de acceso estricto
    - Fomentar el uso de cifrado por los grupos de interés



Implicaciones

Mientras tanto… aspectos prácticos … Datos personales

- No debe/debiera haber en equipos móviles (PCs, tabletas, móviles) o dispositivos de almacenamiento (memorias USB, CDs,…) sin estar cifrados (dispositivos en cifrado preboot y con control fuerte de acceso) (robos/pérdidas/ataques), y con las debidas claves de acceso a los equipos (integridad).

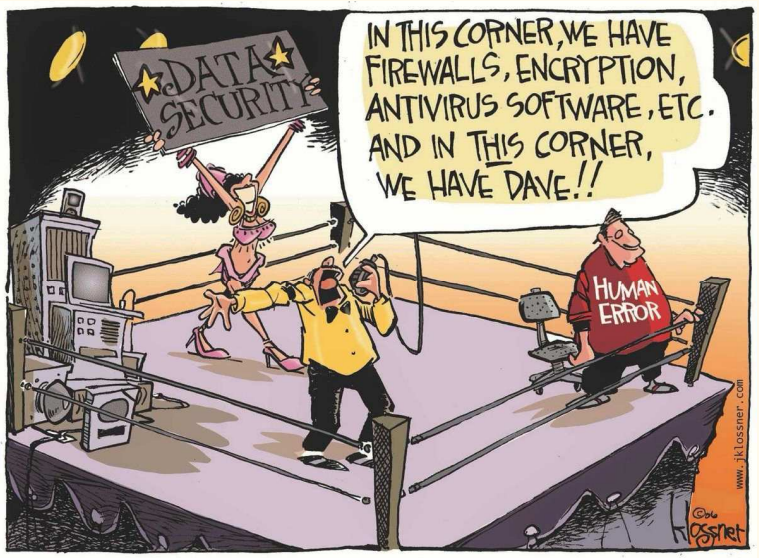
- No remitir datos personales en el cuerpo del correo electrónico, únicamente, en su caso, en adjuntos cifrados. Si es posible, cifrado de correo (PGP). Adjuntos cifrados (puede ser un zipper con AES). También mediante certificados digitales (DNI/Ceres).

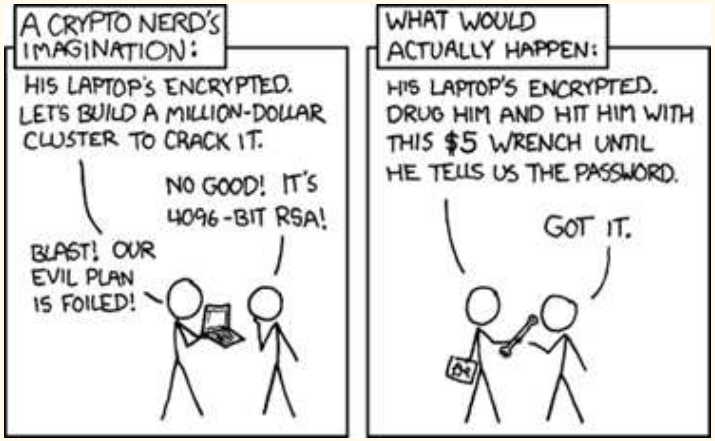
- No debiera emplearse almacenamiento no cifrado en nube (hay hw/sw de cifrado/descifrado transparente)

- Claves fuertes, sin reuso y con cambios frecuentes.

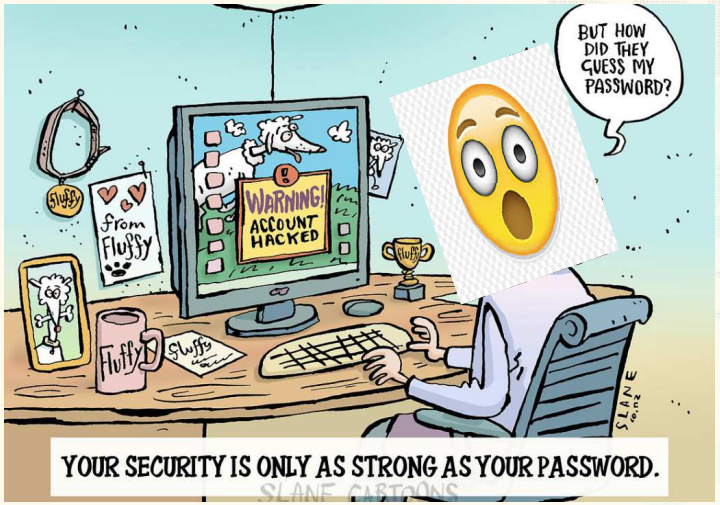
- Almacenes cifrados de claves de cifrado

Despedida y cierre


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06 Klossner


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.


23:10
SLANE
After hours, it's not your desk anymore


BUT HOW DID THEY GUESS MY PASSWORD?
WARNING! ACCOUNT HACKED
from Fluffy
Fluffy
SLANE
YOUR SECURITY IS ONLY AS STRONG AS YOUR PASSWORD.

Caveat emptor

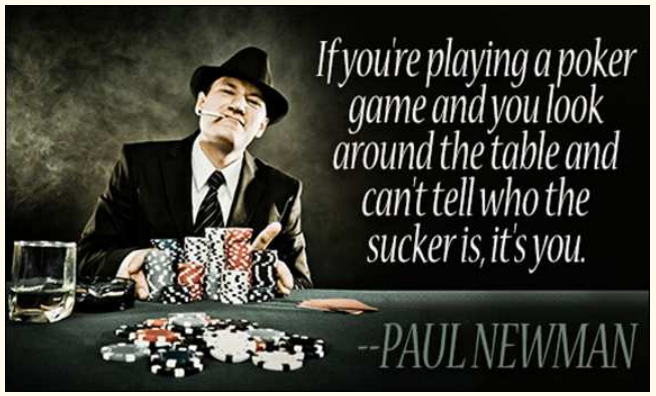
- Webmails: tratan los correos (publicidad) y pueden leer los correos; y los correos de un proveedor a otro no pueden ir cifrados (pueden ir en canal cifrado)

descifra en el navegador web.[10] Los correos electrónicos de una dirección no ProtonMail a otra de ProtonMail se envían como cualquier otro correo electrónico normal.

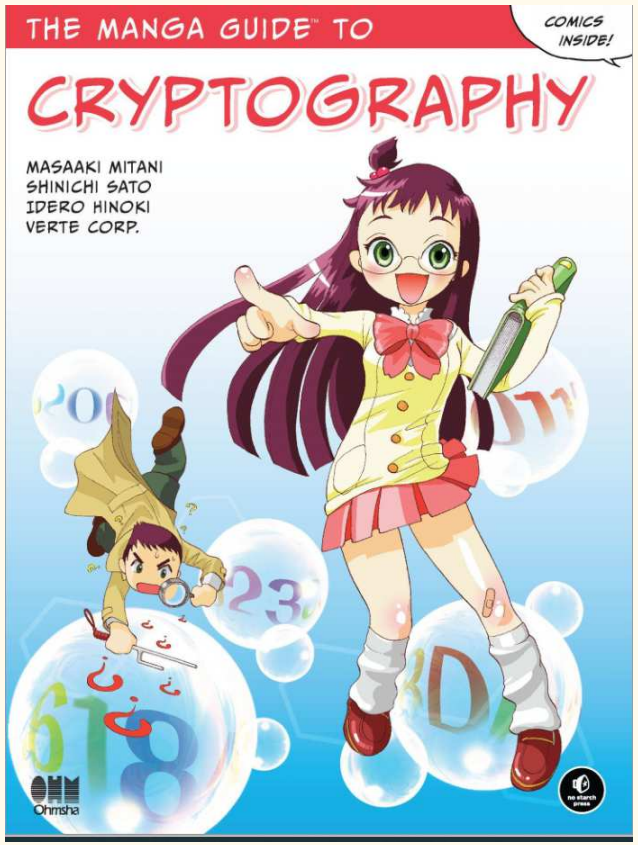
Google on Tuesday also clarified how the company itself uses the data. The search giant said last year it would stop scanning user emails for data that helps marketers target ads.

"The practice of automatic processing has caused some to speculate mistakenly that Google 'reads' your emails," the blog post says. "To be absolutely clear: no one at Google reads your Gmail, except in very specific cases where you ask us to and give consent, or where we need to for security purposes, such as investigating a bug or abuse."

Caveat emptor



Critografía para humanos



Sitios interesantes sobre cifrado y privacidad

https://t.me/catarsisdedpds

谢谢