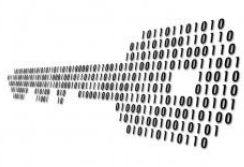


Cifrado & PGP

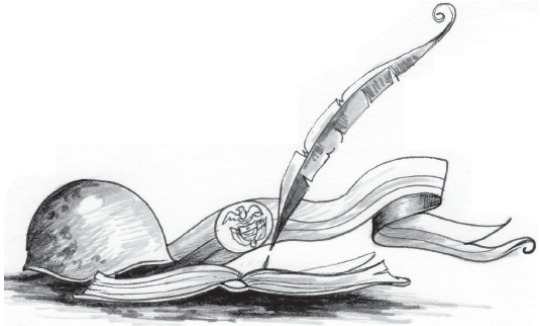
Cryptoparty.ec

Jorge Andrés Delgado

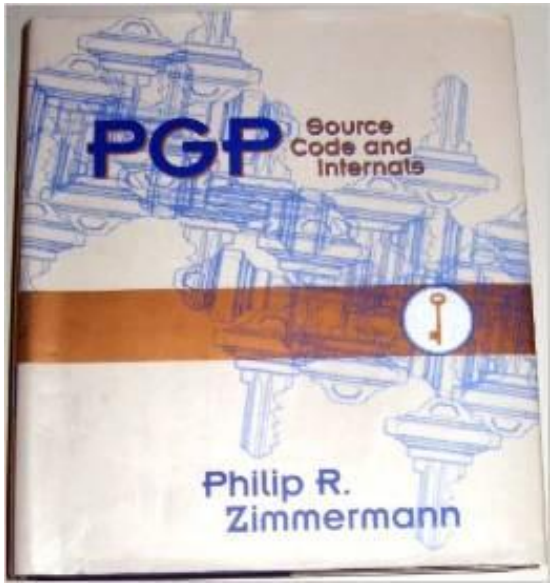
¿Qué?

Crypto Wars

- 70’s: El gobierno de Estados Unidos quiere tratar al software y a los algoritmos de cifrado como armas de guerra.



Crypto Wars



- 90’s: Computadora personal
- Comercio electrónico
- Phil Zimmermann

Crypto Wars

Si la privacidad está fuera de la ley, sólo los proscritos tendrán privacidad. Las agencias de inteligencia tienen acceso a una buena tecnología criptográfica. Lo mismo ocurre con los grandes traficantes de armas y drogas. Lo mismo ocurre con los contratistas de defensa, compañías petroleras y otros gigantes corporativos. Pero la gente común y las organizaciones sociales políticas, en su mayoría, no han tenido acceso a tecnología militar asequible de cifrado de clave pública. Hasta ahora. PGP faculta a las personas a tomar su privacidad en sus propias manos. Hay una creciente necesidad social de la misma. Por eso la escribí.

Philip Zimmermann, Why Do You Need PGP?

Crypto Wars

1920

1901

FOR MUCH OF THE CENTURY, THE BRITISH HAD A MONOPOLY ON WORLDWIDE CABLE TAPPING BECAUSE THEY OWNED MOST OF THE CABLES IN THE WORLD

VAST CABLE NETWORK OWNED BY A BRITISH COMPANY IN 1901

Los gobiernos

1. Siempre buscan espiarte
2. A veces son atrapados y se detienen por momentos
3. Nunca son juzgados

El costo de espiar

El gobierno de Ecuador

- Ha adquirido equipos de espionaje para telefonía celular y ordenadores (de lo que sabemos)
- Tiene un presupuesto anual de 58 millones de dólares
- Y… 1, 2, 3, 4, 5

Espionaje en Ecuador

http://www.larepublica.ec/blog/opinion/2014/04/26/espionaje-quitenos-embajada-estados-unidos

¿Por qué?

La carrera armamentista digital: La NSA prepara a EEUU para la próxima batalla

Posted on **18/01/2015** by **admin**

Artículo original en SPIEGEL por *Jacob Appelbaum, Aaron Gibson, Claudio Guarnieri, Andy Müller-Maguhn, Laura Poitras, Marcel Rosenbach, Leif Ryge, Hilmar Schmundt y Michael Sontheimer*

¿Cuándo?

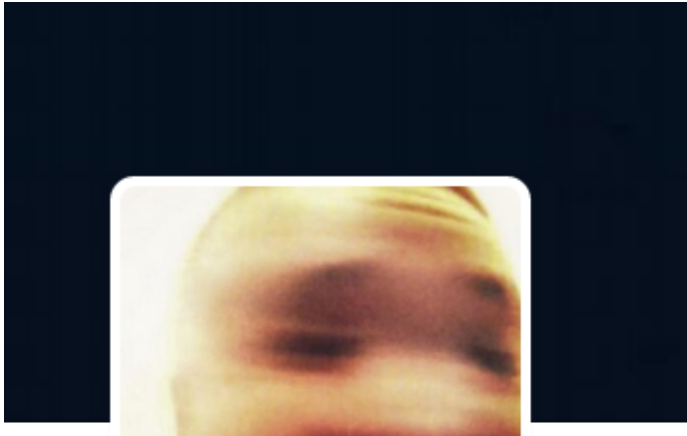
50Sombrasde...
@jose_miguel70

Seguir

@AndresDelgadoEC excelente!! El sepelio de Crudo Ecuador #UstedGanó pero ten cuidado no sea q te tachen de Terrorista =S

RETWEETS
2

10:33 - 20 de feb. de 2015



Jano Molina Torres
@janomolina

Ex-estereotipo de publicista, pecador alcanzado por la gracia de Dios, misionero urbano, futuro perseguido.

¿Cómo nos espían?

Rastros digitales

YO Y MIS SOMBRAS

Estar al tanto de la privacidad en internet, no es una tarea sencilla

english | français | español | العربية | русский | اردو

RASTREAR MI SOMBRA

Usa esta herramienta para ver cuáles rastros has dejado en Internet, y explora formas para mitigarlos.

https://myshadow.org/es

¿Cómo lo uso?

1 MARCA LOS DISPOSITIVOS QUE USAS CON INTERNET.

2 DA CLIC EN Y PARA NAVEGAR

¿Cómo protegerse?

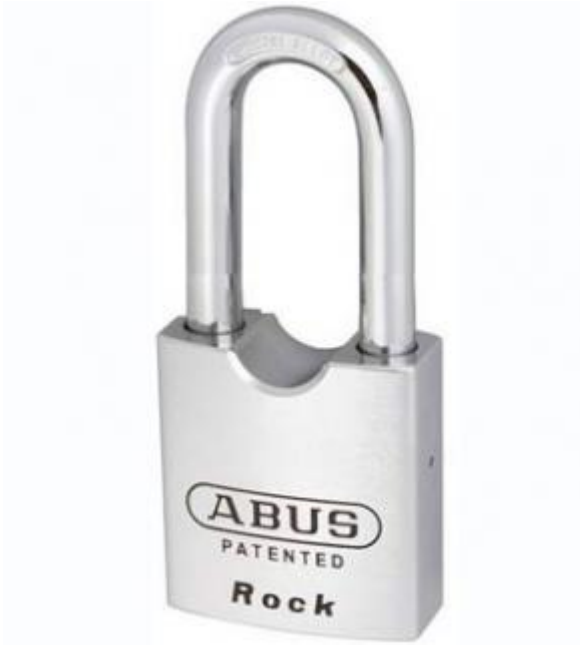
Tu segunda crypto party

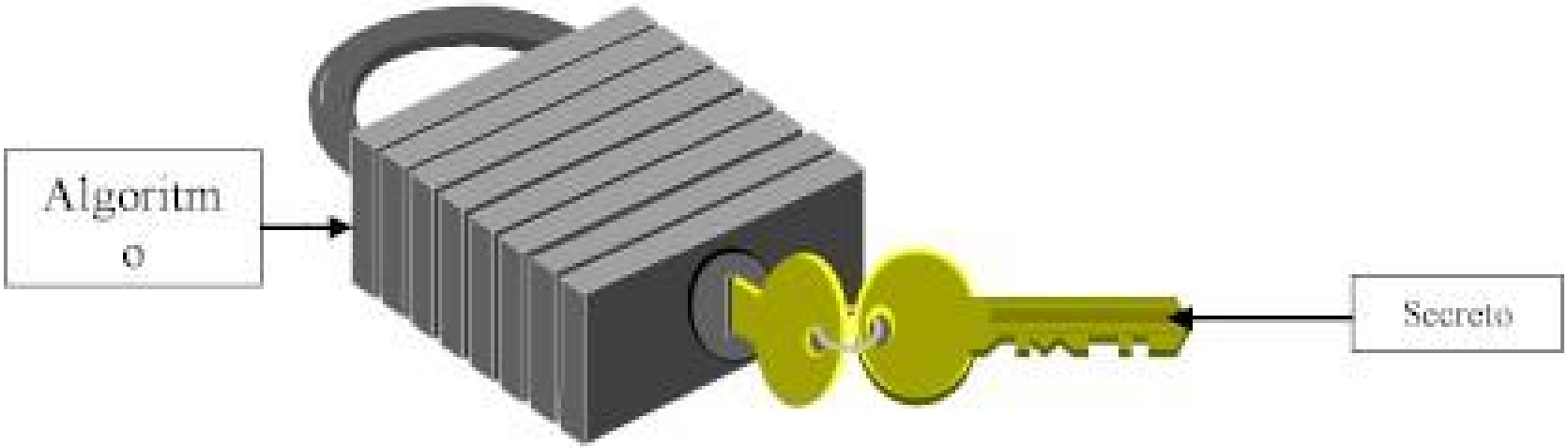
Chaos Computer Club

Niveles de seguridad

Niveles de seguridad

PGP


ABUS
PATENTED
Rock


Algoritm
o
Secreto

CIFRADO | **DESCIFRADO**

Multiplica

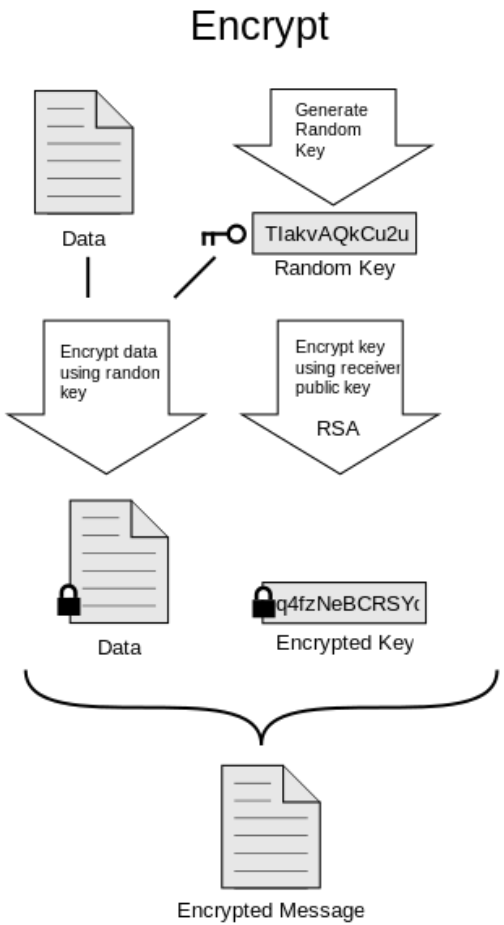
3251

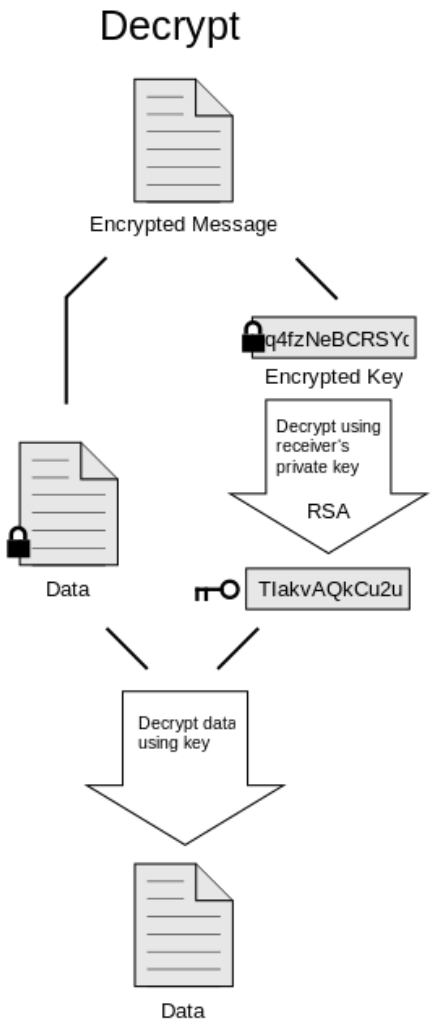
<u>x 125</u>

Factoriza

406377


Factor
565665465345345343543345335345354345435 3
Calculate
Multiply
24347 6835345345564 × 453454345343453534
Calculate
15 Years 10 Months 1 Week 12 Hours 55 Minutes
12 Years 8 Months 6 Days 20 Minutes
9 Years 6 Months 4 Days 12 Hours 11 Minutes 40 Seconds
6 Years 4 Months 3 Days 10 Minutes
3 Years 2 Months 1 Day 12 Hours 1 Minute 40 Seconds
0 Seconds
-3 Years 2 Months 1 Day 12 Hours 1 Minute 40 Seconds
Time Required
50
100
150
200
250
300
Size Of Input
Factor
Multiply


Encrypt
Generate Random Key
Data
TIakvAQkCu2u
Random Key
Encrypt data using randon key
Encrypt key using receiver public key
RSA
Data
q4fzNeBCRSYc
Encrypted Key
Encrypted Message


Decrypt
Encrypted Message
q4fzNeBCRSYc
Encrypted Key
Decrypt using receiver's private key
RSA
Data
TIakvAQkCu2u
Decrypt data using key
Data