



PONTIFICIA
UNIVERSIDAD
CATÓLICA
DE CHILE

IIC3103

Taller de Integración

Profesor

Arturo Tagle / Daniel Darritchon

Arquitectura de Sistemas

1. El nivel más alto de descomposición de un sistema en sus partes
2. Las decisiones que son difíciles de cambiar
3. Problemas de los sistemas existentes
 - Sistemas legados
 - Heterogeneidad
 - Complejidad
 - Lock-in



Seguridad

Principios de seguridad de
sistemas y criptografía

Air Europa sufre un ciberataque que expone los datos bancarios de sus clientes

La aerolínea ha explicado que el jaqueo ha afectado al sistema de pagos online y que habría permitido a los ciberdelicuentes extraer los datos de las tarjetas de crédito de los clientes. Así, recomienda cancelar dichas tarjetas y denunciar cualquier uso fraudulento.



DELITOS INFORMÁTICOS >

El banco chino ICBC sufre un ciberataque a sus servicios financieros en Estados Unidos

Se realizó a través del método 'ransomware', que consiste en el secuestro de datos mediante el cifrado de los mismos, y a cambio se pide un rescate para recuperar la clave




<https://elpais.com/economia/2023-11-10/el-banco-chino-icbc-sufre-un-ciberataque-a-sus-servicios-financieros-en-estados-unidos.html>

Chile fue el objetivo de más de 4 mil millones de intentos de ciberataques en el primer semestre de 2023

Archivado en: Tecnología · Fortinet

Estrategia On line | Jueves, 24 de agosto de 2023, 05:13

 Compartir 0

 Twittear

Fortinet® (NASDAQ: FTNT), el líder global impulsando la convergencia de redes y seguridad, anunció hoy el último informe semestral sobre el Panorama Global de Amenazas de FortiGuard Labs. De acuerdo con el reporte de la organización de investigación e inteligencia de amenazas de Fortinet, Chile fue el objetivo de más de 4.000 millones de intentos de ciberataques en el primer semestre de 2023, ubicándose en el quinto lugar a nivel regional. Por su parte, América Latina y el Caribe sufrieron más de 63 mil millones de intentos de ciberataques en el primer semestre de 2023, Brasil recibió la mayor cantidad de intentos de ataques (23 mil millones), seguido por México (14 mil millones), Venezuela (10 mil millones), Colombia (5 mil millones) y Chile (4 mil millones).



18 octubre, 2023

Ciberataque expone información de 10 millones de chilenos en foros de hackers

Por: El Mostrador



Cuatro grupos de ciberdelincuentes han expuesto los datos de 10 millones de chilenos en foros de hackers, incluyendo nombres, RUT, sexo y nacionalidad. Aunque el CSIRT del Ministerio del Interior no ha activado alarmas, un experto en ciberseguridad advierte sobre riesgo de estafas y suplantación de identidad.



Al menos cuatro grupos de atacantes informáticos, identificados como amenazas cibernéticas, han expuesto los datos de 10 millones de chilenos en foros frecuentados por *hackers*. Nombres, RUT, sexo y nacionalidad son parte

Hacker Breaches Dropbox Sign Database, Views Customer Data

Story by Kate Irwin • 6h • ⌚ 2 min read



An unknown cyberattacker has infiltrated the Dropbox Sign e-signature platform in a breach that puts users' information at risk.

"A third party gained access to a Dropbox Sign automated system configuration tool," Dropbox said in a [blog post](#) this week. "The actor compromised a service account that was part of Sign's back-end, which is a type of non-human account used to execute applications and run automated services. As such, this account had privileges to take a variety of actions within Sign's production environment."



CSIRT

Equipo de Respuesta
ante Incidentes de
Seguridad Informática

 Reportar Incidente

Quiénes somos ▾


Alertas

Servicios

Blog Técnico

Documentos

Muro de la Fama

 [CSIRT de Gobierno](#) / [Alertas](#)

Alertas

 ▾

Alerta de Malware



3 de mayo de 2024 a las 12:21

DHL - Suplantación con malware

CMV24-00461

Alerta de Vulnerabilidad



2 de mayo de 2024 a las 16:10

ArubaOS - Vulnerabilidades

VSA24-01011

Alerta de Vulnerabilidad



2 de mayo de 2024 a las 15:12

Google Chrome - Vulnerabilidades

VSA24-01010

Alerta de Falsificación



Alerta de Phishing

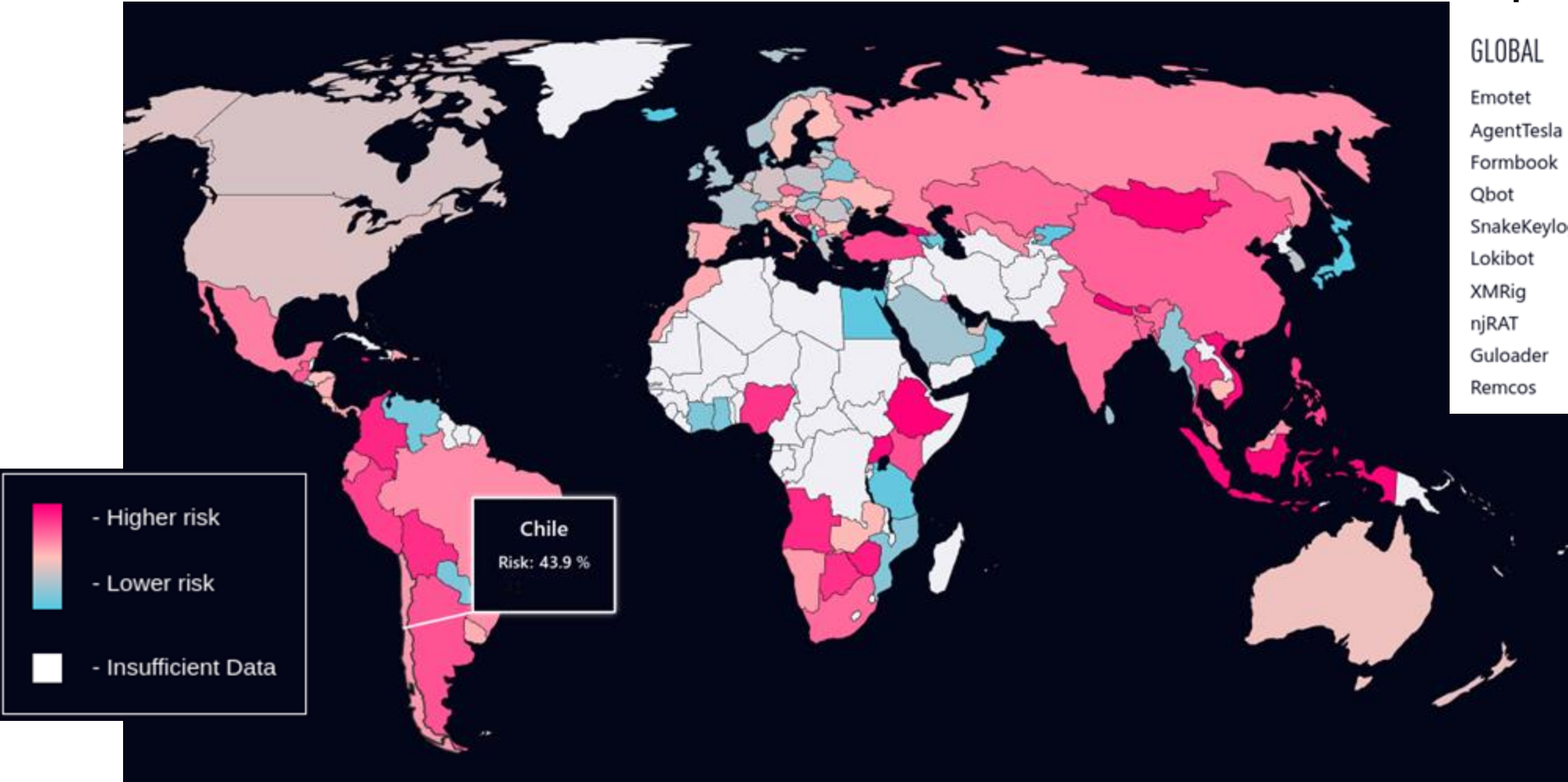


Alerta de Malware



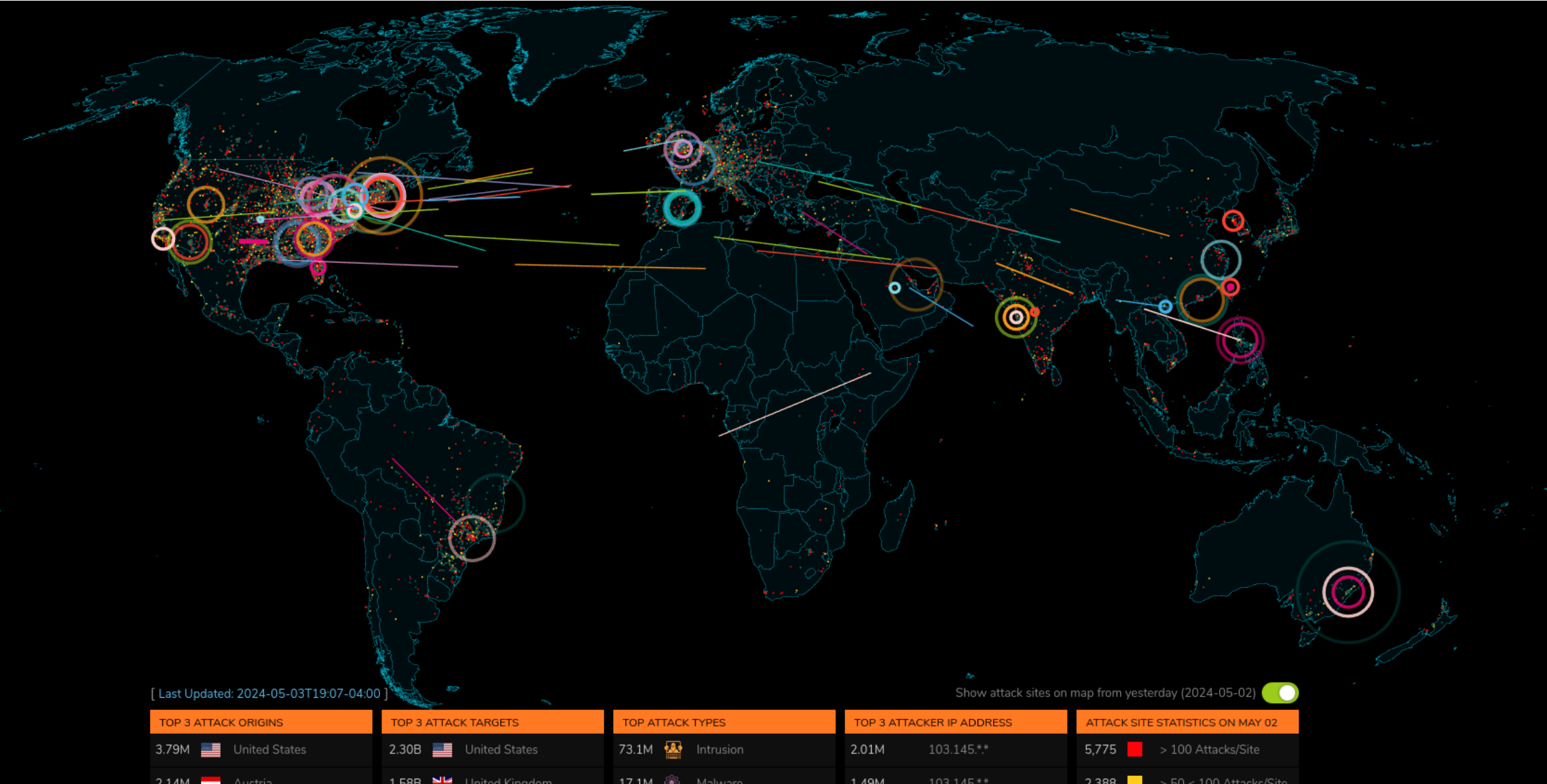
GLOBAL THREAT INDEX MAP

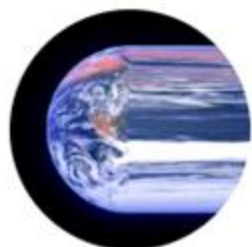
The map displays the cyber threat risk index globally, demonstrating the main risk areas around the world.*



Top Malware Families

World Wide Attacks





Disrupt ✓

@DisruptReality 1.44 M de suscriptores 212 videos

Bringing you the highest-quality content we can >



The hacker that lost control [Chatbots] Part 1

85 k vistas • hace 2 semanas



STUXNET: The World's First Digital Weapon

171 k vistas • hace 2 meses



BONZIBUDDY: Earth's Friendliest [Computer] Virus

292 k vistas • hace 8 meses



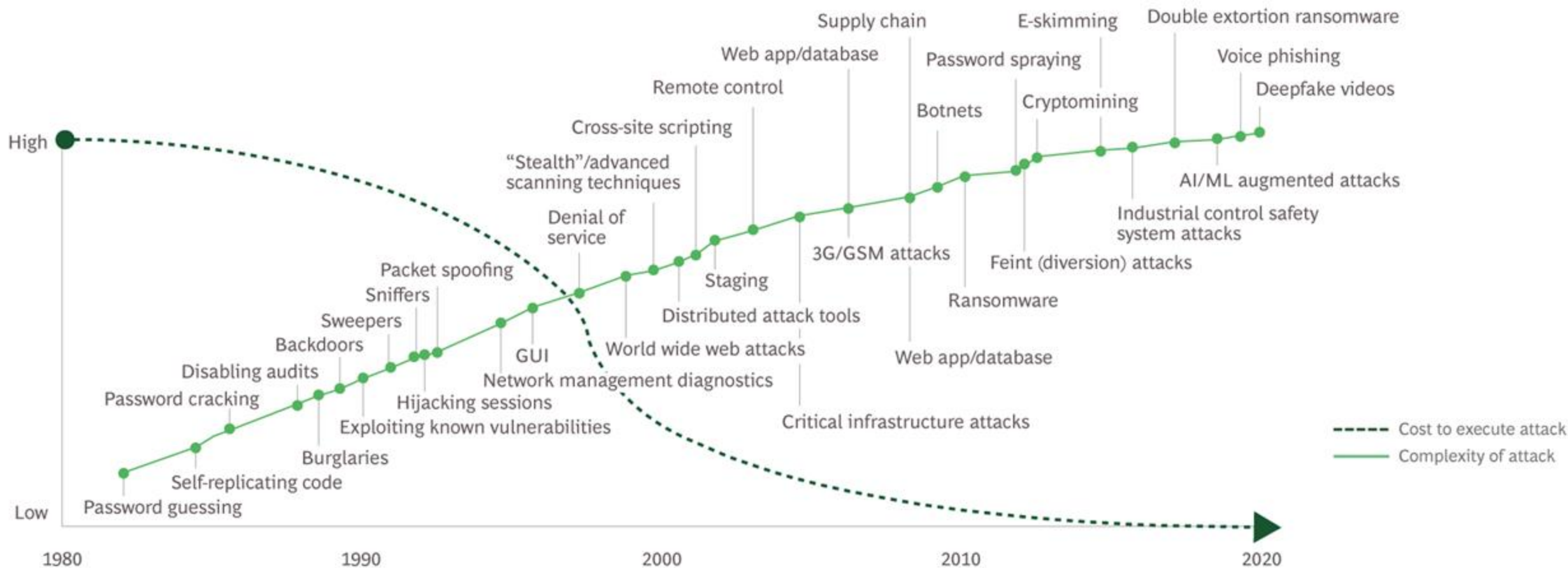
This guy stole 170,000,000 credit cards

705 k vistas • hace 10 meses

Y así, muchos otros casos...

Robo de claves de bancos a través de portales de phishing, exposición de fotos privadas, extorsión, hackeos de bancos para transferir fondos, malware para destruir máquinas de enriquecimiento de uranio en Irán, etc.

Cyber Attack Complexity Increases as Difficulties and Cost to Break-In Decreases



Hacking Email and Social Media Accounts

	Recent Prices
Popular U.S. Email Accounts (Gmail, Hotmail, Yahoo)	\$129
Popular Russian Email Accounts (Mail.ru, Yandex.ru, and Rambler.ru)	\$65 – \$103
Popular Ukrainian Email Accounts (Ukr.net)	\$129
Popular U.S. Social Media Accounts	\$129
Popular Russian Social Media Accounts (VK.ru and Ok.ru)	\$194
Corporate Email Accounts	\$500 per mailbox
IP address of Computer User	\$90

Tools

	Price in 2013	Price in 2014	Recent Prices
Remote Access Trojans (RATs)	\$50 – \$250	\$20 – \$50	\$5 – \$10
Crypters	N/A	\$50 – \$150	\$80 – \$440
Angler Exploit Kit			\$100 – \$135



Resumen

Seguridad

1. Seguridad de la información
2. Algoritmos de Hash
 - Usos prácticos
3. Algoritmos de encriptación
 - Historia
 - Criptografía Simétrica
 - Criptografía Asimétrica
 - Algoritmo RSA
4. Prevenciones
 - Ethical Hacking
 - OWASP

Seguridad de la información

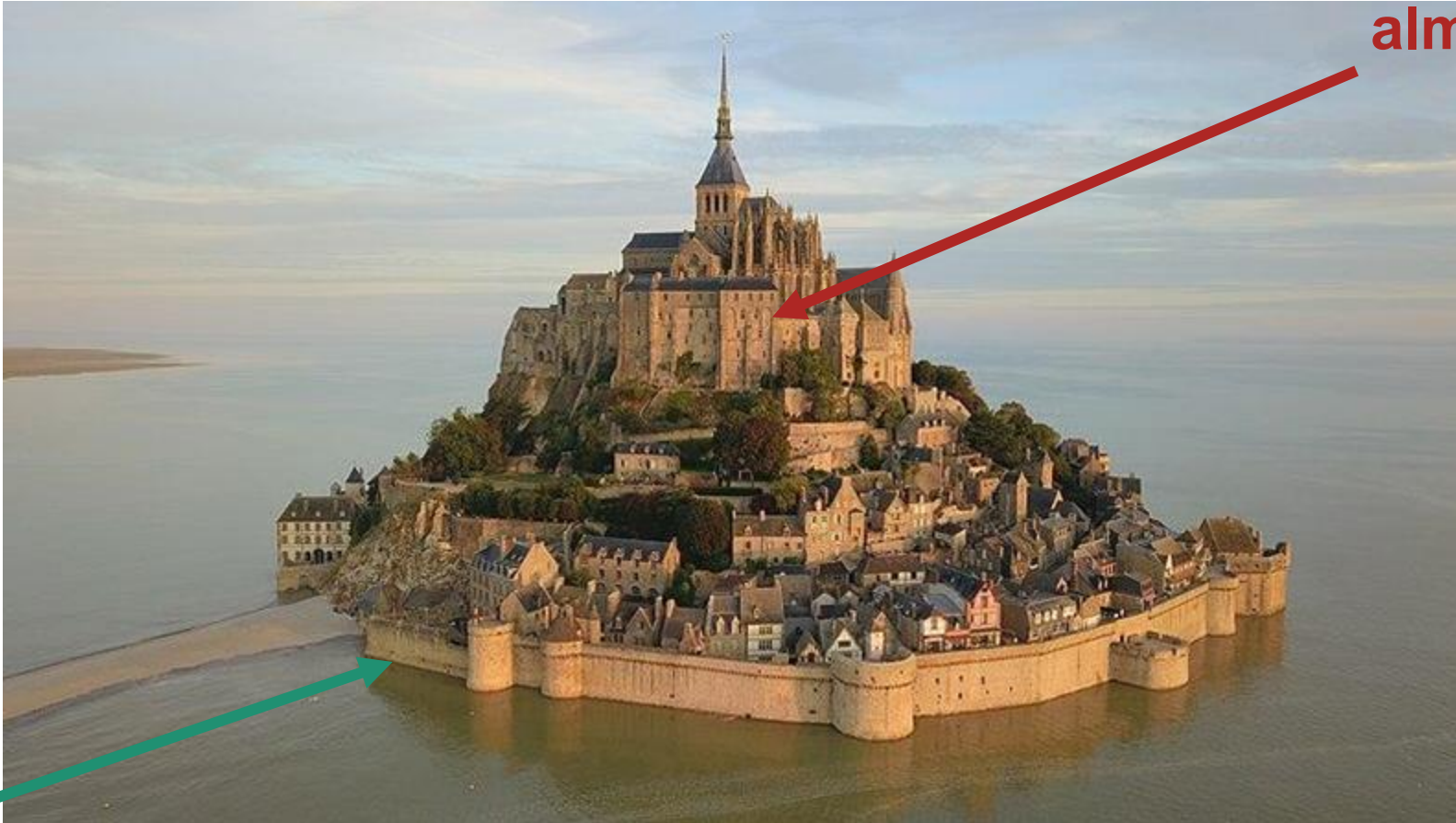
Plan de alto nivel

¿Cómo armar este plan?

- Política: El objetivo que se quiere lograr.
 - Objetivos comunes:
 - Confidencialidad
 - Integridad
 - Disponibilidad
- Modelos de riesgo: Supuestos que se pueden realizar.
 - ¿El atacante puede físicamente robar el servidor?
 - ¿Nos podrían hacer un ataque DDOS?
 - Mejor asumir de más que de menos
- Mecanismos: Como proveeremos la seguridad
 - Encriptación
 - Permisos de archivos
 - Passwords
 - 2/3/N FA



3 aristas de defensa



**Seguridad
almacenamiento
("at rest".)**

**Seguridad
perimetral**



**Seguridad en
tránsito
(“*in transit*”)**

Seguridad es una meta “negativa”

El objetivo es lograr que algo no se pueda realizar

Seguridad: Meta negativa 🚩

- Se debe garantizar la política propuesta y prevenir acciones no autorizadas.
- Es muy difícil pensar en todas las maneras que podemos ser atacados
 - Es mucho más fácil probar que un usuario tiene acceso a un archivo a que otro usuario no tiene acceso
 - Probar la seguridad es como demostrar que una especie está extinta: que nadie haya visto un Tigre de Tasmania en 80 años no significa que esté extinto.
- El link más débil es el que más importa
- Siempre debe ser un proceso iterativo



BENEFIT

RISK



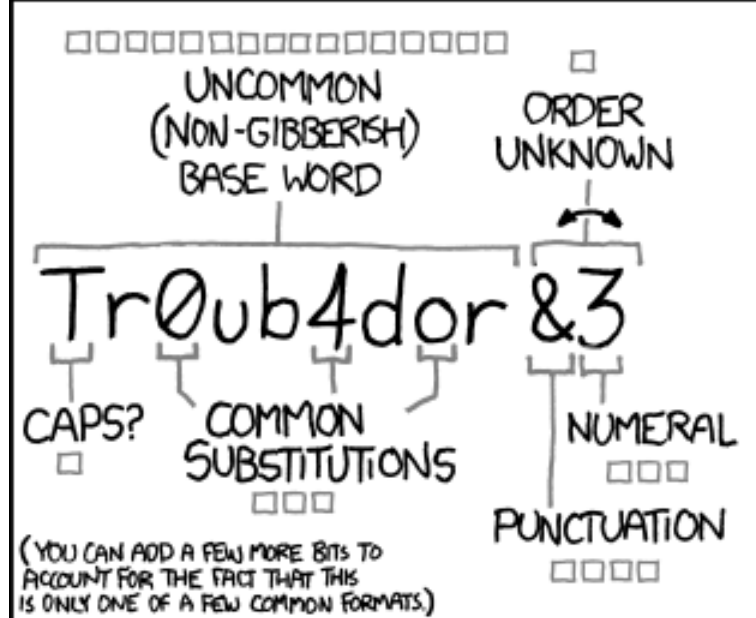
No existe seguridad perfecta

- Trade-off riesgo versus beneficio
 - Sistemas más seguros tienen menor riesgo, pero son más difíciles y más costosos de construir.
- Cada sistema siempre tendrá un punto donde podrá quebrarse
 - Esto no significa que el sistema no sirva: siempre dependerá del contexto.

Distintos problemas de seguridad

- Problemas con política/cultura
 - Reset de claves poco seguros
 - Envío de archivos sensibles
 - Importancia no concientizada
- Modelos de Riesgo
 - Brute force password guessing
 - Vulnerabilidades en código / dependencias
 - Archivos sin control de acceso
 - Mails de phishing
- Mecanismos
 - Engaño a colaboradores
 - Algoritmos poco seguros
 - Datos en memoria

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	instant	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years



~28 BITS OF ENTROPY

□□□□□□□□
□□□□□□□□
□□□
□□□□


$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

(PLAUSIBLE ATTACK ON A WEAK REMOTE
WEB SERVICE. YES, CRACKING A STOLEN
HASH IS FASTER, BUT IT'S NOT WHAT THE
AVERAGE USER SHOULD WORRY ABOUT.)

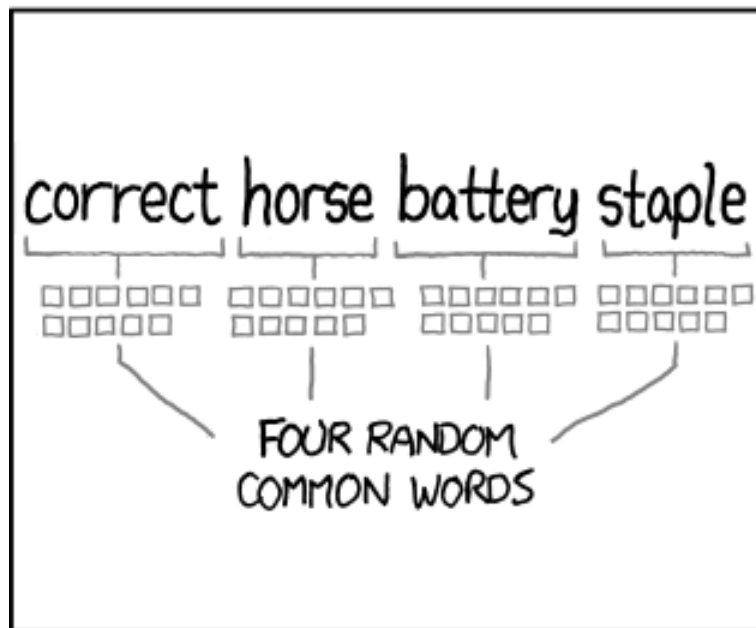
DIFFICULTY TO GUESS:
EASY

WAS IT TROMBONE? NO,
TROUBADOR. AND ONE OF
THE 0s WAS A ZERO?

AND THERE WAS
SOME SYMBOL...



DIFFICULTY TO REMEMBER:
HARD



~44 BITS OF ENTROPY

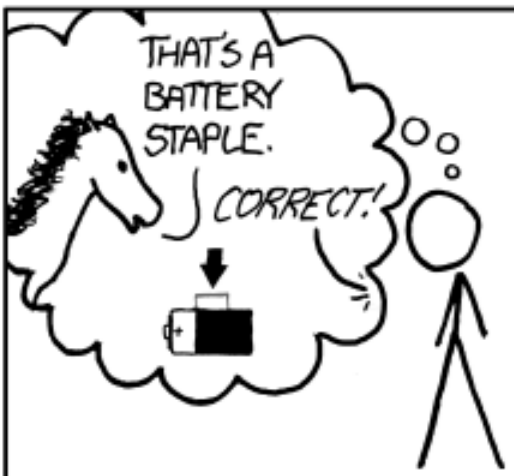
□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS:
HARD

THAT'S A
BATTERY
STAPLE.

CORRECT!



DIFFICULTY TO REMEMBER:
YOU'VE ALREADY
MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED
EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS
TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

MULTI-FACTOR AUTHENTICATION

I WAS ABLE TO STEAL HIS PASSWORD . . .
NOW I'LL LOGIN AS HIM.



OH NO! HE HAS MULTI-FACTOR IDENTIFICATION
SETUP! I'LL TRY LOGGING IN ANYWAY. MAYBE HE
WILL APPROVE THE REQUEST.



WHAT'S THIS? I DIDN'T JUST TRY TO LOGIN.
I BETTER NOT APPROVE THIS REQUEST.



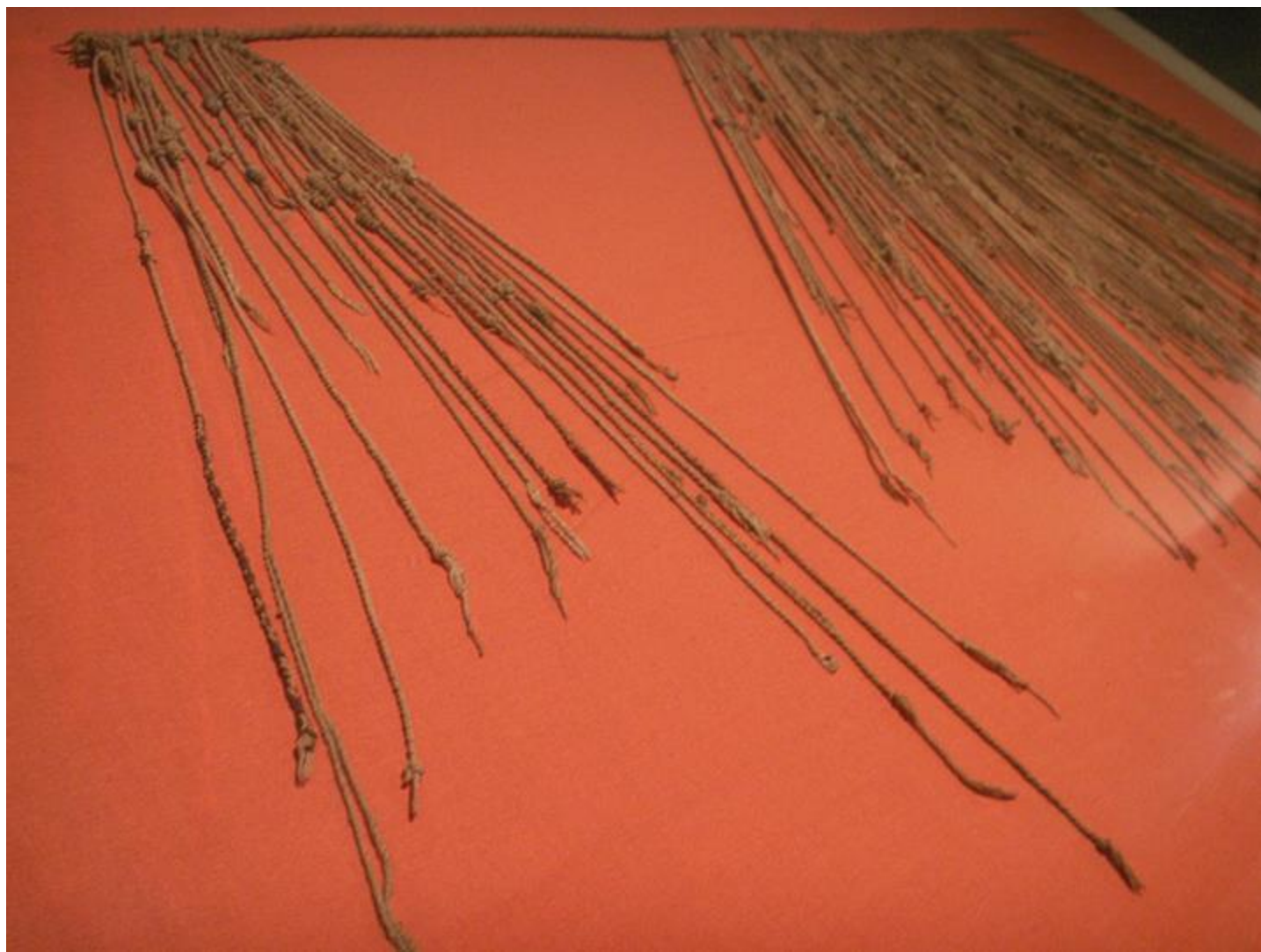
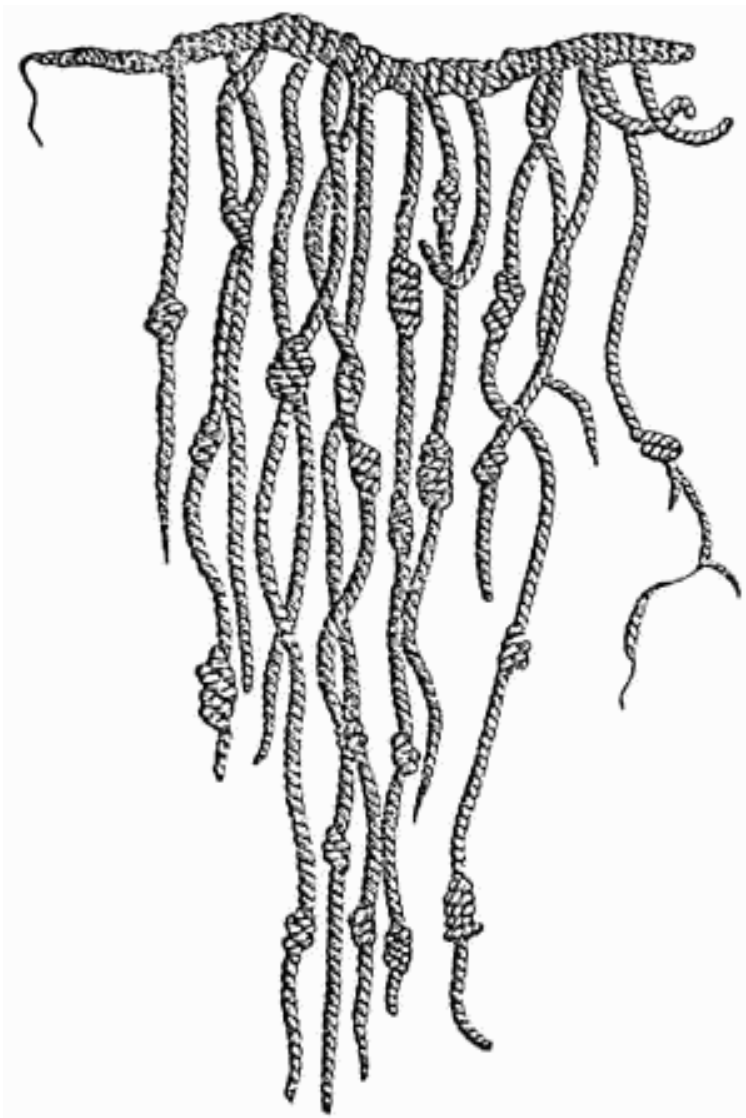
UGH! I HATE MULTI-FACTOR AUTHENTICATION.
HACKING IS SO MUCH HARDER NOW!!!



Principios de criptografía

Seguridad en tránsito y almacenamiento

Técnicas de cifrado o codificado destinadas a alterar un mensaje con el fin de hacerlo ininteligible a receptores no autorizados.



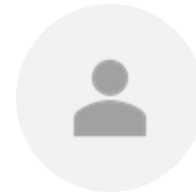
Objetivos



Confidencialidad



Integridad



Autenticación

¿Encriptación o
Hash?

Encryption & Decryption



Plain Text



Encryption



Encryption Text



Decryption



Plain Text

cheap\$\$L
SECURITY

Hashing Algorithm



Plain Text



Hash Function



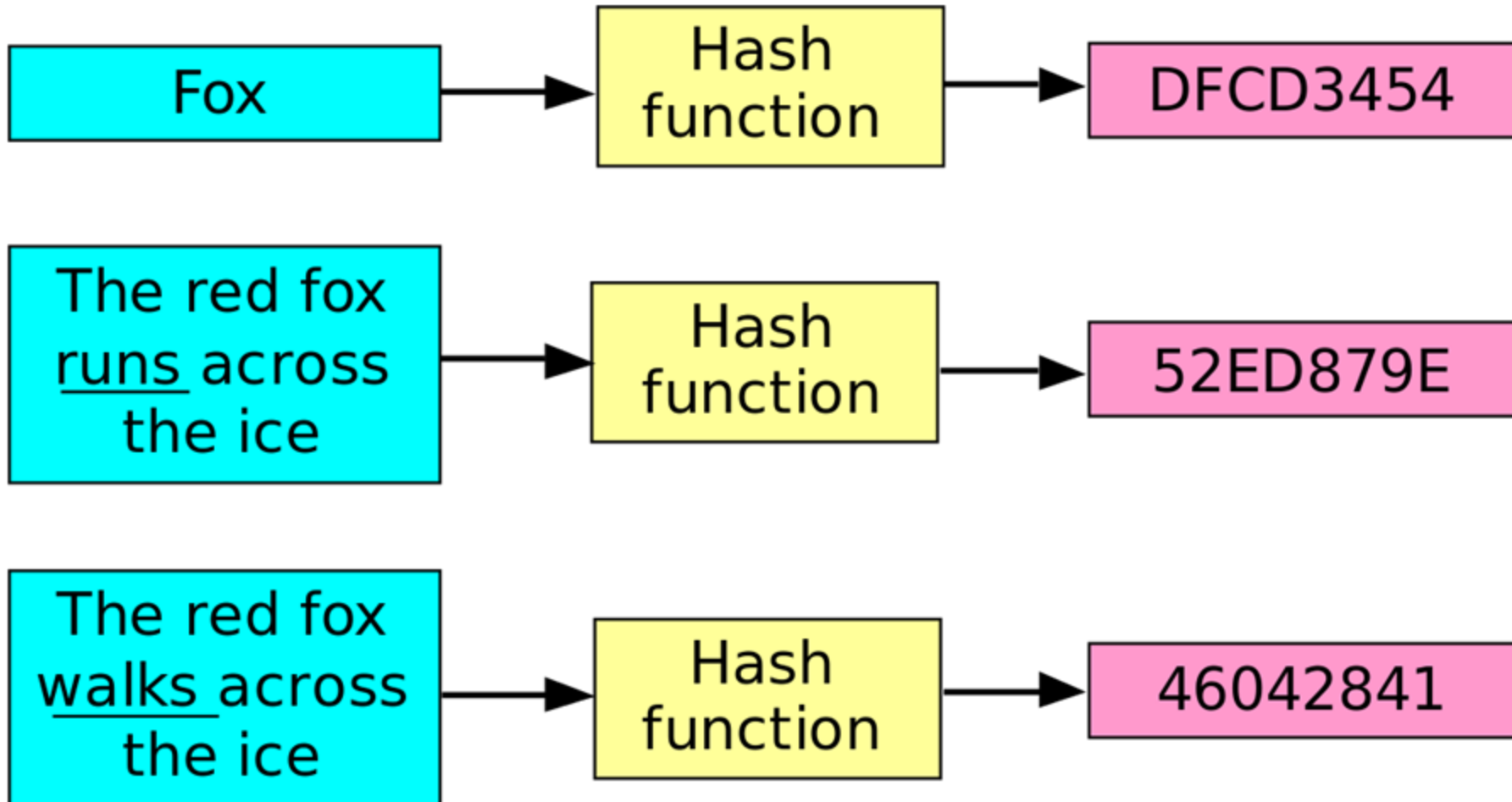
Hashed Text

cheap\$\$L
SECURITY

Algoritmos de hash

Input

Hash sum



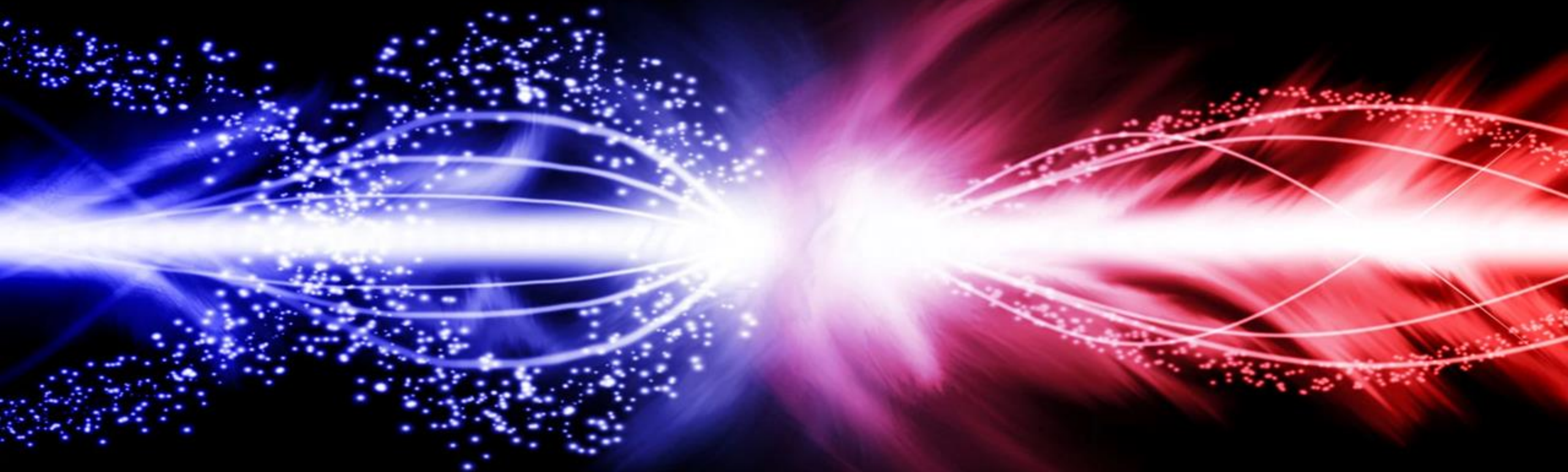
Funciones de hash

- Función que tiene como entrada un elemento, que lo convierte a un rango de salida finito, normalmente de longitud fija.
- Proyección de un conjunto U sobre un conjunto M .
- Destructivos / No reversibles

Propiedades

- Por lo general, las funciones de hash son:
 - De bajo costo de cómputo
 - Rápidos de calcular
 - Resultado más comprimido que original
 - Longitudes grandes a conjunto reducido
 - Probabilidad uniforme
 - Cada hash posible tiene una probabilidad uniforme
 - Determinista
 - Para cada x , siempre es el mismo y

Colisión de HASH



Algunas funciones de hash

MD5

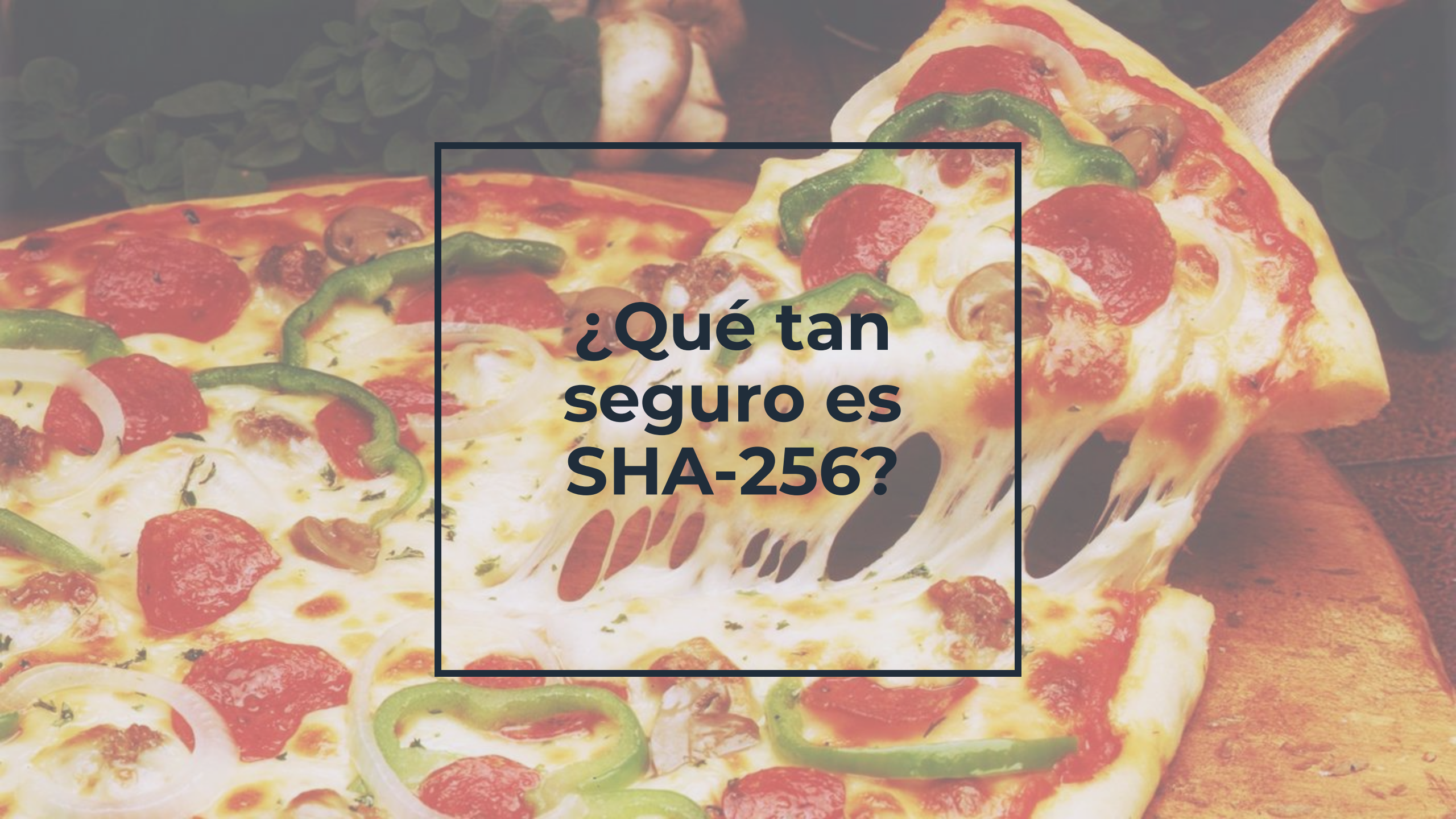
SHA1

SHA-
256

SHA-
512

HMAC

BLAKE
2



**¿Qué tan
seguro es
SHA-256?**

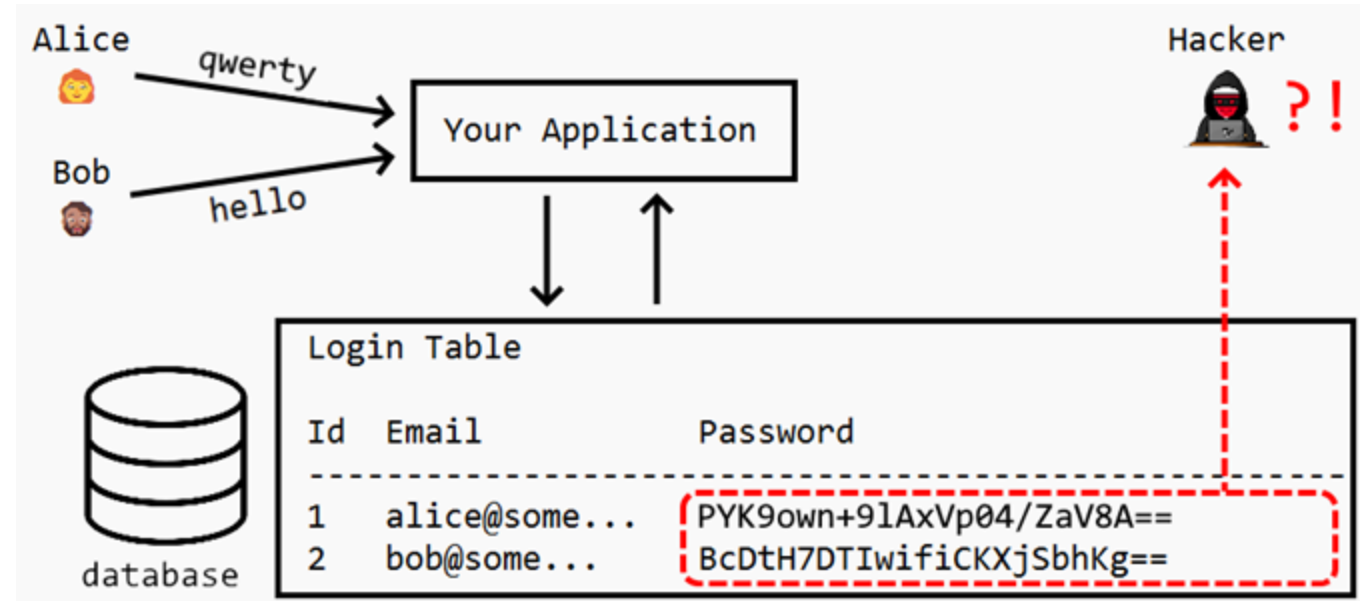
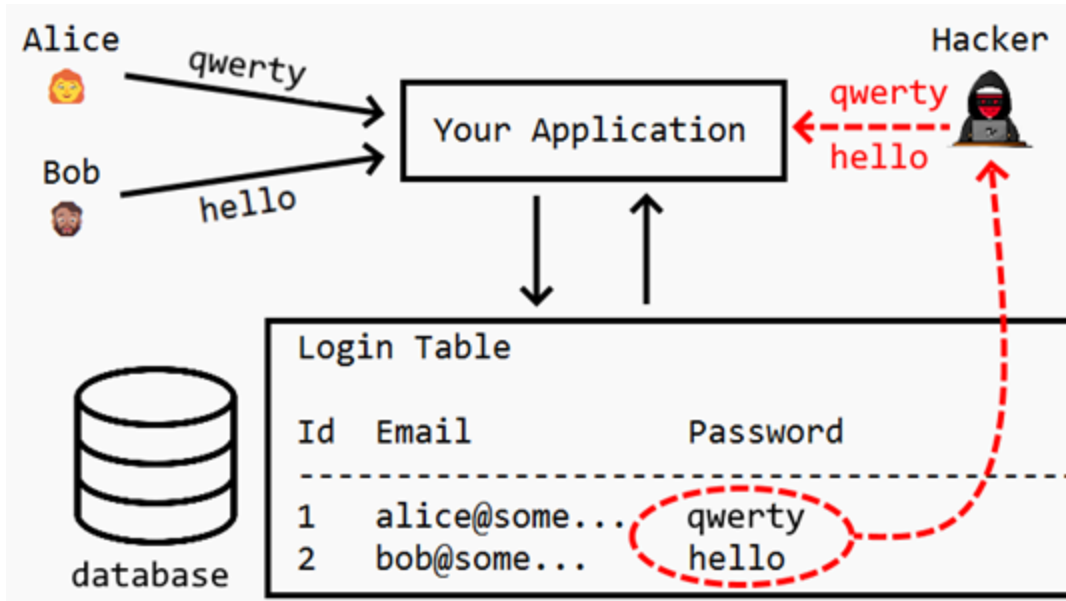
11579208922731619542
3570980078532
69984604039457
58400791329659936



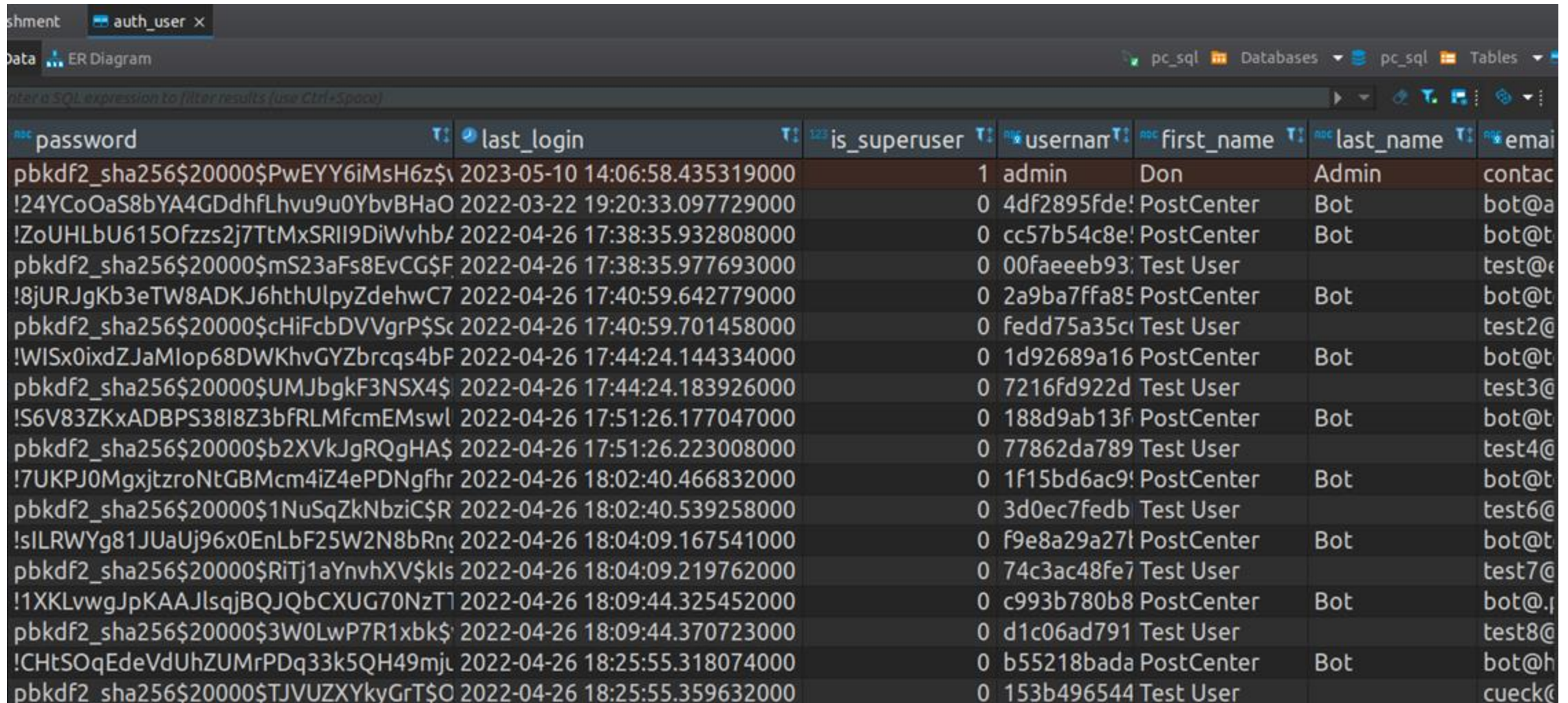
2256

Ver video en: https://www.youtube.com/watch?feature=oembed&v=S9JGmA5_unY

Hashing Aplicado: Guardado de contraseñas



Hashing Aplicado: Guardado de contraseñas

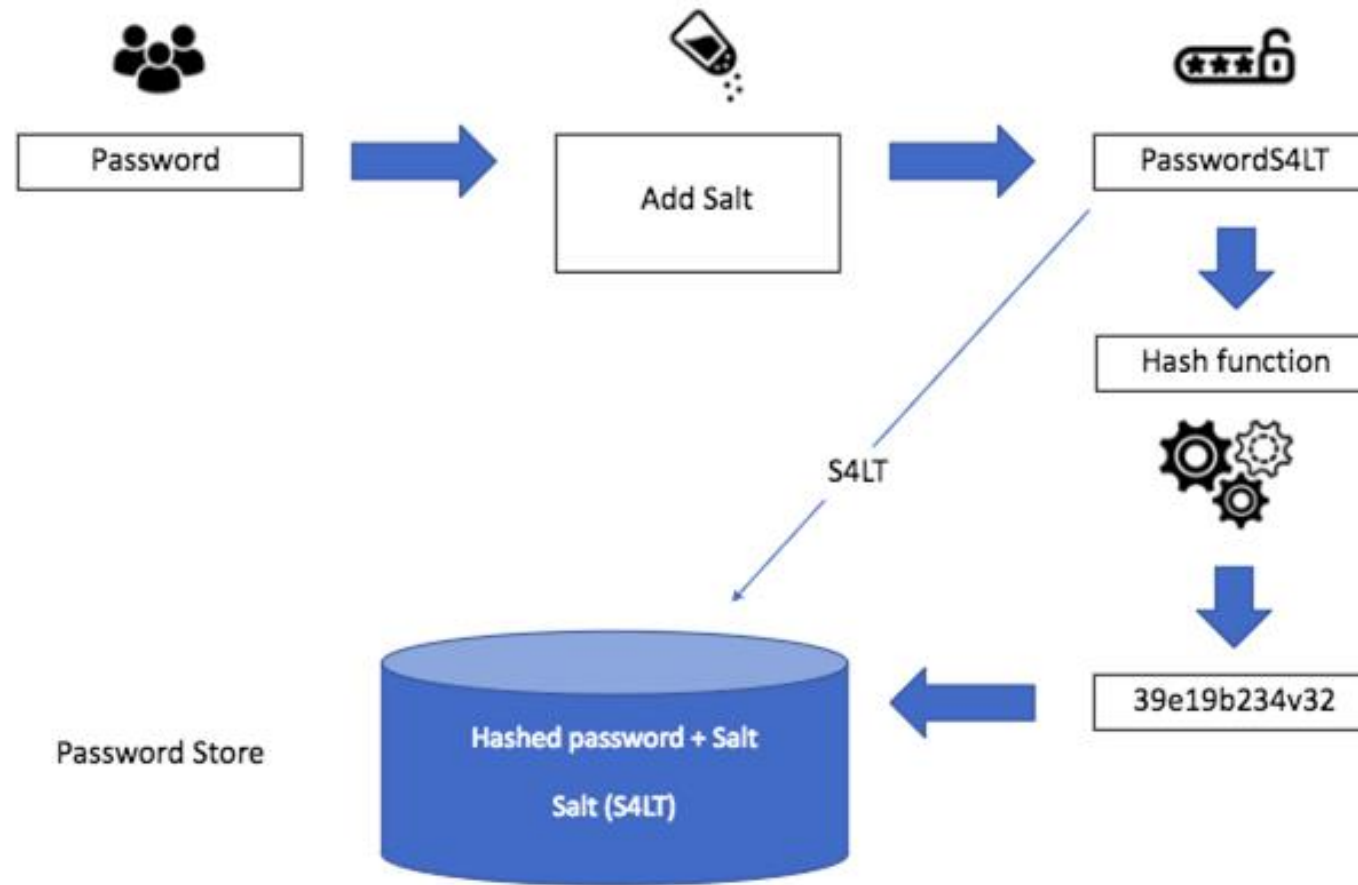


The screenshot shows a database management interface with a table named 'auth_user'. The table contains 15 rows of user data. The columns are: password, last_login, is_superuser, username, first_name, last_name, and email. The passwords are stored as PBKDF2-SHA256 hashes. The users include an admin, several bots, and test users.

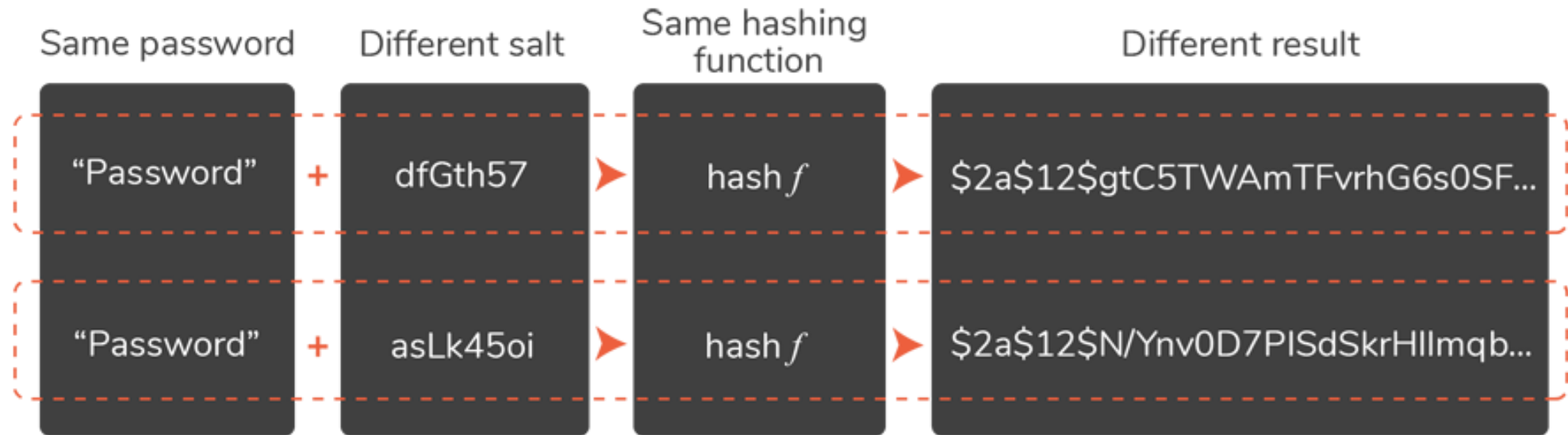
password	last_login	is_superuser	username	first_name	last_name	email
pbkdf2_sha256\$20000\$PwEYY6iMsH6z\$	2023-05-10 14:06:58.435319000	1	admin	Don	Admin	contac
!24YCoOaS8bYA4GDdhfLhvu9u0YbvBHao	2022-03-22 19:20:33.097729000	0	4df2895fde!	PostCenter	Bot	bot@a
!ZoUHLbU615Ofzsz2j7TtMxSRll9DiWvhb/	2022-04-26 17:38:35.932808000	0	cc57b54c8e!	PostCenter	Bot	bot@t
pbkdf2_sha256\$20000\$mS23aFs8EvCG\$F	2022-04-26 17:38:35.977693000	0	00faeeeb93!	Test User		test@e
!8jURJgKb3eTW8ADKJ6hthUlpyZdehwC7	2022-04-26 17:40:59.642779000	0	2a9ba7ffa85	PostCenter	Bot	bot@t
pbkdf2_sha256\$20000\$cHiFcbDVVgrP\$Sc	2022-04-26 17:40:59.701458000	0	fedd75a35ci	Test User		test2@
!WISx0ixdZJaMlop68DWKhvGYZbrcqs4bF	2022-04-26 17:44:24.144334000	0	1d92689a16	PostCenter	Bot	bot@t
pbkdf2_sha256\$20000\$UMJbgkF3NSX4\$	2022-04-26 17:44:24.183926000	0	7216fd922d	Test User		test3@
!S6V83ZKxADBPS38l8Z3bfRLMfcmEMswl	2022-04-26 17:51:26.177047000	0	188d9ab13f	PostCenter	Bot	bot@t
pbkdf2_sha256\$20000\$b2XVkJgRQgHAs	2022-04-26 17:51:26.223008000	0	77862da789	Test User		test4@
!7UKPJ0MgxjtzroNtGBMcm4iZ4ePDNgfhr	2022-04-26 18:02:40.466832000	0	1f15bd6ac9!	PostCenter	Bot	bot@t
pbkdf2_sha256\$20000\$1NuSqZkNbziC\$R	2022-04-26 18:02:40.539258000	0	3d0ec7fedb	Test User		test6@
!sILRWYg81JUaUj96x0EnLbF25W2N8bRnç	2022-04-26 18:04:09.167541000	0	f9e8a29a27l	PostCenter	Bot	bot@t
pbkdf2_sha256\$20000\$RiTj1aYnvhXV\$klS	2022-04-26 18:04:09.219762000	0	74c3ac48fe7	Test User		test7@
!1XKLvwgJpKAAJlsqJBQJQbCXUG70NzTl	2022-04-26 18:09:44.325452000	0	c993b780b8	PostCenter	Bot	bot@.j
pbkdf2_sha256\$20000\$3W0LwP7R1xbk\$	2022-04-26 18:09:44.370723000	0	d1c06ad791	Test User		test8@
!CHtSOqEdeVdUhZUMrPDq33k5QH49mjl	2022-04-26 18:25:55.318074000	0	b55218bada	PostCenter	Bot	bot@h
pbkdf2_sha256\$20000\$TJVUZXykyGrT\$O	2022-04-26 18:25:55.359632000	0	153b496544	Test User		cueck@

¿Qué pasa si 2 contraseñas tienen el mismo hash?

Añadir “sal” a las contraseñas



Añadir “sal” a las contraseñas



Añadir “sal” a las contraseñas

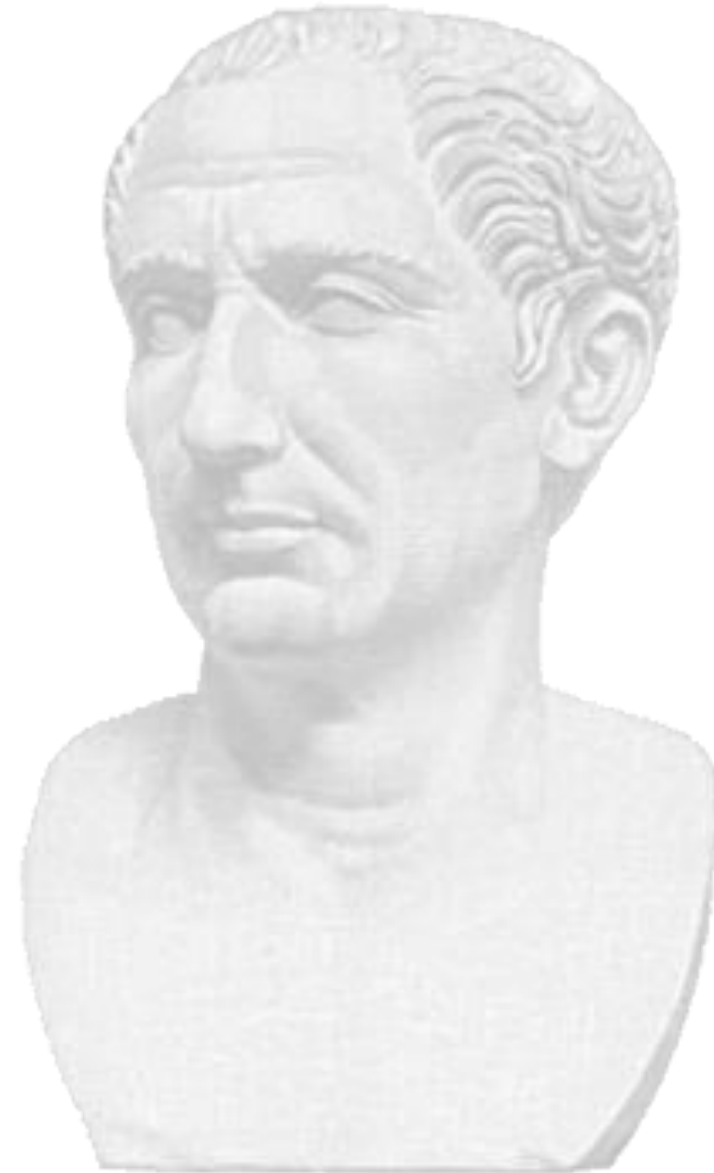
```
hashers.py ×
home > dedarritchon > .virtualenvs > pc > lib > python2.7 > site-packages > django > contrib > auth > hashers.py >

65
66 def make_password(password, salt=None, hasher='default'):
67     """
68     Turn a plain-text password into a hash for database storage
69     """
70     if password is None:
71         return UNUSABLE_PASSWORD_PREFIX + get_random_string(UNUSABLE_PASSWORD_SU
72     hasher = get_hasher(hasher)
73
74     if not salt:
75         salt = hasher.salt()
76
77     return hasher.encode(password, salt)
78
```

Algoritmos de encriptación

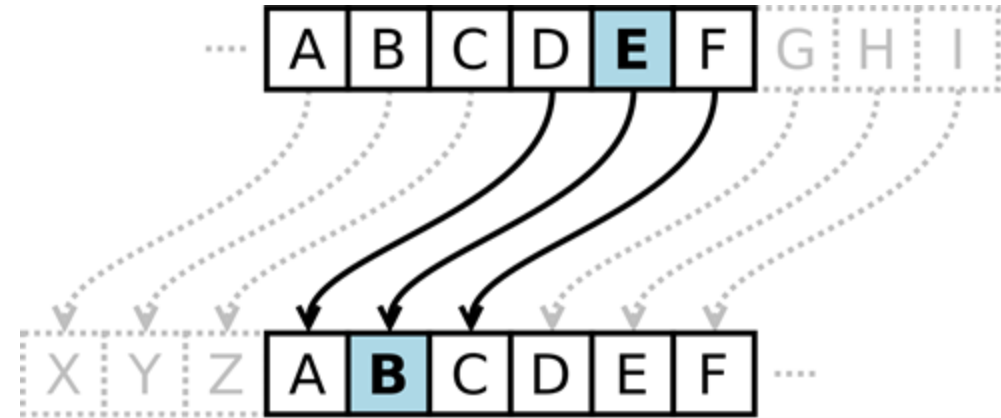
Cifrado del César

~50 dc



“...Si tenía que decir algo confidencial, lo escribía usando el cifrado, esto es, cambiando el orden de las letras del alfabeto, para que ni una palabra pudiera entenderse. Si alguien quiere decodificarlo, y entender su significado, debe sustituir la cuarta letra del alfabeto, es decir, la D por la A, y así con las demás.”

Suetonio, Vida de los doce Césares, 121 d.C.



Texto Plano: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Texto Cifrado: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

Cifrado de Vigenère

~1400



“El cifrado de Vigenère ganó una gran reputación por ser excepcionalmente robusto. Incluso el escritor y matemático Charles Lutwidge Dodgson (*Lewis Carroll*) dijo que el cifrado de Vigenère era irrompible en un artículo titulado "The Alphabet Cipher". En 1917, la revista *Scientific American* afirmó que el cifrado de Vigenère era imposible de romper.”

Texto Plano: P A R I S V A U T B I E N U N E M E S S E

Clave*: L O U P L O U P L O U P L O U P L O U P L

Texto Cifrado: A O M X D K U K E P C T X J H T W S N I O

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	Ñ	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	Ñ	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
Ñ	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
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	Ñ
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	Ñ	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y

Actividad

Premio al primer@ que
descifre la palabra:

XBMXRRN

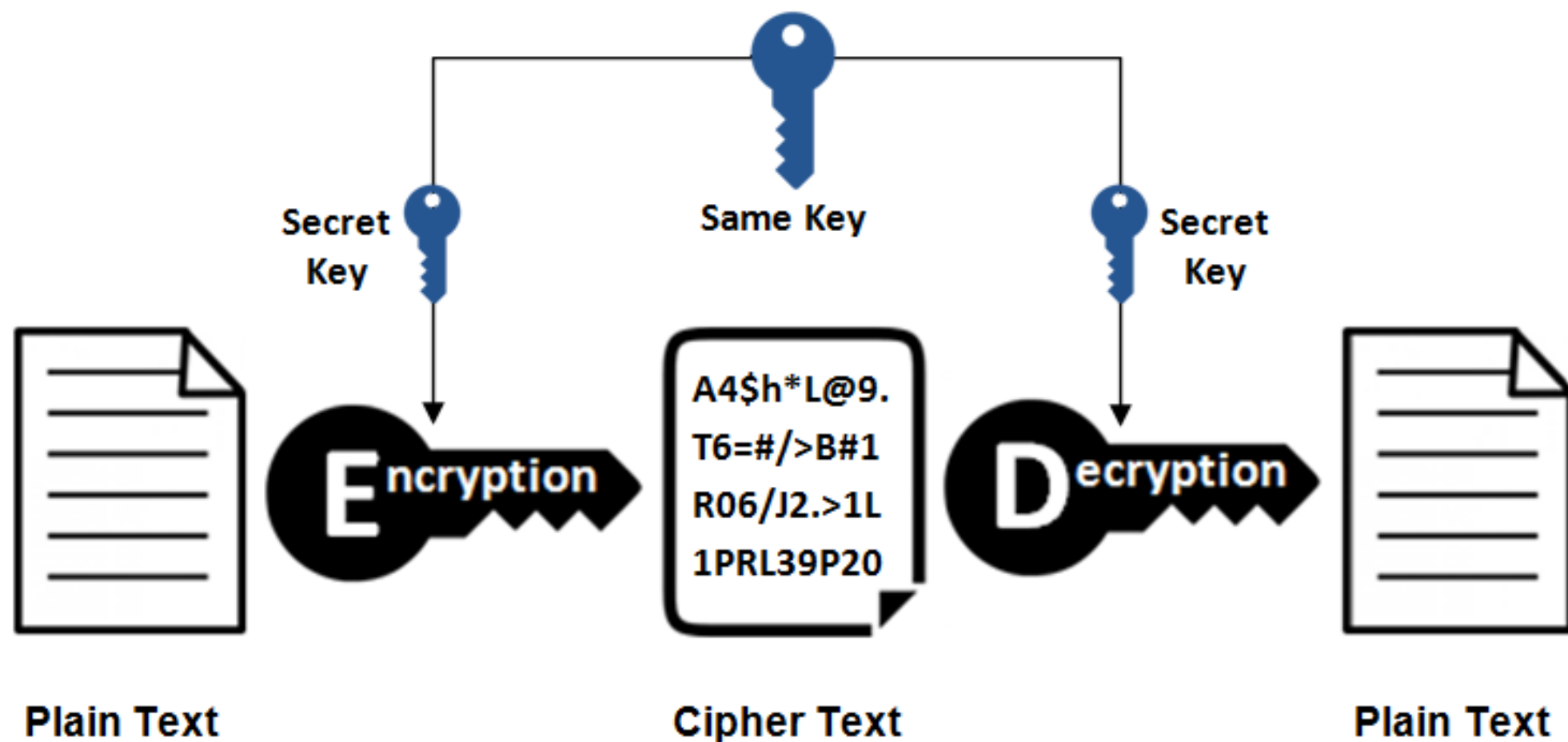
Encriptada con cifrado de
Vignère usando esta clave:

INTEGRA

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	Ñ	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	Ñ	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
Ñ	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
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	Ñ
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	Ñ	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y

Criptografía Simétrica

Symmetric Encryption



Intercambio de llaves

Protocolo Diffie-Hellman

Intercambio seguro de llaves, 1976



Ver video en:

https://www.youtube.com/watch?start=128&feature=oembed&v=YEBfamy-_do

Ejemplo [editar]

Alice			Bob		
Sec		Calc	Calc		Sec
	p, g			p, g	
a					b
		$g^a \bmod p$	→	...	
	...		←	$g^b \bmod p$	
	$(g^b \bmod p)^a \bmod p$		=	$(g^a \bmod p)^b \bmod p$	

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

El logaritmo aprovecha el problema del logaritmo discreto: dado $g^k = a$, es prácticamente imposible calcular $y \bmod p$ sabiendo g y a , con valores suficientemente grandes.

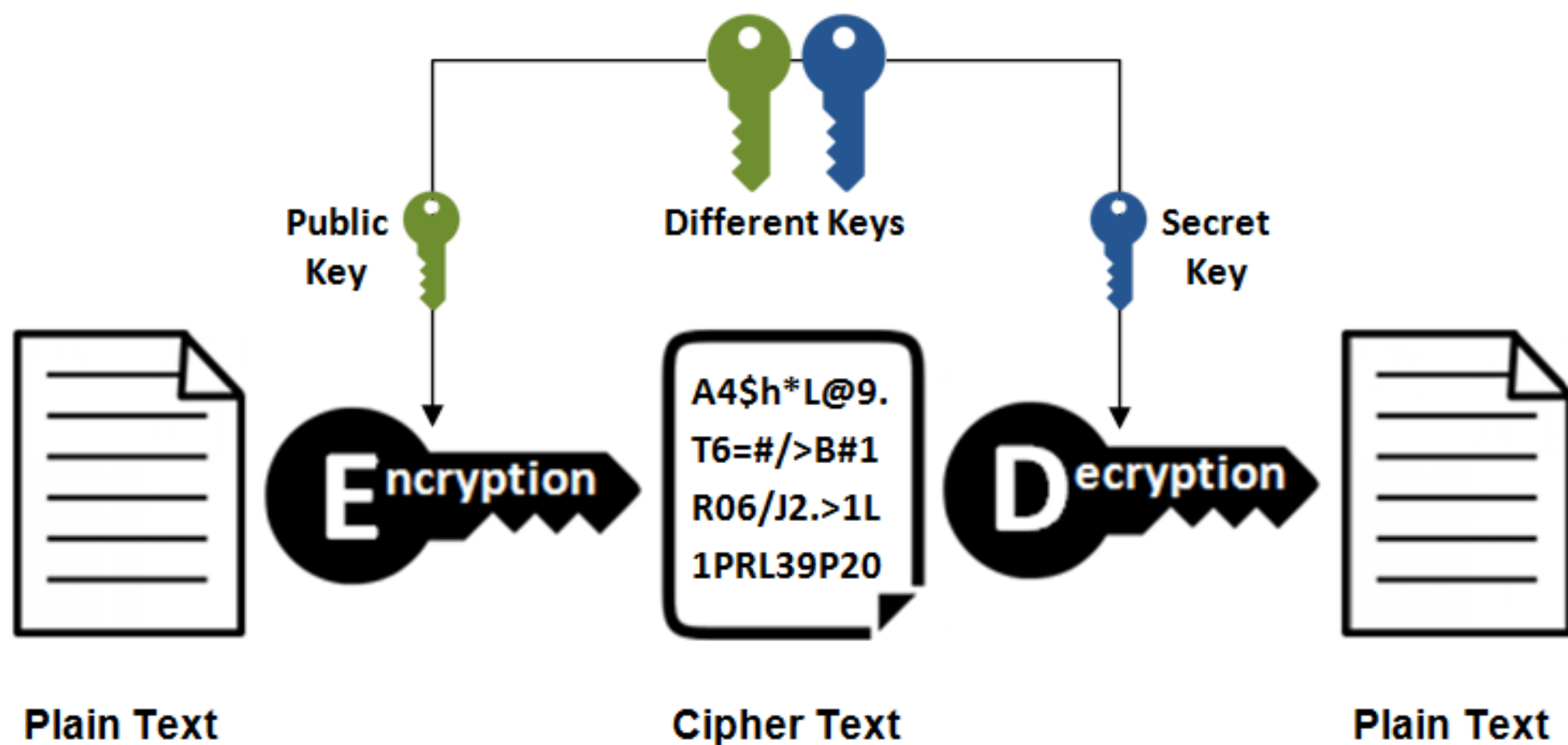
Whitfield Diffie y Martin Hellman
recibieron el prestigioso premio
A.M. Turing de 2015 de la
Association for Computer
Machinery en 2016 por este
trabajo "**que revolucionó la
seguridad informática**"



Criptografía asimétrica

Llaves público-privada

Asymmetric Encryption



Algoritmo RSA

1977

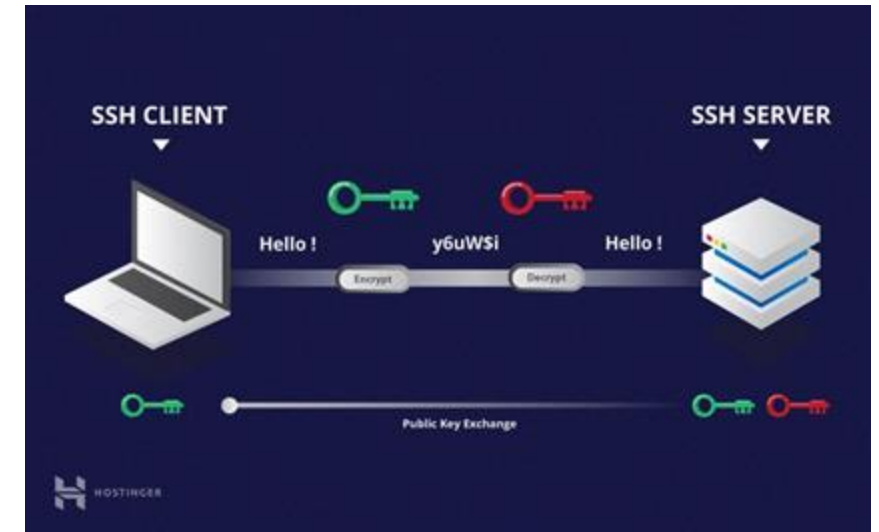
La encriptación **RSA** es un **algoritmo** de cifrado de clave pública que desarrollaron en el año 1977 profesores del MIT: Ron **R**ivest, Adi **S**hamir y Leonard **A**dleman.

La fortaleza de RSA reside en la dificultad computacional de factorizar un número compuesto muy grande compuesto por el producto de los dos números primos **p** y **q**.

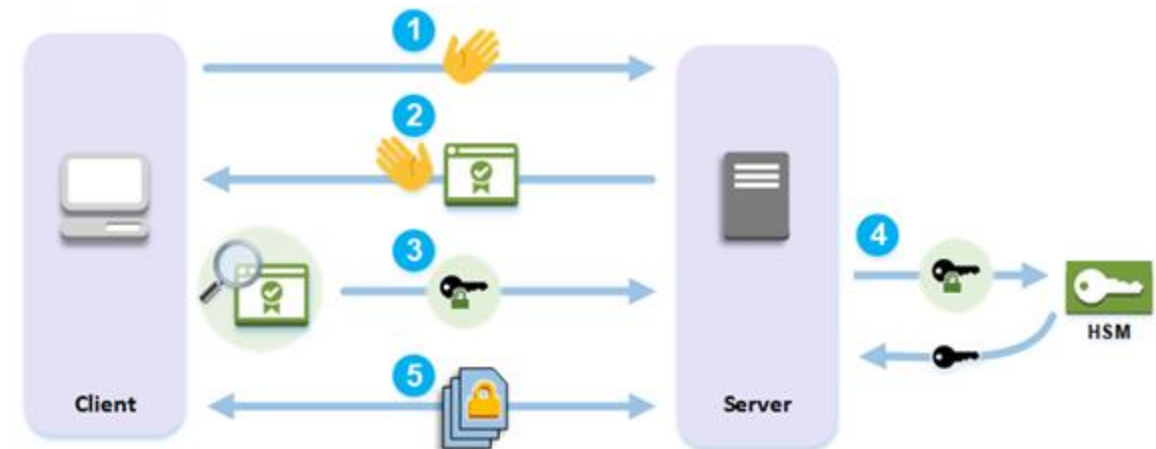
Requiere que el receptor comparta su llave pública al emisor.

Usado ampliamente en protocolos de seguridad:

- SSH
- OpenPGP
- SSL/TLS

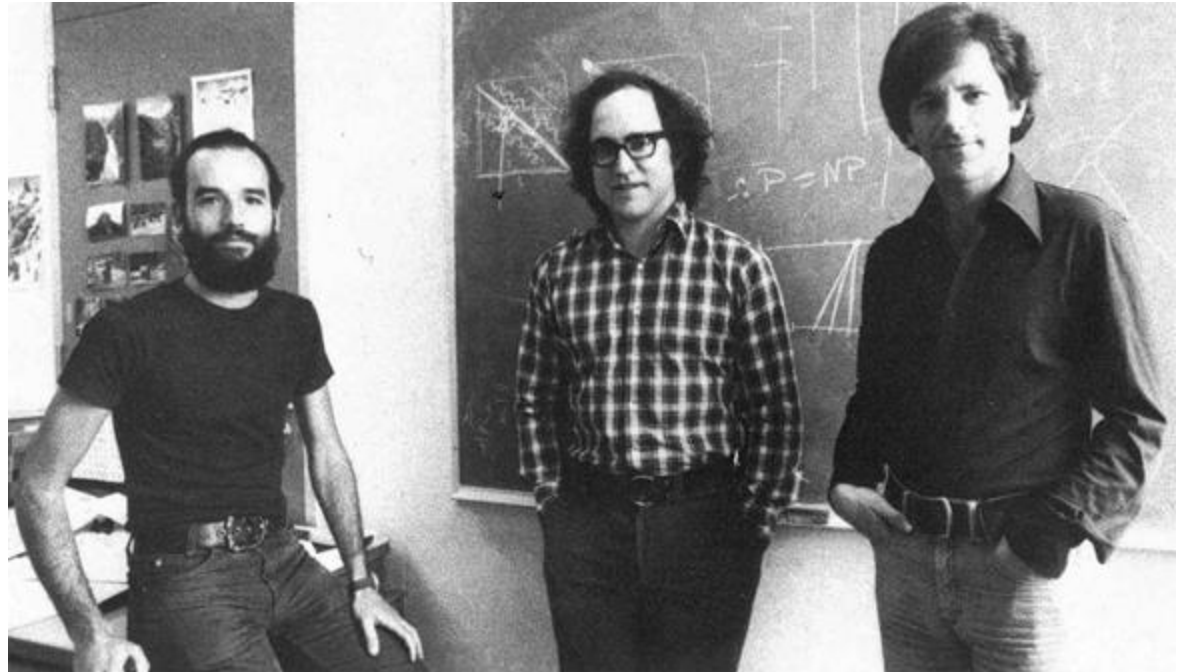


<https://www.hostinger.es/tutoriales/que-es-ssh>



https://docs.aws.amazon.com/es_es/cloudhsm/latest/userguide/ssl-offload-overview.html

La próxima vez que compres algo en línea, puedes agradecer a **Rivest, Shamir y Adleman**, o "RSA", el criptosistema de clave pública que sirve como la columna vertebral del comercio electrónico moderno. Fue desarrollado en la década de 1970 en el MIT.



Three-pass protocol

1980

Shamir-Rivest-Adleman Three Pass Protocol

Author(s): A. Shamir, R. Rivest, L. Adleman

Summary: The following protocol, described in [CJ97], allows two principals to exchange a secret message without sharing any initial secret.

Protocol specification (in common syntax)

A, B : principal
Ka, Kb : symkey
M : fresh number

```
1.   A  ->  B   :   {M}Ka
2.   B  ->  A   :   {{M}Ka}Kb
3.   A  ->  B   :   {M}Kb
```

Description of the protocol rules

This protocol assumes that encryption is commutative, *i.e.*

$$\{\{x\}y\}z = \{\{x\}z\}y.$$

The initiator A encrypts his message M by his secret key Ka, then B encrypts the message he received by his secret key Kb. Since $\{\{M\}Ka\}Kb = \{\{M\}Kb\}Ka$, the agent A can decrypt it and send $\{M\}Kb$ to B. Then, using Kb, B can retrieve M.

- No requiere intercambio de llaves.
- Requiere encriptación conmutativa.
- La comunicación es más ineficiente ya que requiere el envío de 3 mensajes en vez de 1

Cómo podemos hacer
sistemas seguros?

Principios de sistemas seguros

1. Diseño abierto: Obtén toda la ayuda que puedas
2. Minimizar secretos: Eventualmente se sabrán
3. Economía de mecanismos: Mientras menos hay, más fácil hacerlo bien
4. Defaults seguros: Lo más probable es que nadie los cambie
5. Principio de pocos privilegios: “No guardar el almuerzo con las joyas”

- ¿Cómo prevenimos inyección de lógica malintencionada durante el desarrollo de software?
- ¿Cómo prevenimos ataques de software en producción?
- ¿Cómo protegemos nuestros datos, como usuarios de sistemas?

Ethical Hacking



Resumen ejecutivo

Resumen de hallazgos

A continuación, se enumeran a modo de resumen las vulnerabilidades o hallazgos detectados durante la ejecución de esta actividad.

ID	Nombre	Score	Estado
1	Modificación de atributos de usuarios de otras empresas	Crítico (9.1)	Mitigado
2	Subida de archivos con extensiones no permitidas	Medio (5.3)	Mitigado
3	Envío de correos sin control de iteraciones	Medio (5.3)	Mitigado
4	Envío de correos de verificación a terceros	Medio (5.3)	Mitigado
5	Asociación de departamentos a terceros	Medio (5.3)	Mitigado
6	Modificación de atributos de la configuración del plan de la cuenta	Alto (7.5)	Mitigado

OWASP, un framework para desarrollo de aplicaciones seguras



OWASP

Open Web Application Security Project

OWASP TOP 10

- A1:2017 – Inyección
- A2:2017 – Pérdida de autenticación
- A3:2017 – Exposición de datos sensibles
- A4:2017 – Entidades externas XML (XXE)
- A5:2017 – Pérdida de control de acceso
- A6:2017 – Configuración de seguridad incorrecta
- A7:2017 – Secuencia de comandos en sitios cruzados (XSS)
- A8:2017 – Deserialización insegura
- A9:2017 – Componentes con vulnerabilidades inseguras
- A10:2017 – Registro y monitoreo insuficientes

Bibliografía – Métodos de encriptación y hash

- Public key cryptography - Diffie-Hellman Key Exchange (full version)
 - https://www.youtube.com/watch?v=YEBfamv-_do
- SHA1 Hash generator
 - <https://passwordsgenerator.net/sha1-hash-generator/>
- How secure is 256 bit security?
 - https://www.youtube.com/watch?v=S9JGmA5_unY
- Intro to RSA Encryption (step 1)
 - <https://www.youtube.com/watch?v=dleUxfghd5I>
- How does RSA works
 - <https://hackernoon.com/how-does-rsa-work-f44918df914b>
- Are your passwords in the green?
 - <https://www.hivesystems.io/blog/are-your-passwords-in-the-green>

Bibliografía - Curvas elípticas

- Elliptic-curve cryptography
 - https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
- Elliptic Curve Back Door - Computerphile
 - <https://www.youtube.com/watch?v=nybVFJVBwww>
- SafeCurves: choosing safe curves for elliptic-curve cryptography
 - <https://safecurves.cr.yp.to/>

Bibliografía – Temas de seguridad

- Caso virus Stuxnet:
 - What is the most sophisticated piece of software/code ever written?
 - <https://www.quora.com/What-is-the-most-sophisticated-piece-of-software-code-ever-written>
- Casos de estudio Harvard Business Review:
 - Internet insecurity
 - <https://hbr.org/cover-story/2018/05/internet-insecurity>
 - Security trends by the number
 - <https://hbr.org/2018/05/security-trends-by-the-numbers>
- Política nacional de ciberseguridad
 - <http://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf>

Bibliografía – Temas de seguridad

- Accenture
 - COST OF CYBER CRIME STUDY 2017
 - https://www.accenture.com/t20170926T072837Z_w_us-en_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
- Dell SecureWorks
 - Underground hacker markets 2016
 - http://online.wsj.com/public/resources/documents/secureworks_hacker_annualreport.pdf
- Diario Financiero
 - Virus informático que atacó Banco de Chile enciende alarmas en el Central y Hacienda
 - <https://www.df.cl/noticias/empresas/telecom-tecnologia/virus-informatico-que-ataco-banco-de-chile-enciende-alarmas-en-el/2018-05-29/211551.html>

Bibliografía – Temas de seguridad

- XKCD - Password strength
 - https://imgs.xkcd.com/comics/password_strength.png
- Sarah Palin Email Hack
 - https://en.wikipedia.org/wiki/Sarah_Palin_email_hack
 - <https://www.wired.com/2008/09/palin-e-mail-ha/>
- Bangladesh Bank robbery
 - https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery
- Most sophisticated piece of software
 - <https://www.quora.com/What-is-the-most-sophisticated-piece-of-software-ever-written-1/answer/John-Byrd-2>
- Thieves Found Citigroup Site an Easy Entry
 - <https://www.nytimes.com/2011/06/14/technology/14security.html>

Bibliografía – Temas de seguridad

- MIT - Computer Systems Security
 - <https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/index.htm>
- Owasp Top 10
 - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
 - <https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf>