Cifrado e identidad, no todo es anonimato

Foro sobre el Software Libre y las Culturas Libres

Gunnar Wolf

Facultad de Ciencias, UNAM
6 de abril, 2016

gwolf@debian.org
AB41 C1C6 8AFD 668C A045 EBF8 673A 03E4 C1DB 921F

Temas

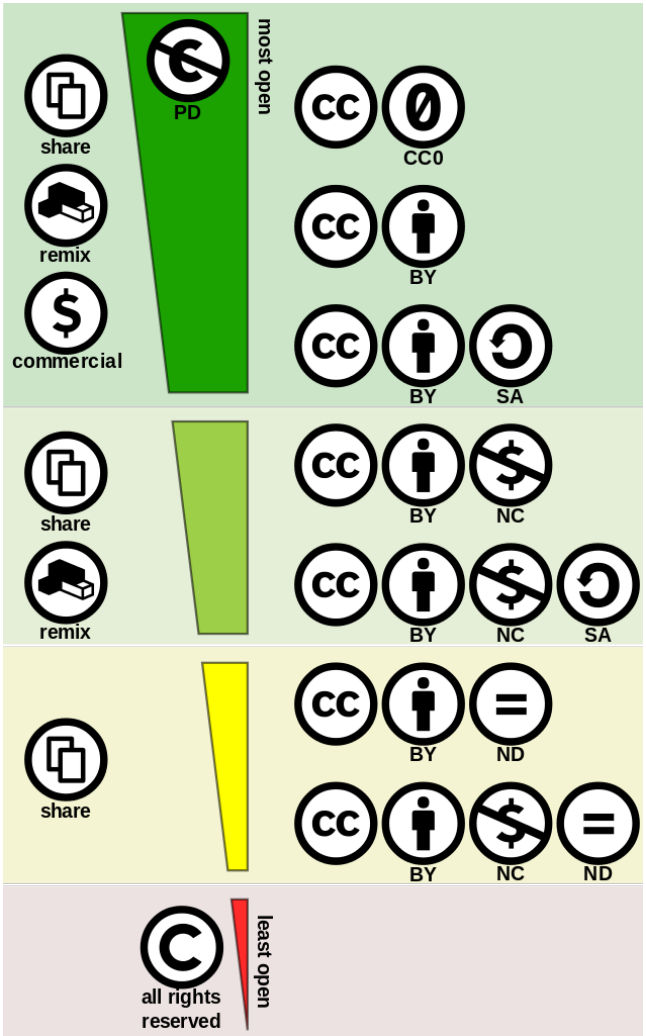
Hola. Soy Gunnar, y soy programador.

(En este punto, se espera que ustedes respondan a coro: *¡Hola Gunnar!*)

Hola. Soy Gunnar, y soy programador.

(En este punto, se espera que ustedes respondan a coro: *¡Hola Gunnar!*)

Pera, pera, pera... ¿CC-BY? ¿...?



¿Se fijaron en el licenciamiento que uso?

Eso significa que esta obra es apta para *obras culturales libres*

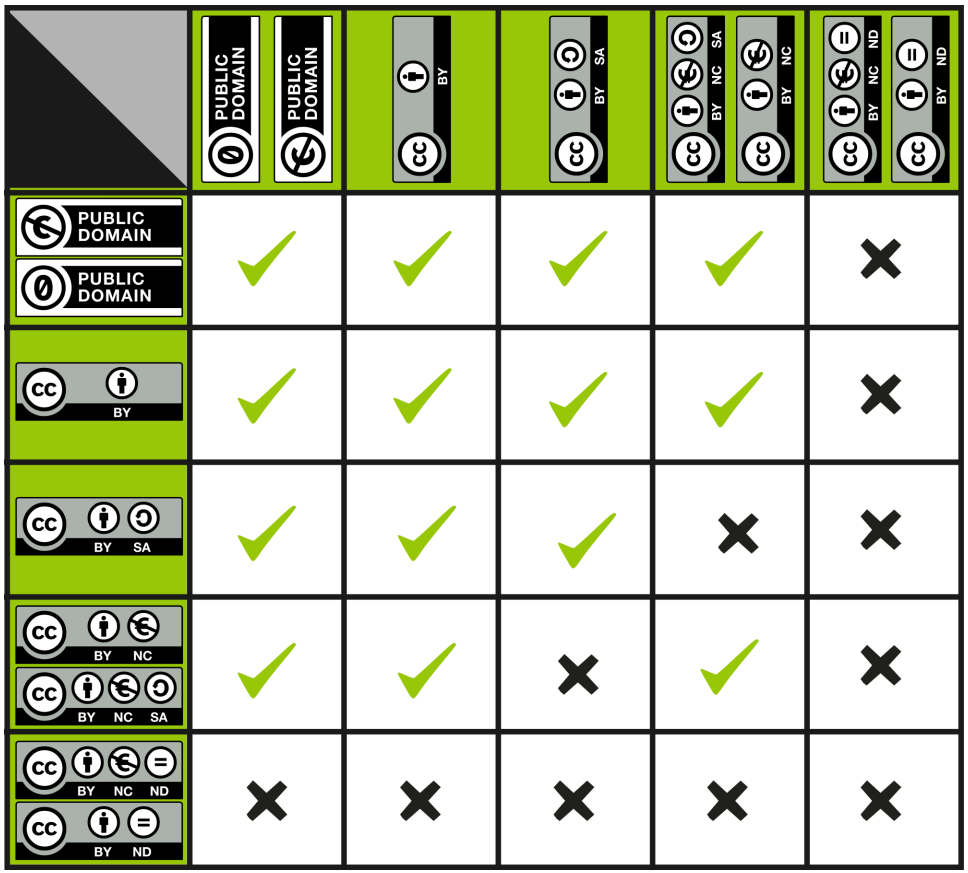
...Pero *incluye material* con términos de uso distintos (¡y potencialmente incompatibles!), aunque *siempre* redistribuible.

Todas las imágenes de terceros empleadas mencionan los detalles de su autoría.

Shaddim (CC-BY)

¿Licenciamiento compatible?

Las licencias empleadas son *mutuamente compatibles*



Wikimedia Commons: The sanest mad hatter (CC-0)

Por si quedan dudas de derechos de autor y similares. . .

Bre Pettis (CC-BY-NC)

¡Perdón! Lo que el ponente quiso decir...

Wikipedia: Home taping is killing music (Dominio público)

Temas

Retomando el *SECO3*...

En este foro retomamos el trabajo que realizamos para el *Seminario Construcción Colaborativa del Conocimiento* (2009–2011)

A estas alturas ya debe estar mencionado el URL del libro, videos e información relacionada, pero va de nuevo:

http://seminario.edusol.info/

Y de ahí, vamos retomando:

Retomando el *SECO3*...

En este foro retomamos el trabajo que realizamos para el *Seminario Construcción Colaborativa del Conocimiento* (2009–2011)

A estas alturas ya debe estar mencionado el URL del libro, videos e información relacionada, pero va de nuevo:

http://seminario.edusol.info/

Y de ahí, vamos retomando:

¿Qué es «Hacker»?

¿«Ética hacker»?

Hackers: Necesarios para la sociedad.

Alexandre Dulaunoy (CC-BY-SA)

Hackers: Víctimas de la polisemia

- *Gran programador*
- Conoce todo acerca de su sistema
- Gurú
- Programa en cualquier lenguaje
- Se opone a la *propiedad intelectual*
- Usa lógica matemática, hasta al abordar esquemas legales
- ...

- Atacante informático
- Puede hacer cualquier cosa con cualquier computadora
- Amenaza a la seguridad
- Escribe virus, espías y todo tipo de *malware*
- *Ciberpirata*
- Rompe candados, roba y redistribuye información ajena
- ...

...Ya no podemos decir que un lado sea más cierto que el otro

Y ya hay inevitables cruzamientos

El imaginario: Hackers en tanto *ninjas*

Brian Klug (CC-BY-NC)

El imaginario (¿y la realidad?): Los hackers y *anonymous*

Santiago Zavala (CC-BY-NC)

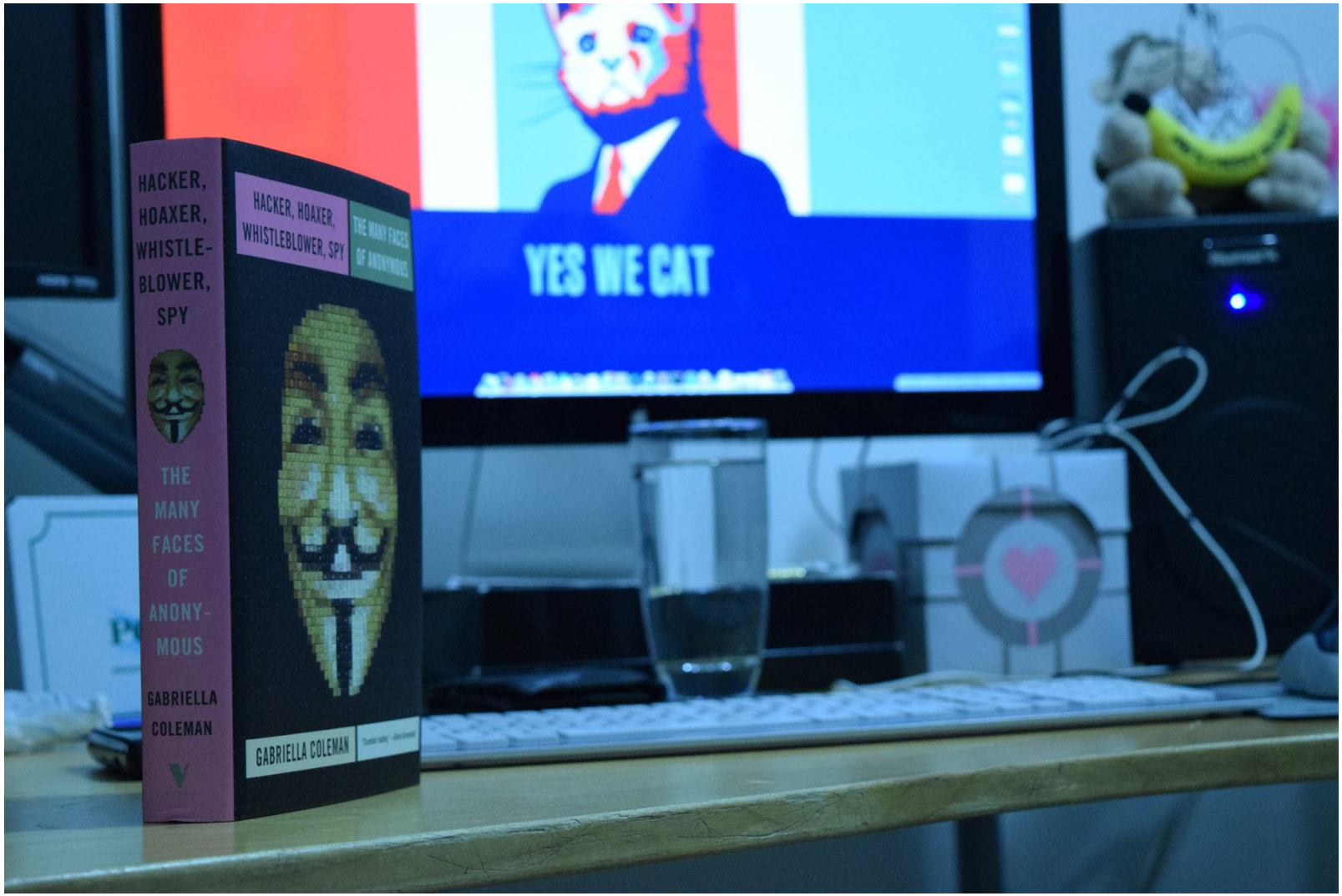
El imaginario (¿y la realidad?): Los hackers y *anonymous*

Katy Levinson (CC-BY-NC-SA)

Los hackers como objeto de estudio: Biella Coleman

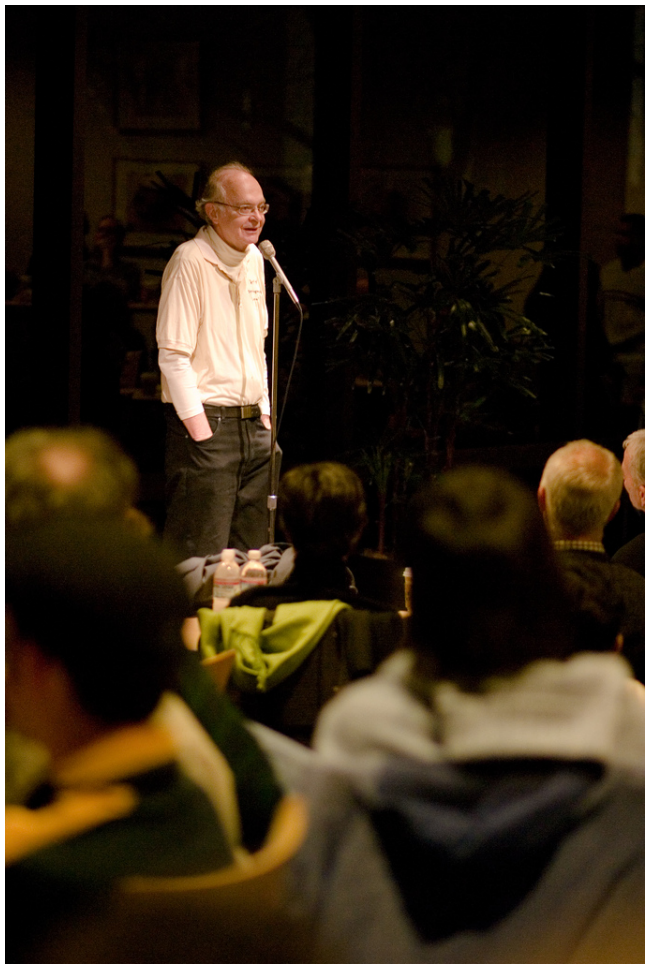
personaldemocracy (CC-BY-SA)

Los hackers como objeto de estudio: Biella Coleman



Biella "GabriellaÇoleman (CC-BY-SA-NC)

Hackers *netos*: Donald Knuth



La programación de computadoras es un arte, porque aplica conocimiento acumulado al mundo, pues requiere habilidades e ingenuidad, y particularmente porque produce objetos de belleza.

Donald Knuth, 1974

Scott Laird (CC-BY-NC-SA)

Hackers en tanto luchadores sociales: Richard Stallman

Pero... ¿No es hacker por ser *gran programador*?

- Peso relativo de sus muy distintas contribuciones
- Carga técnica histórica, realidad actual
- Impacto social y humano

Stallman es... Muy dificil de encasillar en una sola definición. Pero nos da muy buen pie para hablar de *ética hacker*

Ludovic Hirlimann (CC-BY-SA)

Hackers en tanto luchadores sociales: Richard Stallman

Pero... ¿No es hacker por ser *gran programador*?

- Peso relativo de sus muy distintas contribuciones
- Carga técnica histórica, realidad actual
- Impacto social y humano

Stallman es... Muy dificil de encasillar en una sola definición. Pero nos da muy buen pie para hablar de *ética hacker*

Ludovic Hirlimann (CC-BY-SA)

Hackers en tanto luchadores sociales: Richard Stallman

Pero... ¿No es hacker por ser *gran programador*?

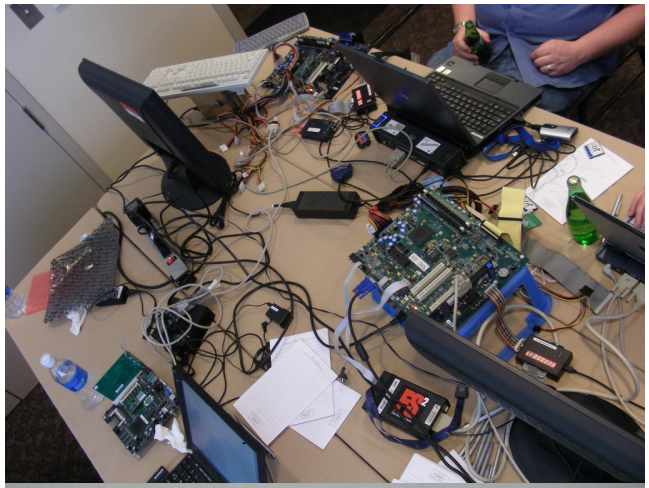
- Peso relativo de sus muy distintas contribuciones
- Carga técnica histórica, realidad actual
- Impacto social y humano

Stallman es... Muy dificil de encasillar en una sola definición. Pero nos da muy buen pie para hablar de *ética hacker*

Ludovic Hirlimann (CC-BY-SA)

Hackers y software libre

Ahora bien... Este foro es de *software libre y cultura libre*. ¿A qué vienen al cuento los *hackers*?



El autor *natural* de software libre es un hacker:

- *Scratch your own itches* → *Ráscate donde te pique*
- Resolver mis propios problemas empleando mi ingenio / inteligencia
- Compartir las soluciones que hallo; valor social del conocimiento colaborativo
- ...Y un largo etcétera!

Wikimedia Commons: Hacking CoreBoot (CC-BY-SA); Wikipedia: PSP-Homebrew (Dominio público)

Del software libre a la cultura libre

- El movimiento del *software libre* nace muy acotado a un área del conocimiento / creatividad
  - Por las *condiciones del mundo* de cuando se crea
  - El *acceso al medio* que hace posible la colaboración ($\approx$ 1980s) está *sesgado* hacia los programadores
- Conforme se masifica Internet, se abre hacia todas las áreas del conocimiento

Ser humano *implica* compartir conocimiento.
Está en nuestra naturaleza.

Wikimedia Commons: Kocio (CC-BY-SA); Wikipedia: shaddim (CC-BY-SA)

Del software libre a la cultura libre

- El movimiento del *software libre* nace muy acotado a un área del conocimiento / creatividad
  - Por las *condiciones del mundo* de cuando se crea
  - El *acceso al medio* que hace posible la colaboración ($\approx$ 1980s) está *sesgado* hacia los programadores
- Conforme se masifica Internet, se abre hacia todas las áreas del conocimiento

Ser humano *implica* compartir conocimiento.
Está en nuestra naturaleza.

Wikimedia Commons: Kocio (CC-BY-SA); Wikipedia: shaddim (CC-BY-SA)

¿Ética hacker?

Mil aspectos... Yo podría comenzar diciendo que:

- Pasar la realidad por un *filtro lógico*
  - ¿Algo disonante? ¡Señal de que algo anda mal!
- Negar los *monopolios artificiales sobre bienes intangibles*
  - *¡La información quiere ser libre!*
- Admirar la *belleza técnica*
- Desdén por la autoridad
  - Promover la *descentralización*
- Desdén por los grados y certificaciones formales
  - Se aprende haciendo, nunca se termina de aprender
- Participar en proyectos por *el gusto de hacerlo*
- ...

¿Ética hacker?

Al mismo tiempo, la otra *mitad* del concepto de hacker tiene otras ideas, más formalizadas (ej.: http://www.eccouncil.org/ o http://www.computerhope.com/jargon/e/ethihack.htm):

Certified Ethical Hacker

Para ser considerado ético, un hacker debe

- Obtener permiso escrito y expreso para probar redes e identificar riesgos
- Respetar la privacidad de la compañía e individuos
- Cerrar su programa sin dejar agujeros que otros puedan explotar
- Notificar al desarrollador o solicitante de cualquier vulnerabilidad localizada en su equipo

¿Mi opinión?

- Definición endógena / exógena
- Definición social / comercial
- Definición inclusiva / restrictiva

El segundo conjunto de definiciones me parece demasiado enfocado a... La venta de una certificación. Y por ende, anti-hacker.

Ze'ev Barkan (CC-BY)

¿Mi opinión?

- Definición endógena / exógena
- Definición social / comercial
- Definición inclusiva / restrictiva

El segundo conjunto de definiciones me parece demasiado enfocado a... La venta de una certificación. Y por ende, anti-hacker.

El mundo no es en blanco y negro.

Ze'ev Barkan (CC-BY)

Temas

¿Qué es la criptografía?

$\kappa\rho\upsilon\pi\tau o\sigma$ (Kryptos): Oculto
$\gamma\rho\alpha\phi\eta$ (Grafe): Escritura

Escritura oculta

Se refiere tanto al *arte* como a la *ciencia* de las técnicas de creación y recuperación de mensajes ocultos

¿Arte o ciencia?

Criptografía clásica Por más de 3000 años, *arte*

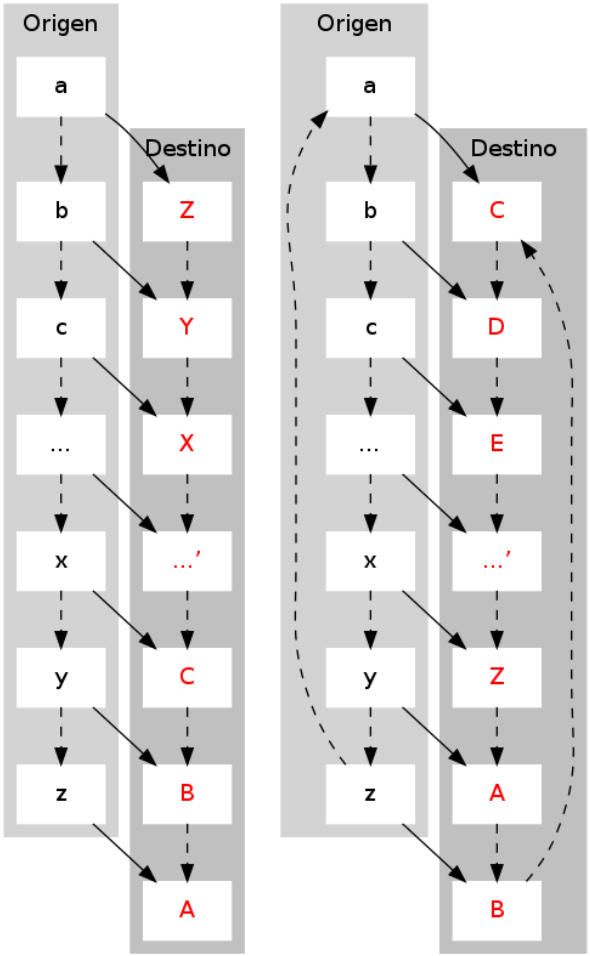
- Los métodos criptográficos, resultado del *ingenio* de cada creador
- Basan su *fuerza* en la *secrecía* sobre su existencia y funcionamiento
  - No en una *llave*
  - Espacio de búsqueda muy reducido, insuficiente

Criptografía moderna Desde los $\approx 1940 - 1970$ (distintos aspectos), *ciencia*

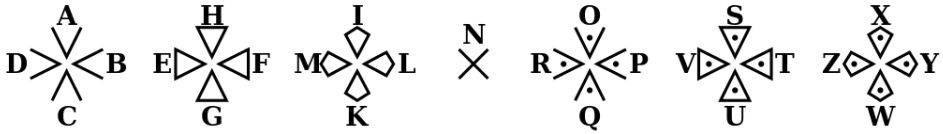
Criptografía como arte: Trasposición — la *escítala*

Wikimedia Commons: Luringen (CC-BY-SA)

Criptografía como arte: Substitución — *Atbash*, *César*, templarios y masones



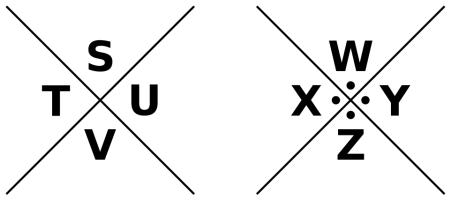
Cifrado *Atbash* (con alfabeto latino) y *César* (con n=2)



Cifrado *templario* (Wikimedia Commons: Alphabet templier)

A	B	C
D	E	F
G	H	I

J	K	L
M	N	O
P	Q	R



Cifrado *masónico* (Wikimedia Commons: Pigpen cipher key)

Criptografía como arte: En la cultura general

Figura: Arthur Conan Doyle: *La aventura de los bailarines* (Sherlock Holmes)

```
"53++!305))6*;4826)4+)4+).;806*;48!8]60))85;1+8*:+(;:+*8!83(88)5*!;
46(;88*96*?;8)*+(;485);5*!2:*+(;4956*2(5*-4)8]8*;4069285);)6!8)4++;
1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?34;48)4+;161;:
188;+?;"
```

Edgar Allan Poe, "The gold bug"

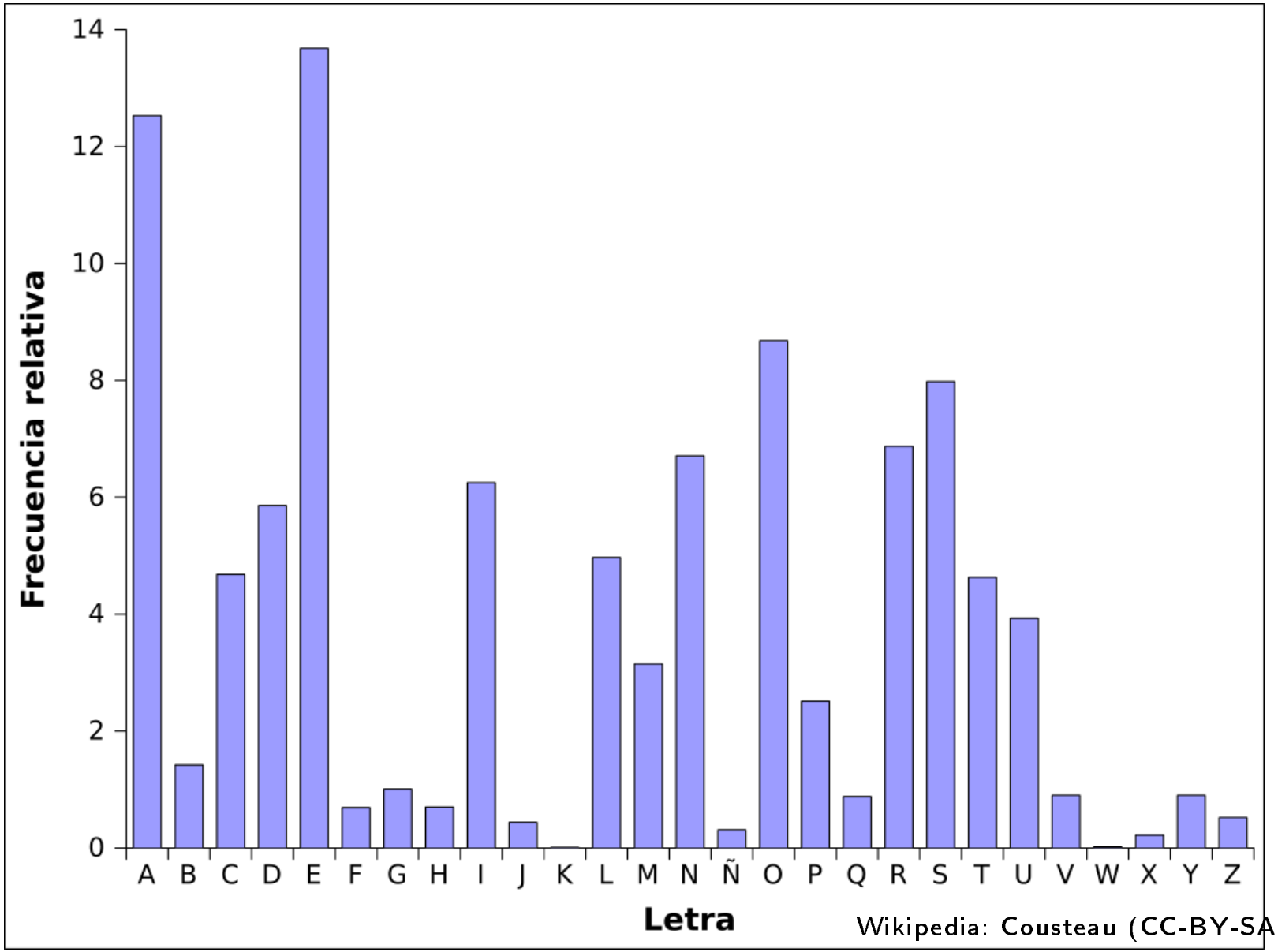
Edgar Allan Poe se equivoca...

Human ingenuity cannot concoct a cypher which human ingenuity cannot resolve

El ingenio humano no puede concebir un cifrado que no pueda ser resuelto por el ingenio humano

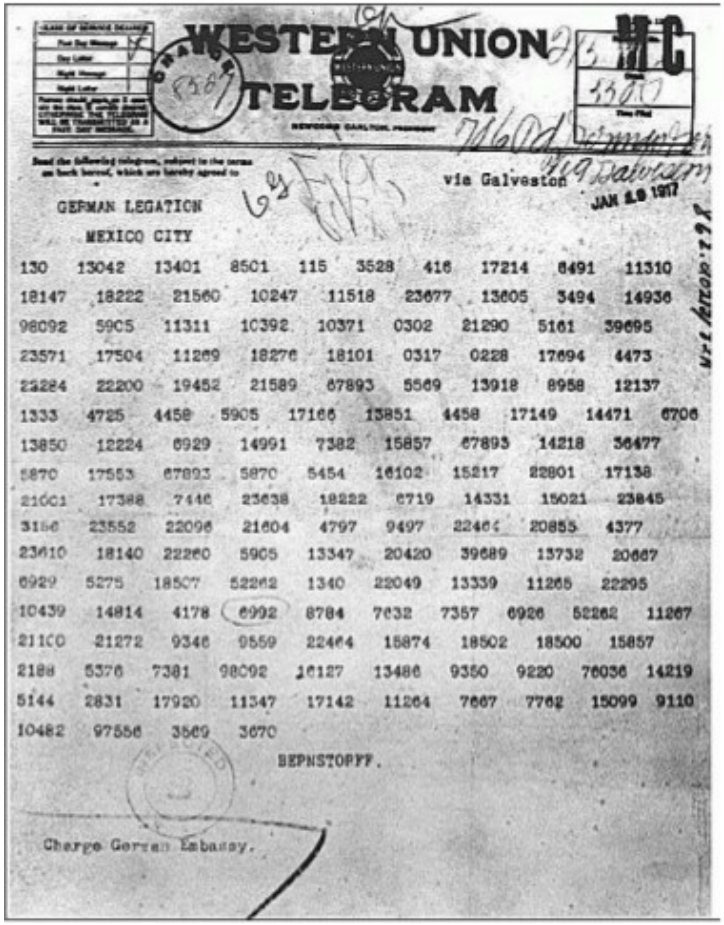
E. A. Poe ca. 1849
Dominio público; Wikimedia Commons

Criptoanálisis; análisis de frecuencias



Wikipedia: Cousteau (CC-BY-SA)

Criptografía en México: El *Telegrama Zimmermann* (1917)



WESTERN UNION TELEGRAM

via Galveston

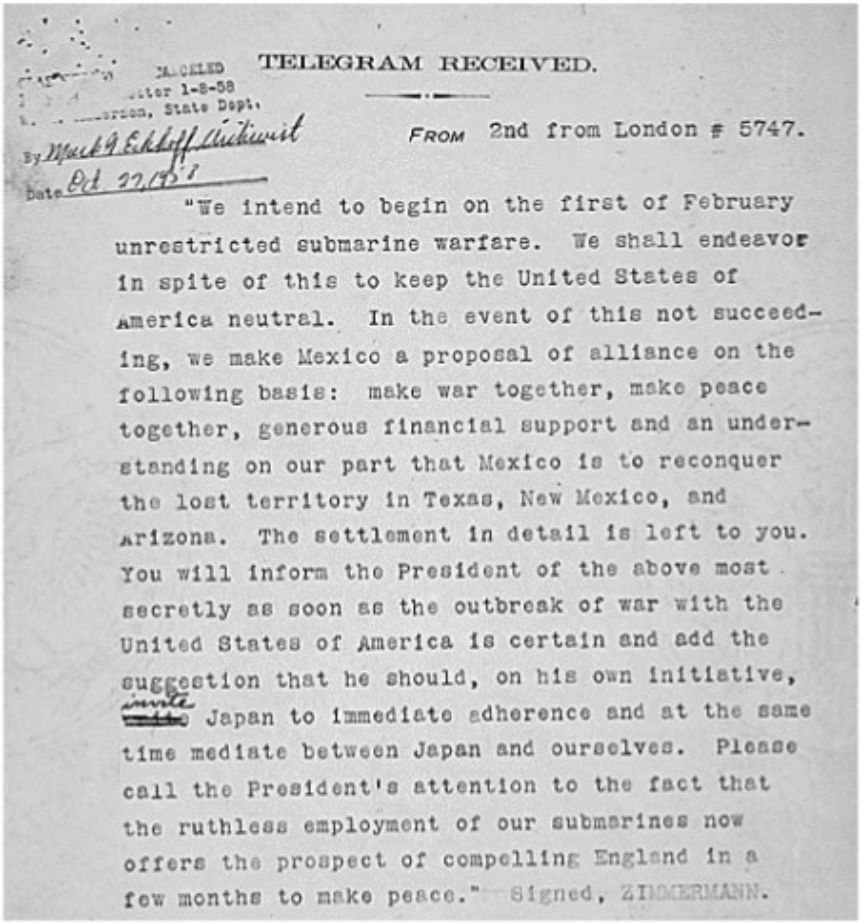
JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTORFF.

Charge German Embassy.



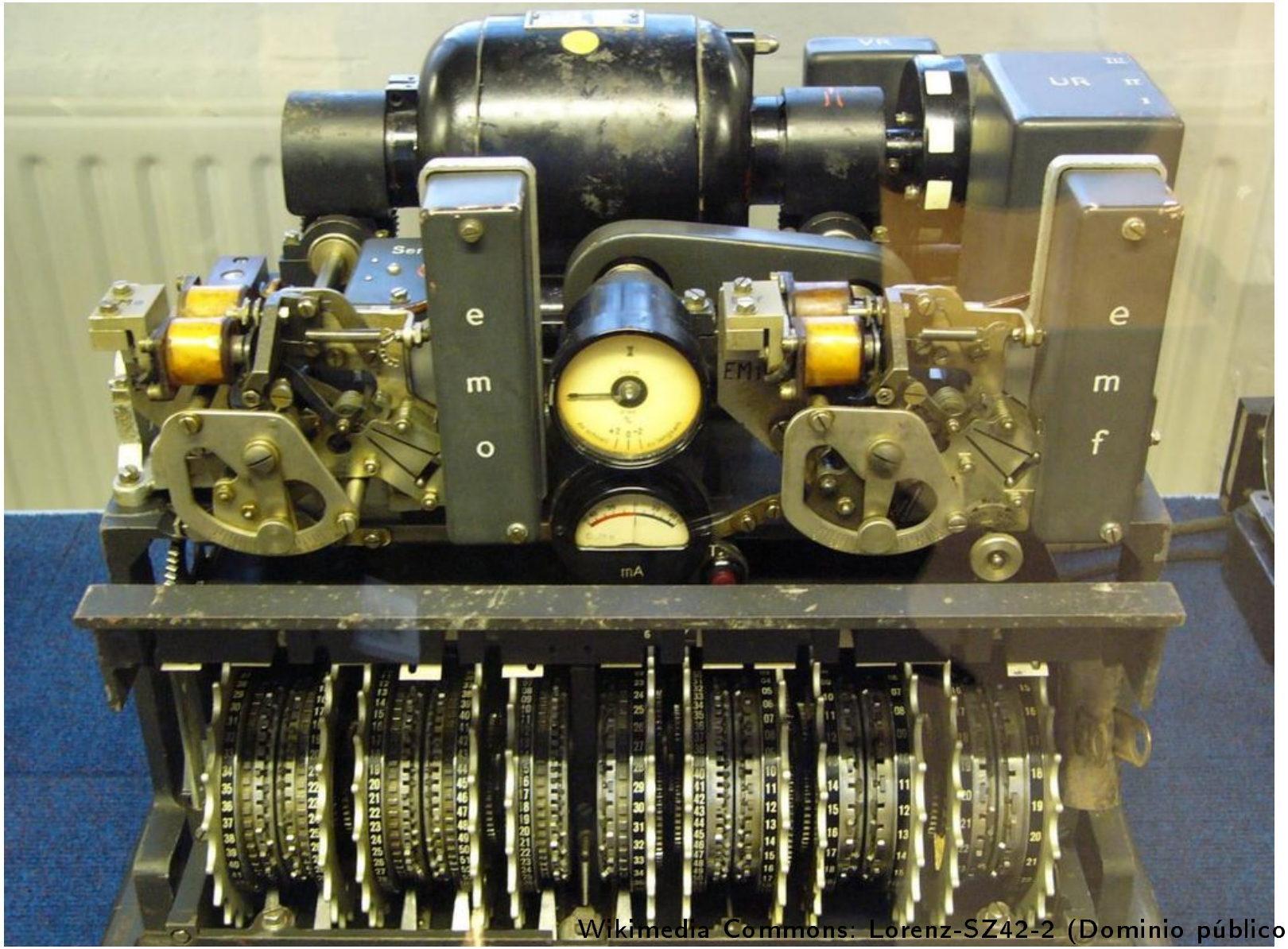
TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

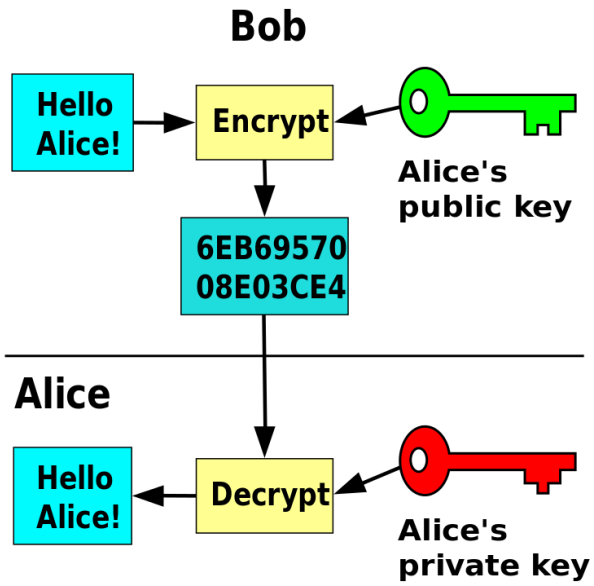
Wikipedia: Zimmermann Telegram (Dominio público)

S. XX: Criptografía mecánica



Wikimedia Commons: Lorenz-SZ42-2 (Dominio público)

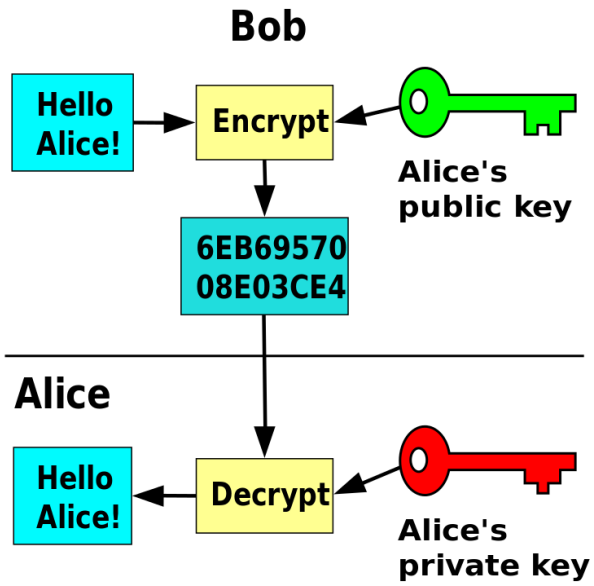
1976: *New directions in cryptography*



- Aparece la idea de que el cifrado maneje *dos llaves* por participante
  - Pública
  - Privada
- ¿Y qué son estas llaves?
  - Simplemente, números

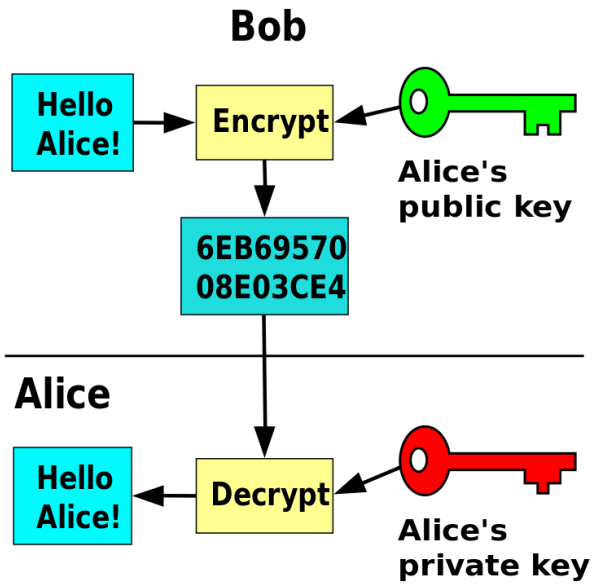
- ¿Y qué ganamos?
  - Poder compartir *libre y públicamente* las llaves de cifrado sin preocuparnos por la secrecía del *canal*

1976: *New directions in cryptography*



- Aparece la idea de que el cifrado maneje *dos llaves* por participante
  - Pública
  - Privada
- ¿Y qué son estas llaves?
  - Simplemente, números que guardan una relación especial entre ellos
- ¿Y qué ganamos?
  - Poder compartir *libre y públicamente* las llaves de cifrado sin preocuparnos por la secrecía del *canal*

1976: *New directions in cryptography*



- Aparece la idea de que el cifrado maneje *dos llaves* por participante
  - Pública
  - Privada
- ¿Y qué son estas llaves?
  - Simplemente, números que guardan una relación especial entre ellos y están unidos por una *transformación con puerta trasera*
- ¿Y qué ganamos?
  - Poder compartir *libre y públicamente* las llaves de cifrado sin preocuparnos por la secrecía del *canal*

¿Puerta trasera?

Micro-ejemplo **hiper**-simplificado

- Es relativamente fácil multiplicar dos números, pero muy dificil *factorizarlos*
- Tengo elegidos dos números *primos* de dos dígitos

  y
- Su producto es 391.
- Si no conozco a ninguno, tengo que hacer una búsqueda por *fuerza bruta*.

¿Cuáles son?

¿Puerta trasera?

Micro-ejemplo **hiper**-simplificado

- Es relativamente fácil multiplicar dos números, pero muy dificil *factorizarlos*
- Tengo elegidos dos números *primos* de dos dígitos
  - 17 y
- Su producto es 391.
- Si no conozco a ninguno, tengo que hacer una búsqueda por *fuerza bruta*.

¿Cuáles son?

- Basta saber con que uno es 17 para hacer una simple división: $\frac{391}{17} = \ldots$

¿Puerta trasera?

Micro-ejemplo **hiper**-simplificado

- Es relativamente fácil multiplicar dos números, pero muy dificil *factorizarlos*
- Tengo elegidos dos números *primos* de dos dígitos
  - 17 y 23
- Su producto es 391.
- Si no conozco a ninguno, tengo que hacer una búsqueda por *fuerza bruta*.

¿Cuáles son?

- Basta saber con que uno es 17 para hacer una simple división: $\frac{391}{17} =$ **23**
- ... Pero no lo hacemos con números de dos dígitos, sino que de entre *600 y 2000*

Únicamente un primer paso... ¡Hay que desarrollar un algoritmo alrededor del principio!

- Lo anteriormente explicado es sólo el *fundamento* de *uno de los algoritmos* de cifrado por llave pública
  - Para los curiosos, RSA
- Quede únicamente enunciado que:
  - Se eligen dos primos aleatorios p, q
  - $n = pq$
    - n será el *módulo* a emplear para ambas llaves, y es parte de la llave pública.
  - $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1) = n - (p+q-1)$
  - Se elige un entero aleatorio e tal que $1 < e < \phi(n)$ y $gcd(e, \phi(n)) = 1$ (*primo relativo* a $\phi(n)$)
    - e será parte de la llave pública.
  - Se encuentra $d \equiv e^{-1} (\mod \phi(n))$
    - d es la llave privada.
    - Para cifrar un mensaje m, $c = m^e \mod n$
    - Para descifrar un mensaje c, $m = c^d \mod n$

¡Cifremos al universo!

¡Felicidades!

- Con esto que sabemos, podemos realizar cifrado de *grado militar* (si usamos llaves suficientemente grandes/fuertes).
- Para mucha gente, el fin mismo de la criptografía es *cifrar nuestras comunicaciones*
  - Las protege del espionaje de terceros

Pixabay (Dominio público)

¡Cifremos al universo!

¡Felicidades!

- Con esto que sabemos, podemos realizar cifrado de *grado militar* (si usamos llaves suficientemente grandes/fuertes).
- Para mucha gente, el fin mismo de la criptografía es *cifrar nuestras comunicaciones*
  - Las protege del espionaje de terceros
  - ...Aunque no oculta el hecho de que *hay comunicación* entre dos actores A y B. Y recordamos lo que hemos aprendido respecto a los *metadatos*...

Pixabay (Dominio público)

Ahora, pongamos las cosas de cabeza

CoolKoon, Wikimedia Commons (CC-BY)

Pero... No nos detengamos *tanto* en el cifrado

La criptografía da para mucho más.

- Cifrar (*esconder el significado* de) las cosas es tal vez la menos divertida y útil de las propiedades
- ¿Qué pasa cuando comenzamos a *hackear* a la criptografía?

Pero... No nos detengamos *tanto* en el cifrado

La criptografía da para mucho más.

- Cifrar (*esconder el significado* de) las cosas es tal vez la menos divertida y útil de las propiedades
- ¿Qué pasa cuando comenzamos a *hackear* a la criptografía?
- Aparecen nuevas propiedades, podemos *inventar y comprender* otros usos y posibilidades.

Temas

¿Cómo podemos hacer las cosas al revés?

Sabemos que podemos cifrar y descifrar con la misma operación, empleando esto números "complementarios":[1]

$$c = m^e \text{ y } m = c^d$$

Pero... ¿Qué pasa si *invierto las llaves* que uso?

$$s = m^d \text{ y } v = s^e$$

[1] Definición no-matemática, *ad-hoc* e informal

¿Cómo podemos hacer las cosas al revés?

Sabemos que podemos cifrar y descifrar con la misma operación, empleando esto números "complementarios":[1]

$$c = m^e \text{ y } m = c^d$$

Pero... ¿Qué pasa si *invierto las llaves* que uso?

$$s = m^d \text{ y } v = s^e$$

Pera, pera, pera...

[1] Definición no-matemática, *ad-hoc* e informal

¿Cómo podemos hacer las cosas al revés?

Sabemos que podemos cifrar y descifrar con la misma operación, empleando esto números "complementarios":[1]

$$c = m^e \text{ y } m = c^d$$

Pero... ¿Qué pasa si *invierto las llaves* que uso?

$$s = m^d \text{ y } v = s^e$$

Pera, pera, pera... ¿Qué es eso de s y v?
¿Y qué gano con eso?

[1] Definición no-matemática, *ad-hoc* e informal

Imprimir mi identidad

Andy Hay (CC-BY)

Hackeando agrego funcionalidad a los criptosistemas

- Si únicamente yo conozco mi llave privada (d)...
  - Nadie más que yo puede pasar de m a s (llamémosle s por *signature*)
  - Pero cualquiera puede *verificar* (de ahí v) con mi llave pública que s viene de mí
- Más fuerte que una firma autógrafa o una huella digital
  - Aseguro que el mensaje *es genuinamente mío*
  - Y mi firma *cambia según cada mensaje*
  - No hay dos mensajes que generen la misma firma

Ojo: Primer acercamiento *super-incompleto* al tema. ¡Las firmas digitales no se emplean realmente así!

Aldon Hynes (CC-BY-SA)

¿Por qué a un *hacker* le interesa *firmar documentos*?

Belleza matemática Agregar funcionalidad y casos de uso por el mero hecho de hacerlo

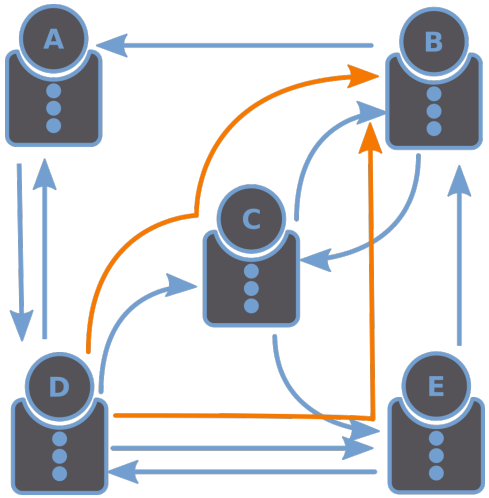
Credibilidad ¿Qué otra manera tengo de *demostrar a los demás* que algo realmente proviene de mí?

Colaboración en Internet Nuestros proyectos son de ámbito de desarrollo mundial. ¿Cómo podemos mantener un mínimo de cohesión?

¿Cómo confiar en alguien a no conozco?

(cómo confiar en *su identidad*, ¡no en *su persona*!)

- *David* leyó un texto interesante de *Beto*, y lo quiere invitar a colaborar para su proyecto secreto
  - Pero *David* y *Beto* no se conocen
- Pero *David* conoce a *Carolina* y a *Emilio*
  - Ambos firmaron un documento que dice, *Yo conozco a Beto, su llave pública es (n=391, e=125)*
- Con esta doble confirmación, *David* tiene ya *suficiente* confianza en la identidad de *Beto*.



Esto constituye una *red de confianza* (*Web of Trust*)

¿Red de confianza?

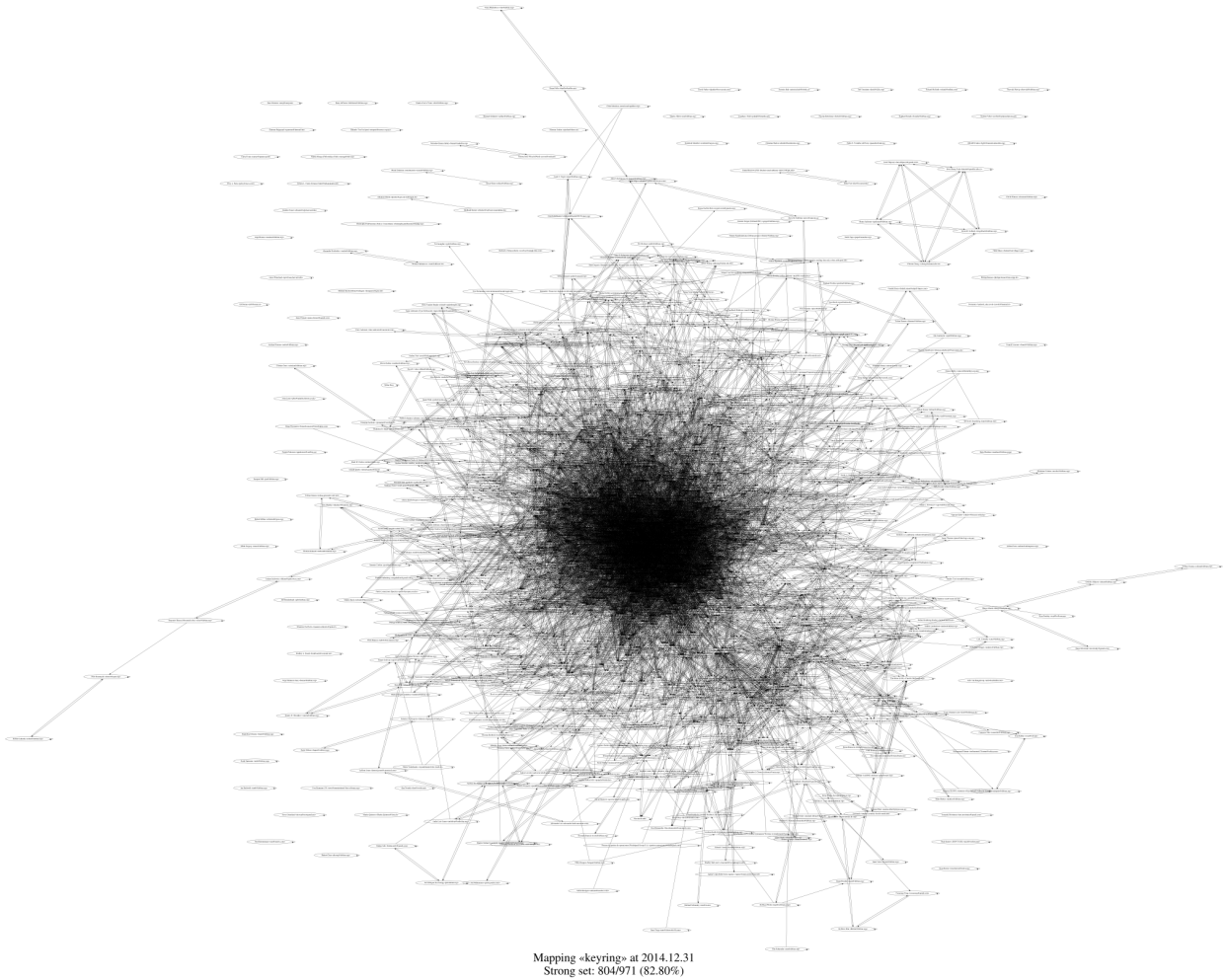


Figura: *Fotografía* del proyecto en el que participo, diciembre 2014. 971 llaves (identidades)

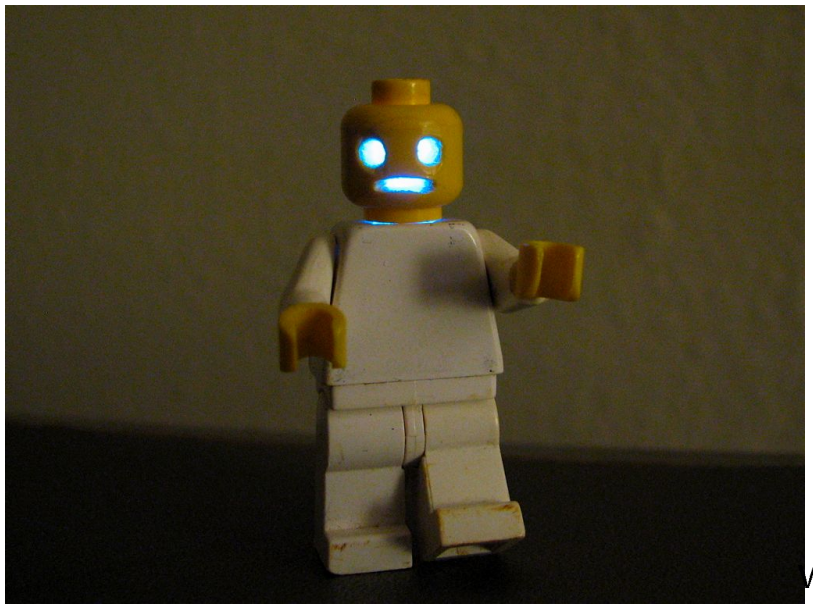
¿Y como pa' qué o qué?

Nomás por poner un ejemplo...
Los 971 de la foto anterior podemos...

Windell Oskay (CC-BY); Geoff Parsons (CC-BY-SA)

¿Y como pa' qué o qué?

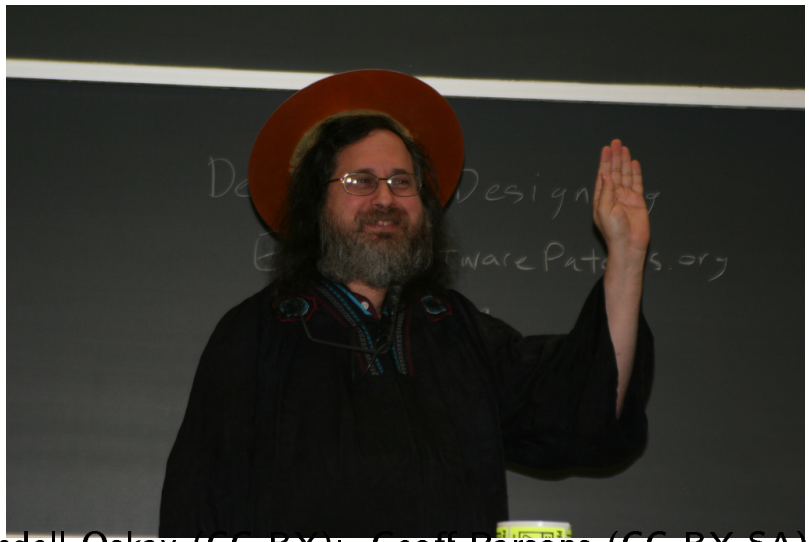
Nomás por poner un ejemplo...
Los 971 de la foto anterior podemos...
Subir y ejecutar programas arbitrarios en los *millones de computadoras* de usuarios de Debian



Windell Oskay (CC-BY); Geoff Parsons (CC-BY-SA)

¿Y como pa' qué o qué?

Nomás por poner un ejemplo...
Los 971 de la foto anterior podemos...
Subir y ejecutar programas arbitrarios en los *millones de computadoras* de usuarios de Debian
Pero, claro, somos gente linda, buena y honorable, de buena fé y tenemos palabra. No vamos a hacer nada malo.



Windell Oskay (CC-BY); Geoff Parsons (CC-BY-SA)

Temas

Bueno, pero... ¿y por qué nos cuentas esto?

- La tecnología por sí sola no es buena
  - Tampoco es mala
- Pero comprenderla nos permite aprovecharla
  - Comprenderla mejor nos permite *hackearla*
  - La creatividad nos permite encontrar nuevos usos
- Estas herramientas pueden trabajar para nosotros
  - También pueden trabajar *contra* nosotros

Colin Kinner (CC-BY)

Ya no hace falta que *venga yo* a ponerlos paranóicos (1)

Wikimedia Commons: Magnus Manske (CC-BY)

Ya no hace falta que *venga yo* a ponerlos paranóicos (2)

Wikimedia Commons: Smuconlaw (CC-BY-SA)

Ya no hace falta que *venga yo* a ponerlos paranóicos (3)

Gage Skidmore (CC-BY-SA)

Un mundo nos vigila

Wikimedia Commons: Guruharsha (CC-BY-SA, GFDL)

Ejemplo: Ruteo cebolla (va nomás platicadito)

Commons: Tor Project (CC-BY-SA)

Pero tarde o temprano, la puerca tuerce el rabo

Pixabay: Gellinger (Dominio público)

Conclusiones apuradas

- Hay mucho por hablar
- Temas apasionantes, que dan para mucha discusión
- Lo fundamental:
  - Apreciar la belleza algorítmica...
  - No quedarse contento con un conocimiento básico de las herramientas; *ser un hacker*
  - No confiarse con las herramientas que dicen protegernos, *pensar bien en las consecuencias de nuestro comportamiento*

Ok, ok, ya me voy. Quedan mis datos.

¡Muchas gracias por su atención, tiempo y paciencia!

Gunnar Wolf – gwolf@debian.org

AB41 C1C6 8AFD 668C A045 EBF8 673A 03E4 C1DB 921F

Instituto de Investigaciones Económicas – UNAM

Desarrollador del Proyecto Debian

http://gwolf.org/cifr_ident_anon