TIB

Seguridad en la Información

# Rainbow Tables para revisiones de seguridad

# Quien soy?

Maximiliano Alonzo

Consultor en Seguridad Informática.

Integrante del OWASP capítulo Uruguay.

malonzo@tib.com.uy

# De que se trata esta charla?

# Cuando podemos necesitar usar una Rainbow Table?

- Evaluar la robustez de los hash de contraseñas

También podemos utilizar herramientas de crackin

Pero el uso de herramientas de cracking por fuerza bruta requiere tiempo y poder de computo suficiente.

Con que inconvenientes nos encontramos al utilizar herramientas de cracking por fuerza bruta?

Tenemos un problema de TIEMPO!

- Insuficiente poder de computo.

- Insuficiente tiempo para realizar el trabajo.

- Cada nueva búsqueda HASH hace que sea necesario volver a realizar todo el proceso de computo.

Esto hace que pueda resultar inviable su utilizació

# Pero....

Podríamos generar todas las combinaciones de HASH/CLAVE y almacenarlas?

A fin de ahorrase tener que volver a calcularlas y facilitar la futura búsqueda.

Varios algoritmos de resumen
CRC, MD5, SHA1, LM,
Whirlpool, etc.

Cada algoritmo genera resultados diferentes:

**password**

**LM** E52CAC67419A9A224A3B108F3FA6CB6D

**MD5** 5f4dcc3b5aa765d61d8327deb882cf99

Necesario generar todas las combinaciones
por cada algoritmo

Tenemos un problema de ESPACIO!

Inviable almacenar todas las combinaciones de claves para cada algoritmo de resumen.

# Resumiendo los inconvenientes

TIEMPO necesario para generar cada uno de los resúmenes de las claves.

ESPACIO necesario para almacenar todas las combinaciones generadas previamente.

# Que nos puede facilitar la vida?

“Making a Faster Cryptoanalytic Time-Memory Trade Off”
by Philippe Oechslin

Implementación practica de un compromiso Espacio-Tiempo mas óptimo.
Rainbow Tables

Que son las Rainbow Tables?

Implementación de compromiso espacio-tiempo

Permite almacena de una forma optima el resultado previamente calculado de la generación de claves y su hash.

mite realizar búsquedas de claves a partir de un ha

# Como funciona una Rainbow Tables?

# Resumen, Reducción, Resumen, Reducción, ....

## RESUMEN

Nos permite obtener un HASH a partir de una CLAVE.

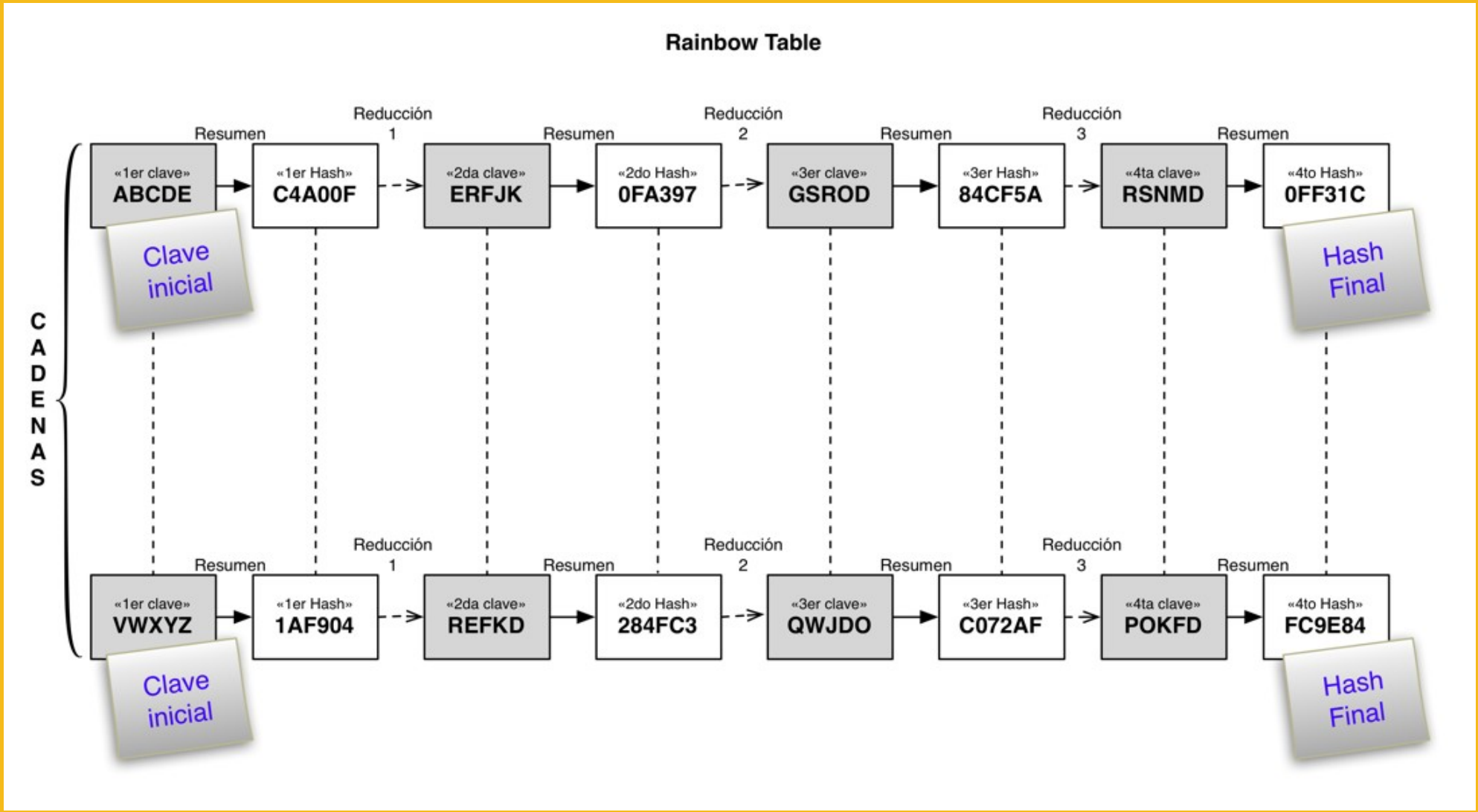
## REDUCCION

Nos permite obtener una CLAVE a partir de una HASH.

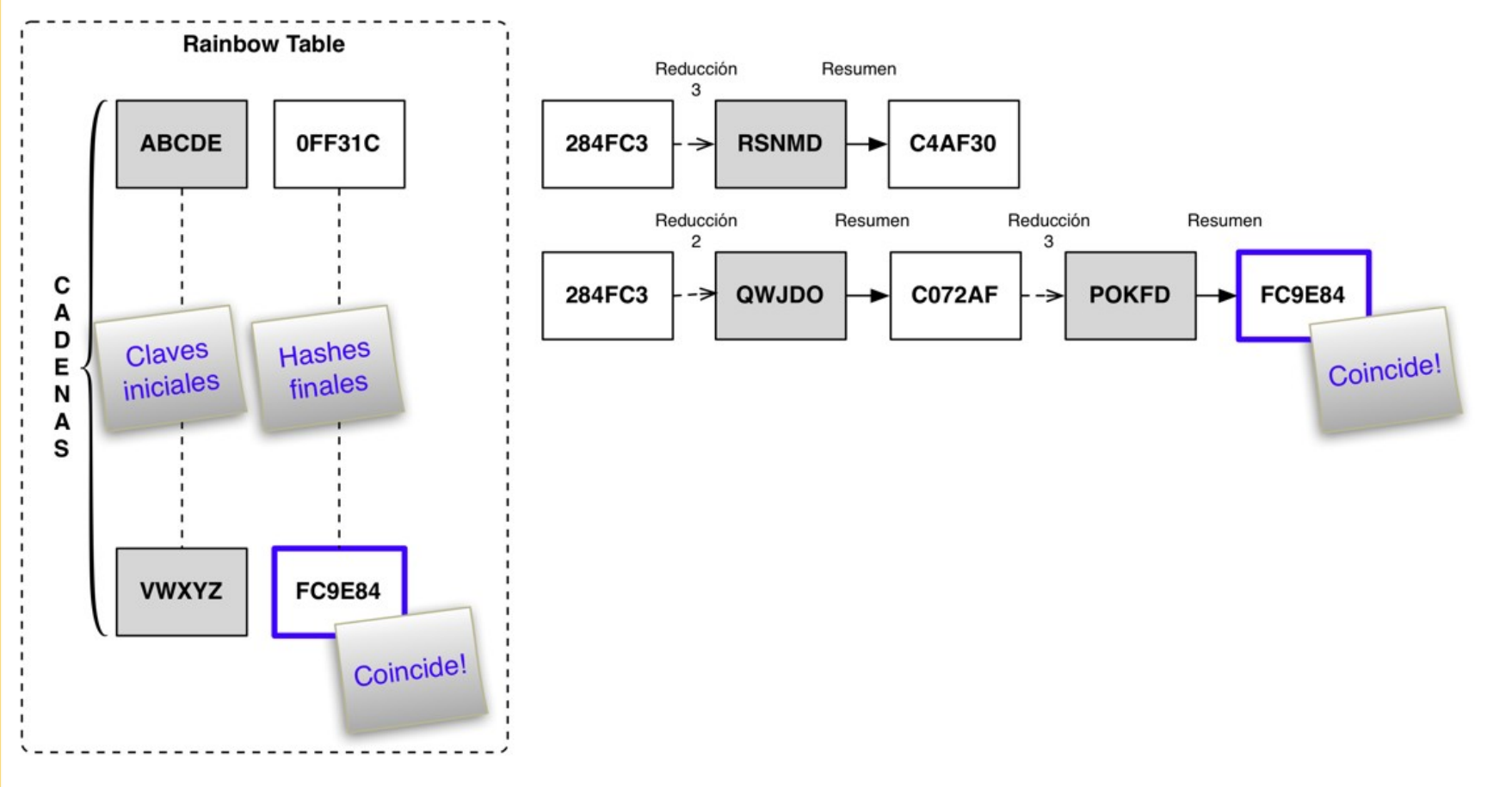
Nunca se almacena toda la tabla generada.

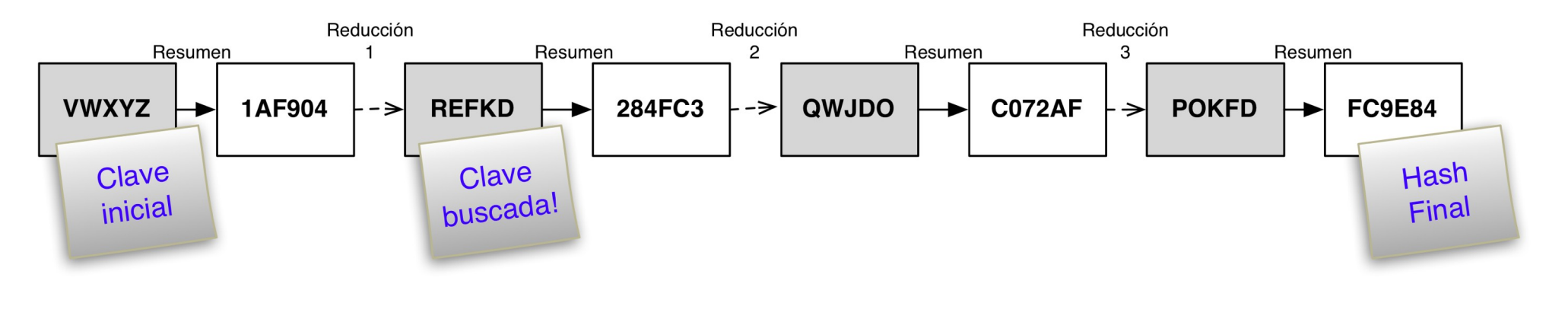
Se generan cadenas y se almacena la Clave inicial y el Hash final de la misma.

0mil a 200mil iteraciones por cade


Rainbow Table
CADENAS
Resumen
Reducción 1
Resumen
Reducción 2
Resumen
Reducción 3
Resumen
«1er clave» ABCDE
«1er Hash» C4A00F
«2da clave» ERFJK
«2do Hash» 0FA397
«3er clave» GSROD
«3er Hash» 84CF5A
«4ta clave» RSNMD
«4to Hash» 0FF31C
Clave inicial
Hash Final
Resumen
Reducción 1
Resumen
Reducción 2
Resumen
Reducción 3
Resumen
«1er clave» VWXYZ
«1er Hash» 1AF904
«2da clave» REFKD
«2do Hash» 284FC3
«3er clave» QWJDO
«3er Hash» C072AF
«4ta clave» POKFD
«4to Hash» FC9E84
Clave inicial
Hash Final

# Como es el proceso de búsqueda?




Resumen
Reducción 1
Resumen
Reducción 2
Resumen
Reducción 3
Resumen
VWXYZ
1AF904
REFKD
284FC3
QWJDO
C072AF
POKFD
FC9E84
Clave inicial
Clave buscada!
Hash Final

# DEMOSTRACIÓN

## ohn the Ripper VS Ophcrack (by Philippe Oechslin)

Búsqueda de hash LM

Tamaño de tablas LM 18GB

# OWASP TOP10

## A7: Almacenamiento criptográfico inseguro

El error más común en este área es simplemente no cifrar datos que deberían ser cifrados. Cuando se cifra la información, son comunes la generación y almacenamiento inseguros de claves, no rotación de claves y el uso de algoritmos débiles. También es común el uso de hashes inseguros y sin sal para la protección de contraseñas. Los atacantes externos tendrán dificultades para identificar este tipo de vulnerabilidades debido al acceso limitado que disponen. Normalmente es necesario explotar alguna otra vulnerabilidad primero con el objetivo de obtener el nivel de acceso necesario.

# Recomendaciones

- Utilizar HASH que incluyan SALT.
(Las RT son inefectivas.)

- Hacer uso de claves complejas.

- Seleccionar algoritmos de resumen robustos.

# ¿Preguntas?

TIB

Seguridad en la Información

# Gracias!