Criptografía Simétrica - Parte 1

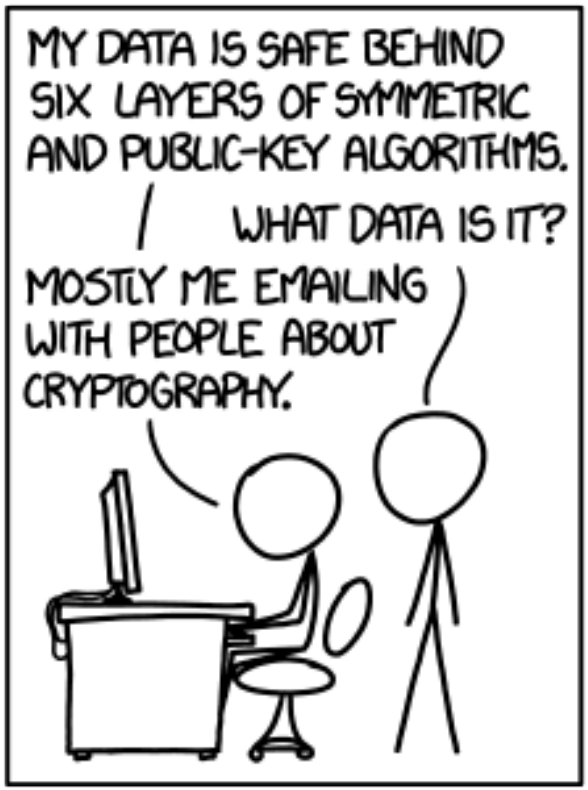
Miguel Angel Astor Romero

17 de mayo de 2019

Agenda

Introducción

- Supongamos que tenemos que comunicar un mensaje cuyo contenido es delicado.
  - Espionaje.
  - Disidencia política.
  - Inteligencia militar.
  - Información bancaria.
  - Información médica.
  - Otra información sensible.
- Hay que encontrar un mecanismo para ocultar mensajes en tránsito.



Definiciones

Criptología

Ciencia que estudia la criptografía y el criptoanálisis.

Criptografía

Ciencia que estudia las propiedades y el diseño de criptosistemas.

Criptosistema

Algoritmo, técnica y/o herramienta para cifrar mensajes.

Criptoanálisis

Ciencia que estudia el descifrado de un mensaje encriptado sin necesidad de la clave, basándose en propiedades del algoritmo o del texto cifrado.

Tipos de cifrado

Cifrado simétrico

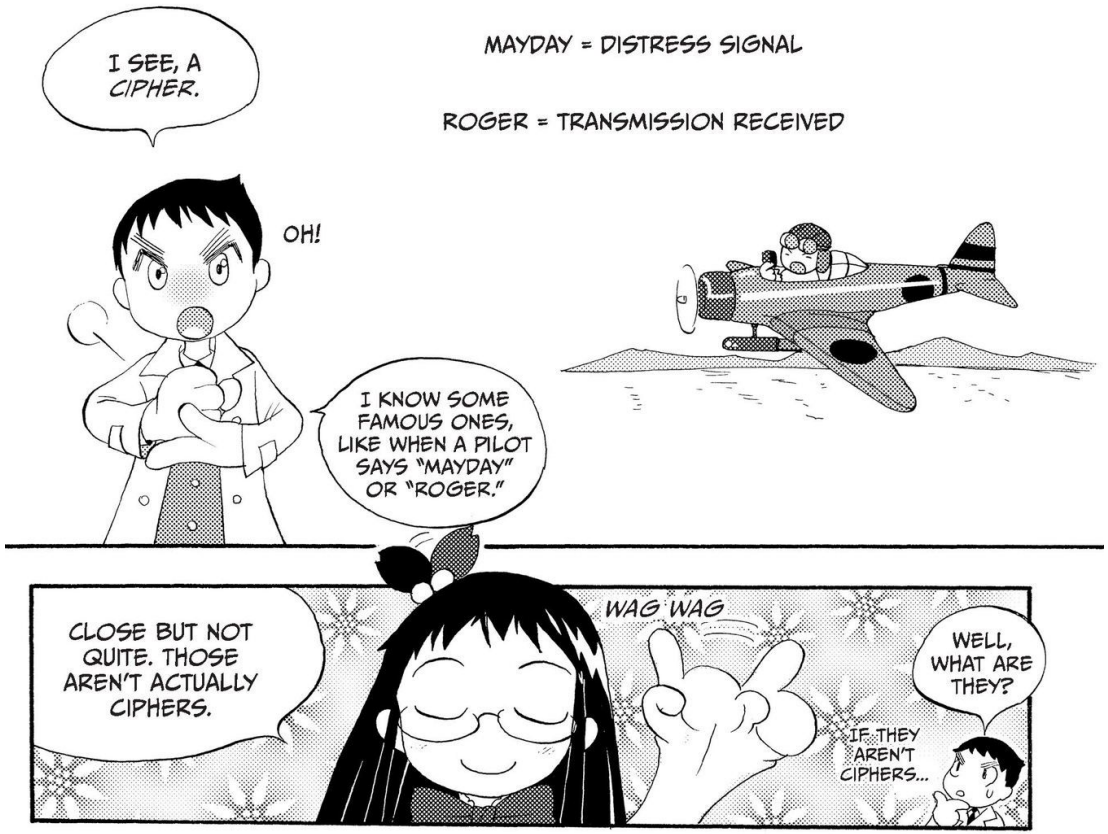
Conjunto de algoritmos y técnicas de cifrado que utilizan una única clave de cifrado secreta, compartida entre los participantes de la comunicación cifrada.

Cifrado asimétrico

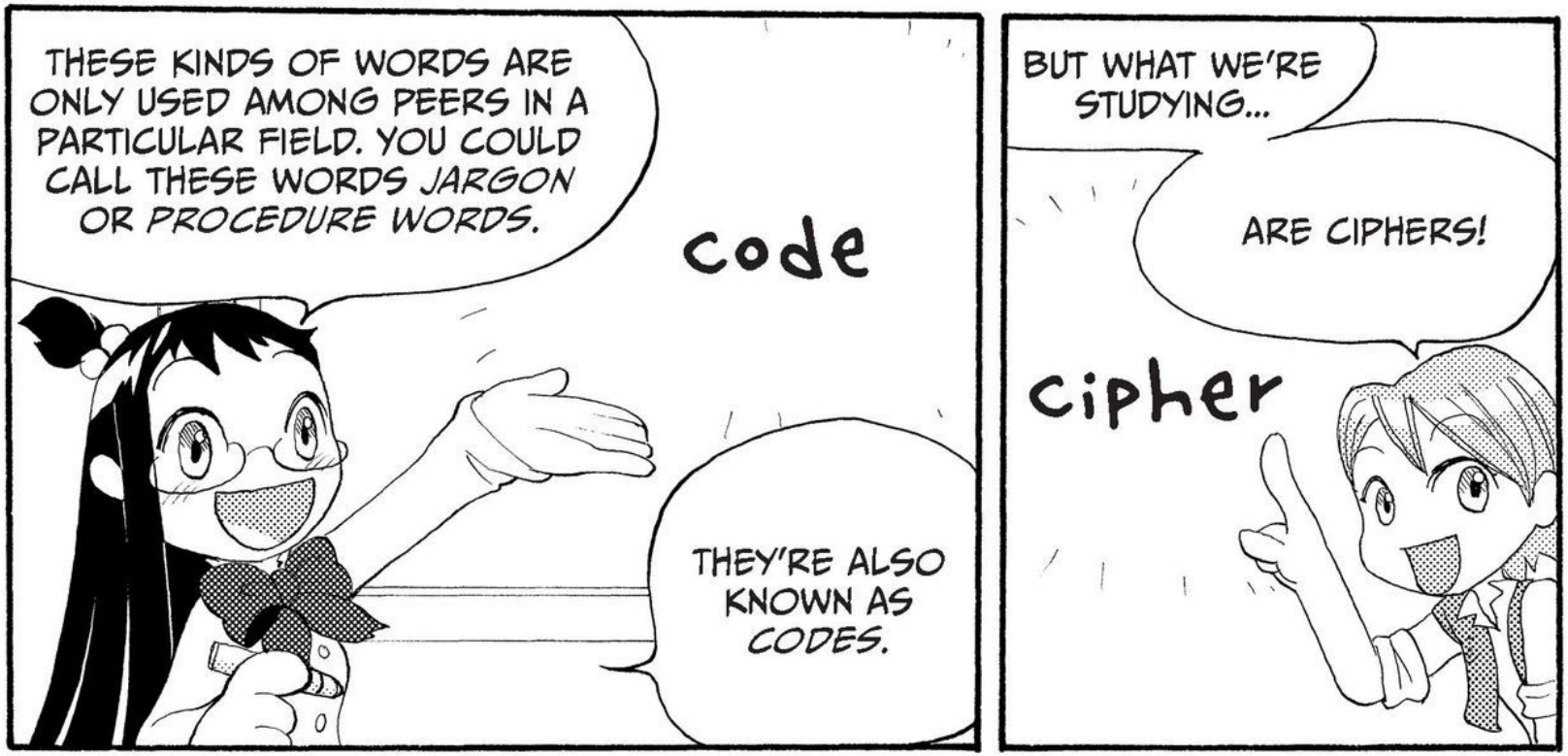
Conjunto de algoritmos y técnicas de cifrado que utiliza dos claves de cifrado, una secreta o privada conocida solo a su dueño, y otra publica conocida por todo el mundo.

Relación Entre Cifrado y Codificación

No es lo mismo un sistema de codificación que un criptosistema.

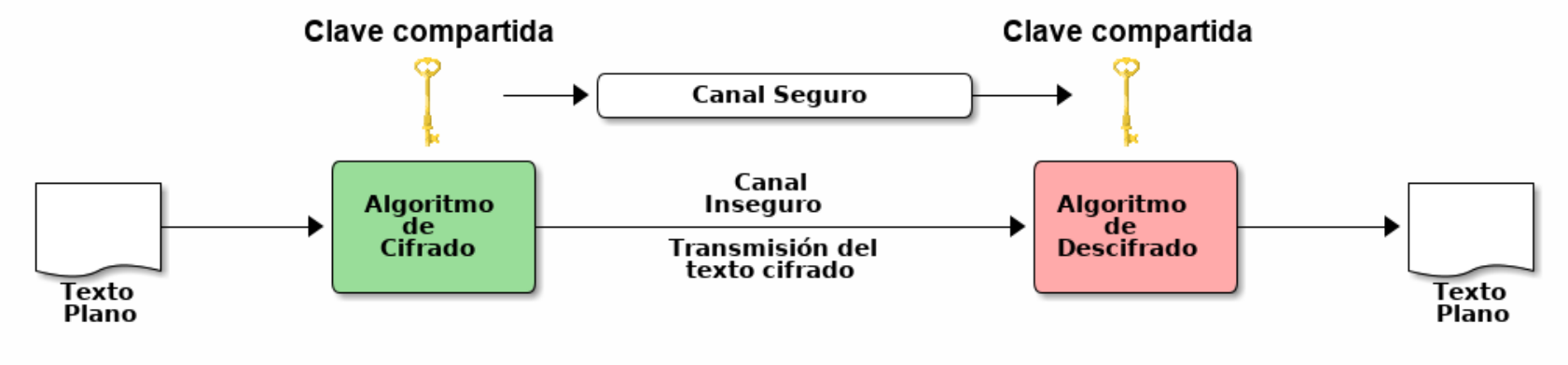


Codificación != Cifrado



Un Modelo Básico de Criptografía Simétrica

Un Modelo más Completo



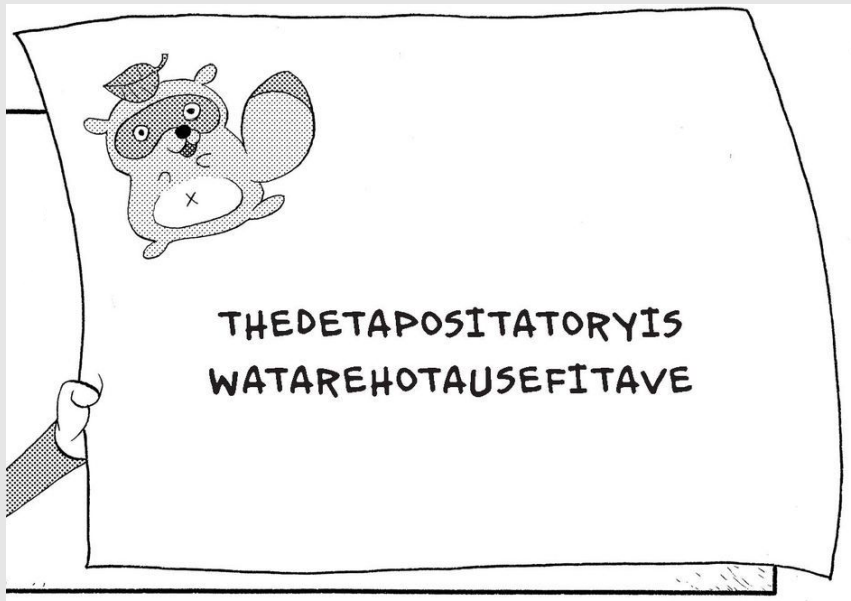
La Criptografía es Muy Antigua

Cifrados Elementales - Códigos

Latín Cerdo

1. Si la palabra empieza en consonante:
   - Mover todas las primeras consonantes al final de la palabra.
   - Agregar la sílaba “ay”.
2. Si la palabra empieza en vocal:
   - Agregar la sílaba “way” al final.

Cifrado Tanuki



Cifrado de Cesar

- Atribuido a Julio Cesar, quien lo usaba para su correspondencia privada.
- Consiste en desplazar cada letra del alfabeto 3 posiciones.

Cifrados de Rotación

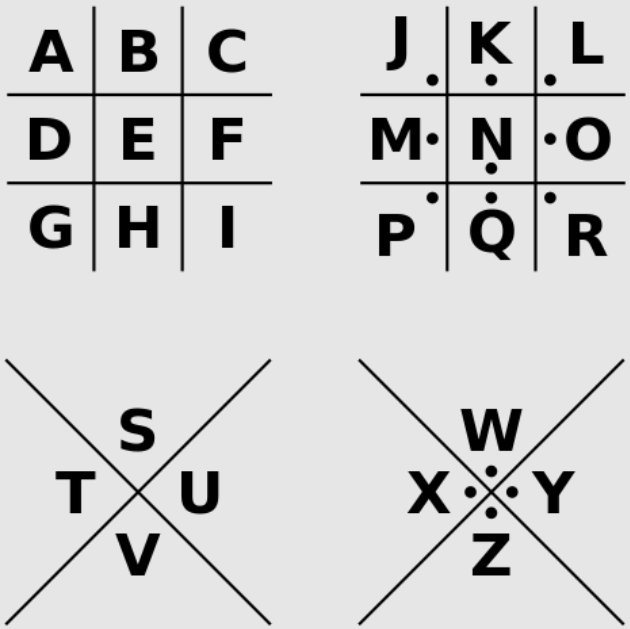
Rueda de Cifrado

Cifrado de Vigenère

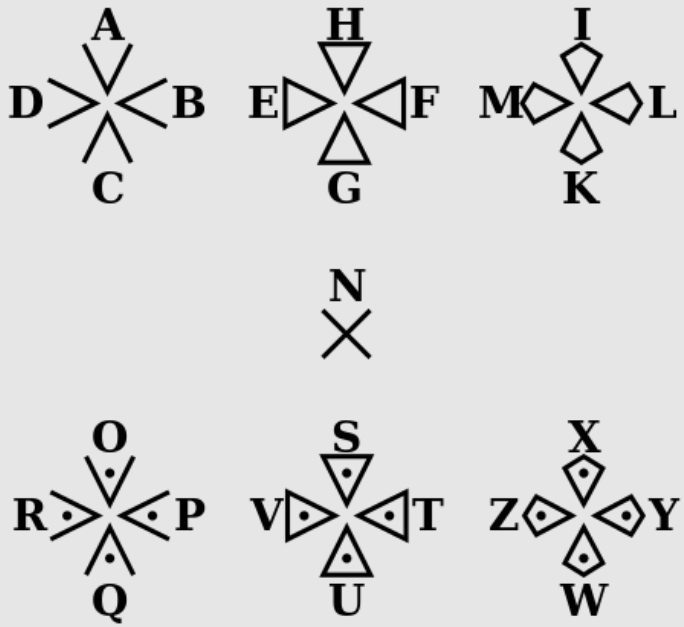
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	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
G	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Cifrados de Sustitución

Parque de cerdos



Cifrado Templario



Cifrados de Transposición

Texto plano:
Hola, Mundo!

H	a	M	d
o	,	u	o
l		n	!

Texto cifrado:
HaMdo,uol n!

La Escítala

Cifrados Mecánicos

- Basados en máquinas electro-mecánicas con engranajes.
- Muy utilizados en la primera y segunda Guerras Mundiales.
- El más famoso de todos es la máquina Enigma.

Cifrado de Vernam

- Inventado en 1919 por Gilbert Vernam.
- Cifrado de flujo, basado en suma modular.
- Puede aplicarse manualmente o mediante máquinas.
- Trabaja sobre flujos de símbolos o bits.

Extensión a Libretas de Un Solo Uso

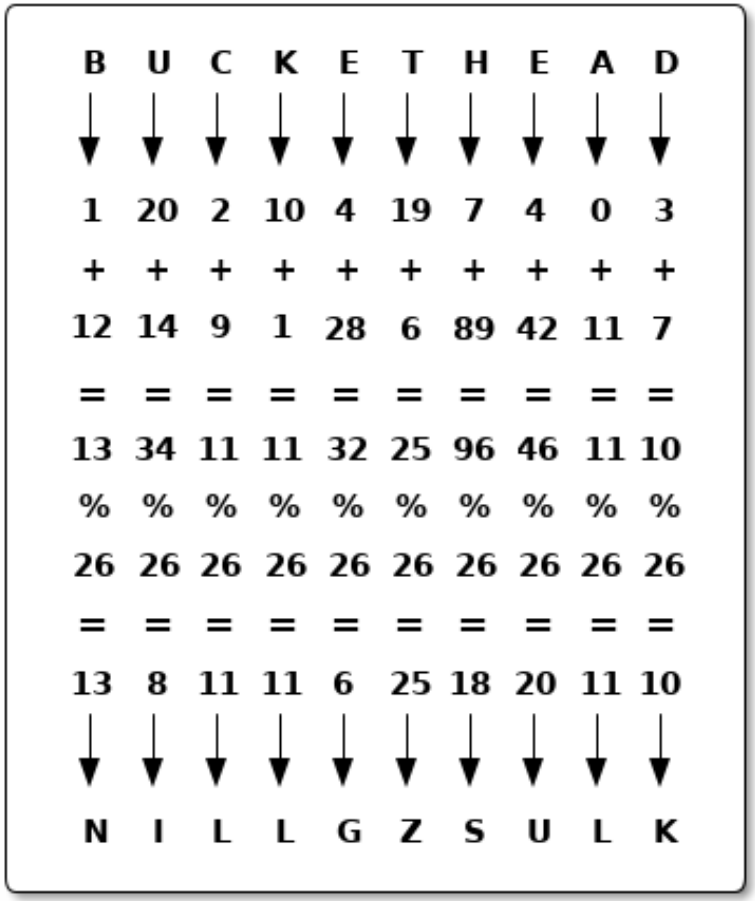
- Inventada en 1919 por Joseph Mauborgne.
- Usar una clave aleatoria de *la* misma longitud que el mensaje.
- Descartar cada ***clave*** después de ser usada.
- Siguiendo estas reglas este método de cifrado ***es*** irrompible.

Communication Theory of Secrecy Systems

CLAUDE SHANNON (1916–2001) WAS A 20TH-CENTURY ENGLISH MATHEMATICIAN WHO CAME TO BE KNOWN AS THE FATHER OF INFORMATION THEORY. IN 1948, HE WROTE AN ARTICLE ENTITLED "A MATHEMATICAL THEORY OF COMMUNICATION" IN WHICH HE COINED THE TERM *BIT* AND DEVELOPED SEVERAL CONCEPTS KEY TO CRYPTOGRAPHY.

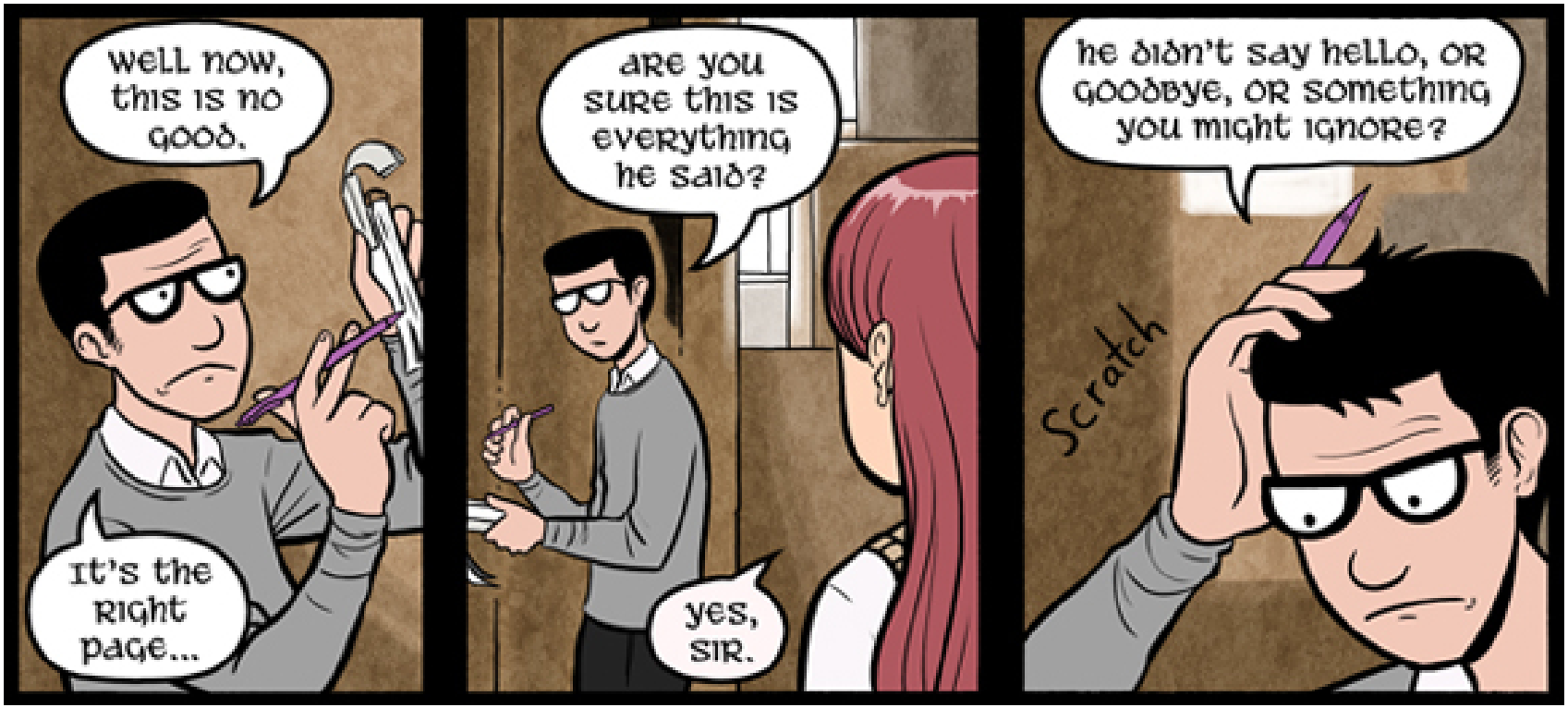
Ejemplo

Texto plano:
Buckethead



Texto cifrado:
Nillgzsulk

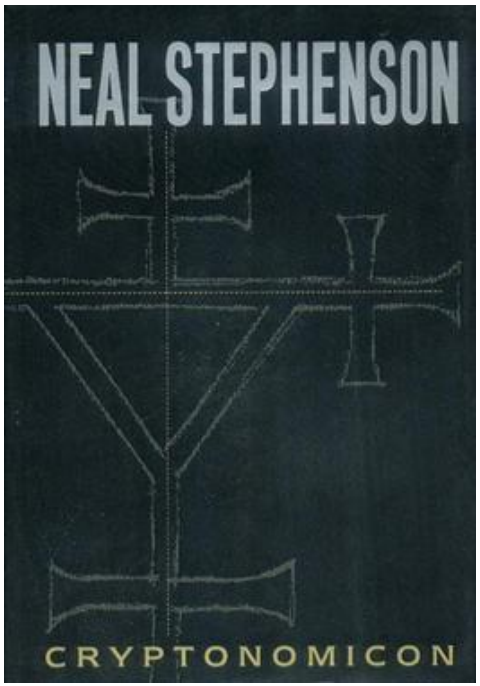
Los One-Time Pads son imprácticos

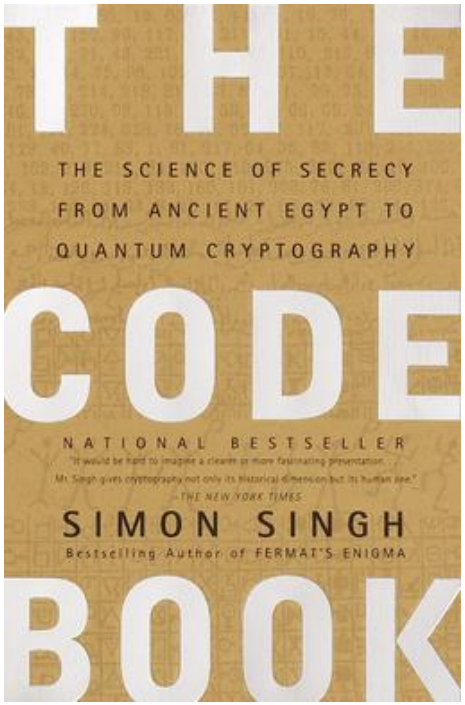


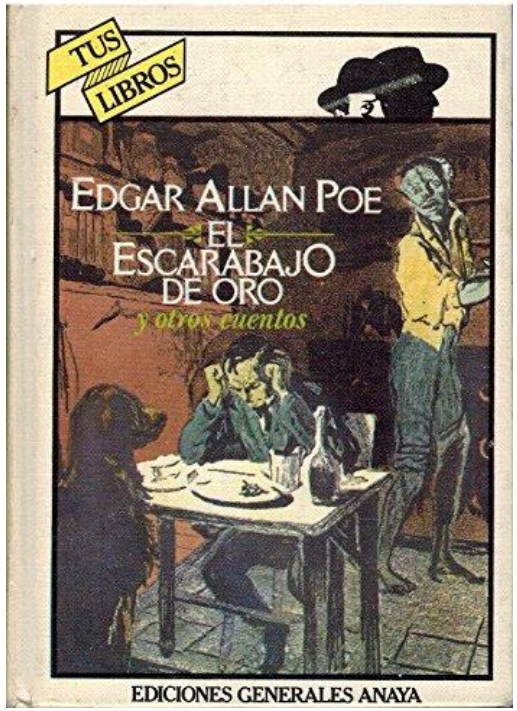
Conclusiones

- La criptografía es una herramienta muy antigua y aún es crucial para las comunicaciones modernas.
- Se pueden aplicar técnicas criptográficas facilmente con herramientas manuales.
- Es posible pero impráctico tener criptografía perfecta.
- ¡La criptografía clásica es divertida!

Bibliografía Recomendada







Próxima clase - 24/05/2019

- Cifrado de flujo
- Cifrado de Feistel
- Cifrado de Bloques
- Algoritmos DES y Triple DES
- Algoritmo AES

Tarea

Qrfpvsene ry fvthvragr zrafnwr pvsenqb pba ry nytbevgzb qr lvtraèer:

Grkgb pvsenqb

Zh kbijuurho apovg yj euuhaxiry 20 ubboytp rr jibvszdo. . .

Ragertnoyrf

Erqnpgne ha vasbezr qr n yb fhzb 1 cntvan qbaqr qrfpevon ry cebprqvzvragb dhr fvthvb cnen qrfpvsene ry zrafnwr. Vapyhln phnydhvre pbqvtb shragr qrfneebyynqb cnen ernyvmne rfgn npgvivqnq pbzb ha narkb n fh vasbezr.

¿Preguntas?