Seguridad de la Información

Introducción a la Criptografía

Federico Pacheco

 @FedeQuark

 www.federicopacheco.com.ar

 info@federicopacheco.com.ar

Contenidos

- Conceptos y elementos
- Usos de la criptografía
- Clasificación histórica
- Tipos de algoritmos
- Protocolos de cifrado
- Protección de datos locales y en tránsito
- Esteganografía y esteganálisis

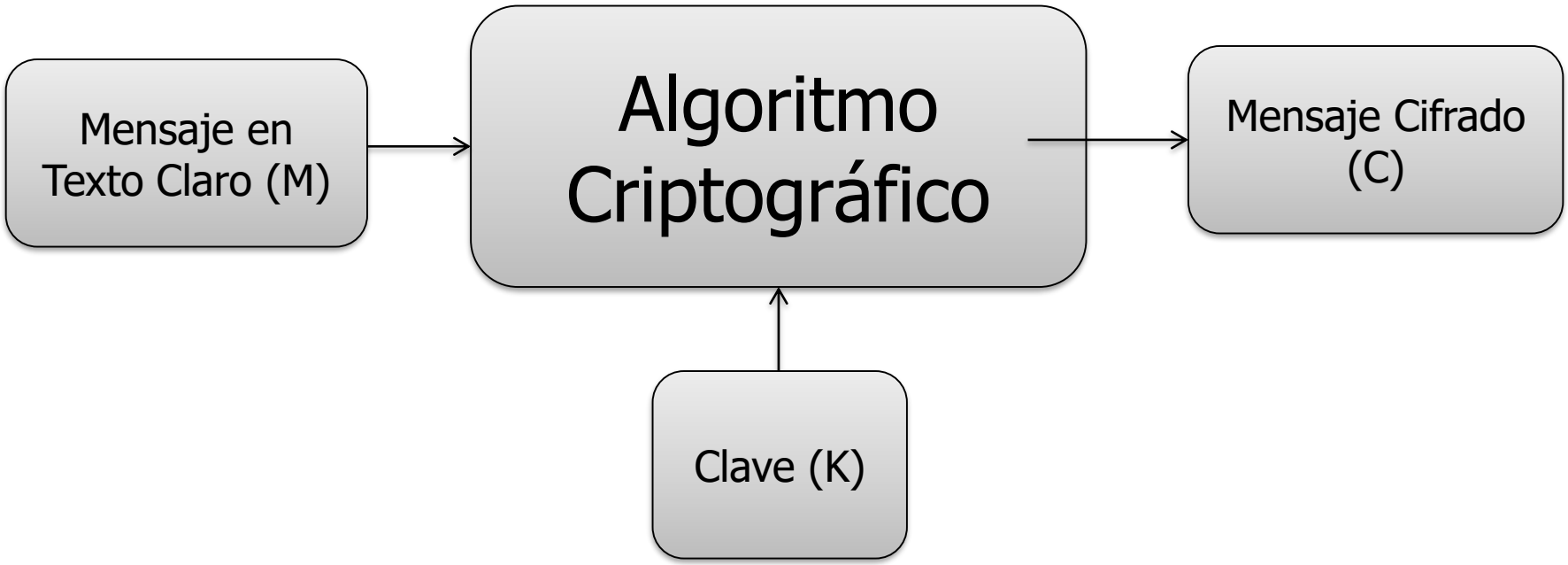
Conceptos y elementos

- Criptografía: protección de información ante observadores no autorizados
  - Provee confidencialidad e integridad

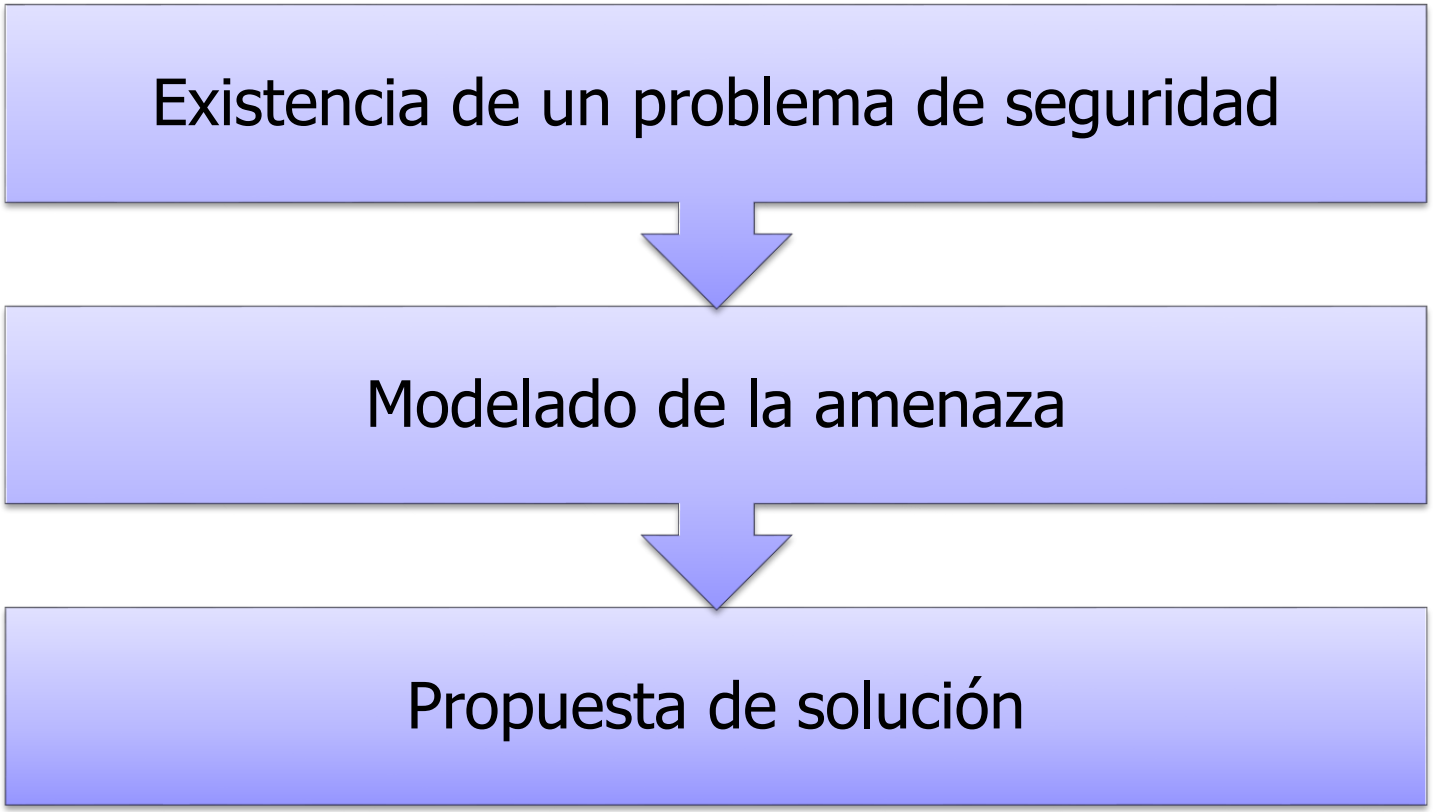
- Estado del arte
  - Base: Matemáticas
  - Dominio: Cs. de la Computación
  - Estandarizado internacionalmente
  - Cutting-edge: criptografía cuántica

- Criptoanálisis: estudio del cifrado para lograr romperlo

Esquema general



Modelo subyacente



Definiciones

Criptología	• Criptografía + Criptoanálisis
Cifrar	• Aplicar un algoritmo criptográfico
Texto Plano / Claro	• Texto original o Mensaje (M)
Texto Cifrado	• Criptograma (C)
Clave / Llave	• Criptovariables que permiten cifrar y descifrar
Protocolo criptográfico	• Conjunto de reglas para interactuar en un criptosistema
Criptosistema	• Conjunto completo de elementos de un criptosistema

Definiciones – Espacios

- Espacio de llaves
  - Conjunto de todas las llaves posibles

- Espacio de Mensajes
  - Todos los mensajes posibles: M = {m1, m2, ..., mn}

- Espacio de Criptogramas
  - Todos los criptogramas posibles: C = {c1, c2, ..., cn}

Propósitos técnicos

- Almacenamiento seguro
- Comunicaciones seguras
- Autenticación
- Firma digital
- Verificación de integridad

Propósitos prácticos

Garantizar el secreto

- Protección de información ante personas no autorizadas

Garantizar la anonimidad

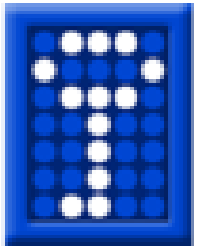
- Comunicaciones anónimas y privacidad online

Garantizar la identidad

- Acceso seguro a sistemas y firmado digital

Usos personales

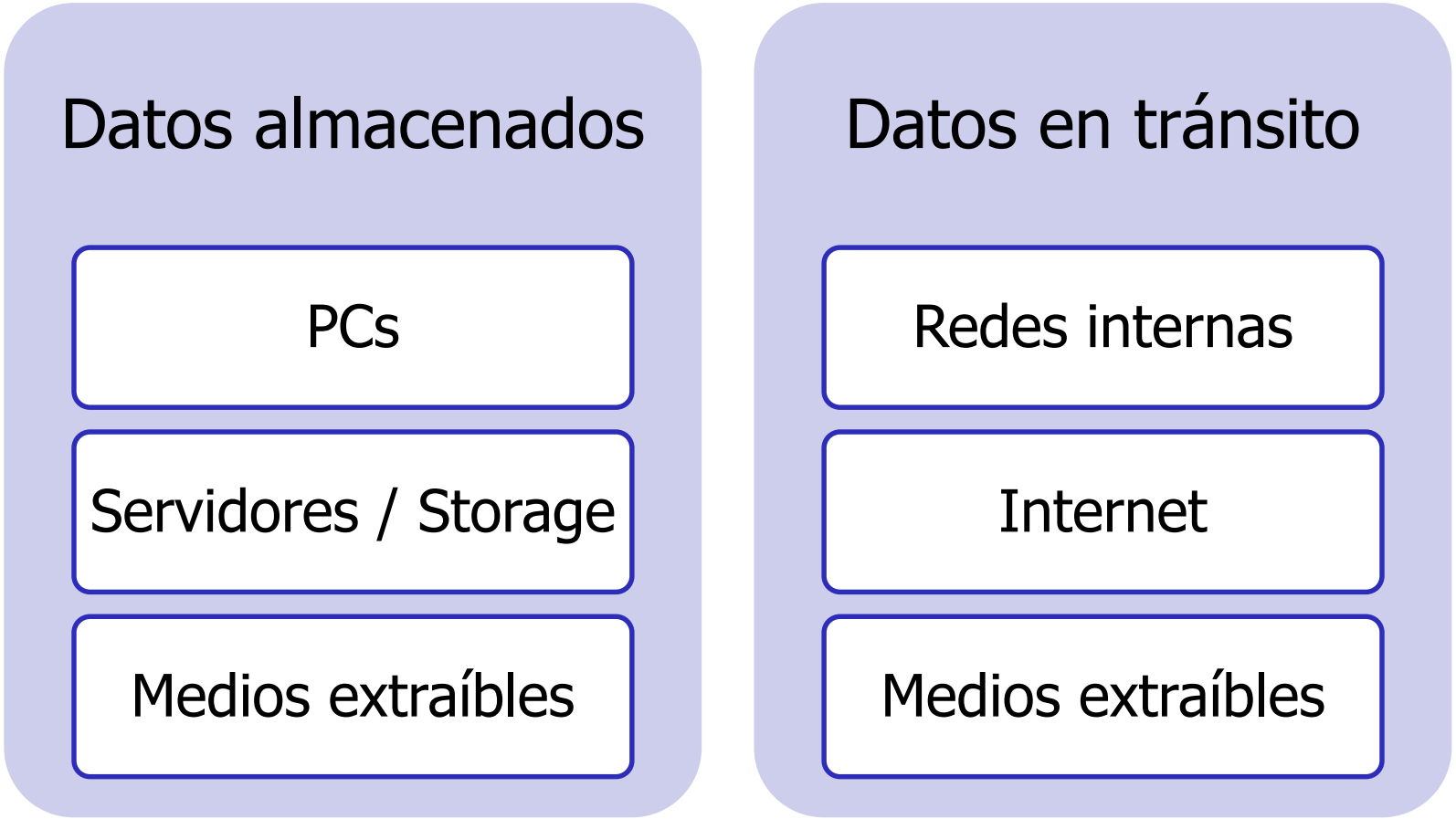
- Protección de datos
  - Caso Truecrypt



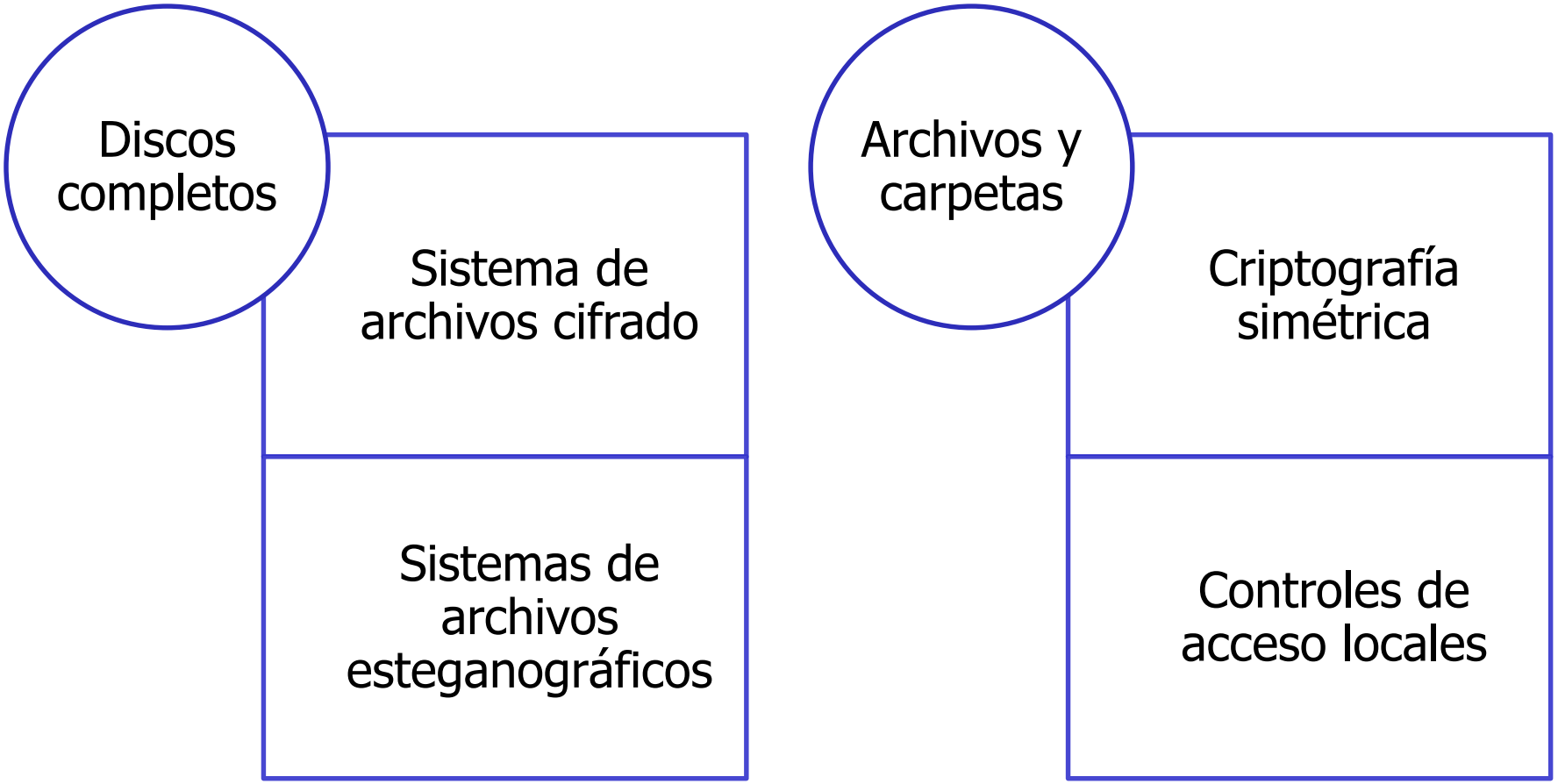
- Navegación privada
  - Caso TOR

- Correo electrónico seguro
  - Caso PGP

Ubicación de los datos a proteger



Protección de datos almacenados



Niveles de seguridad criptográfica

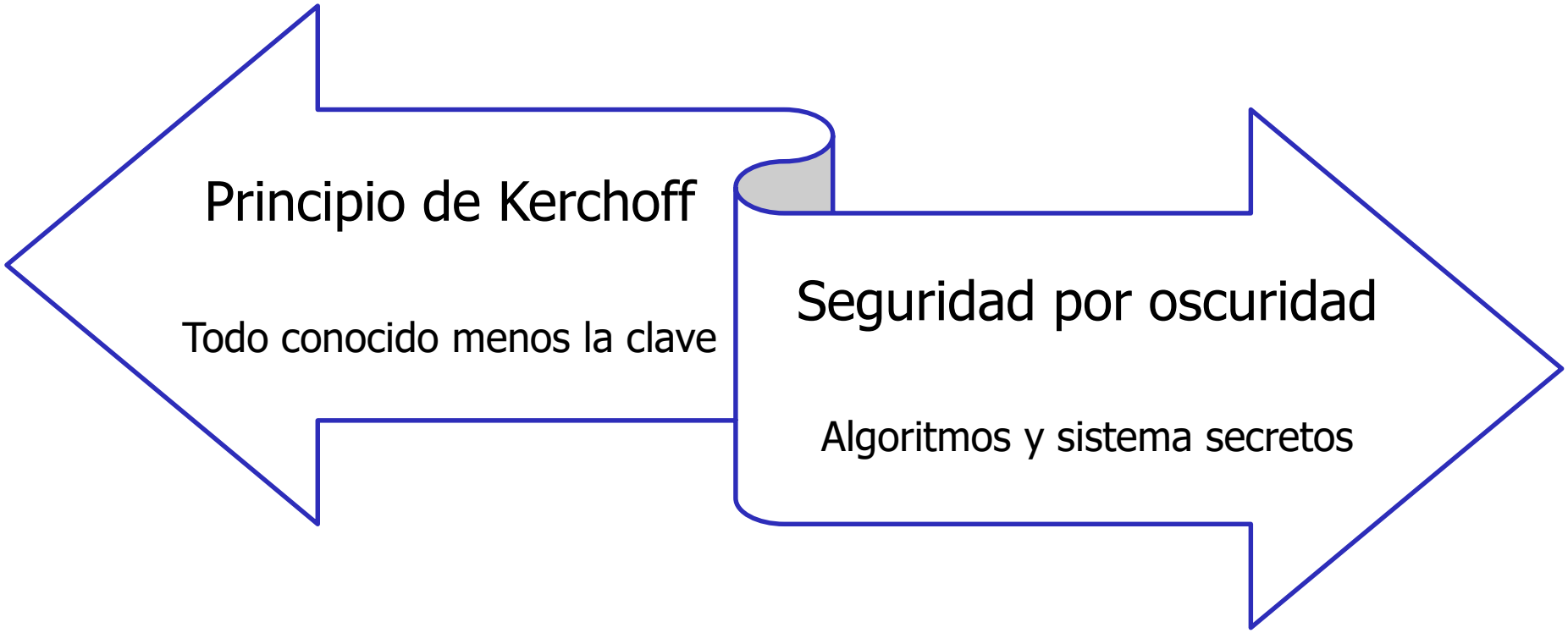
Seguridad teórica

- No se puede romper incluso con tiempo y recursos ilimitados

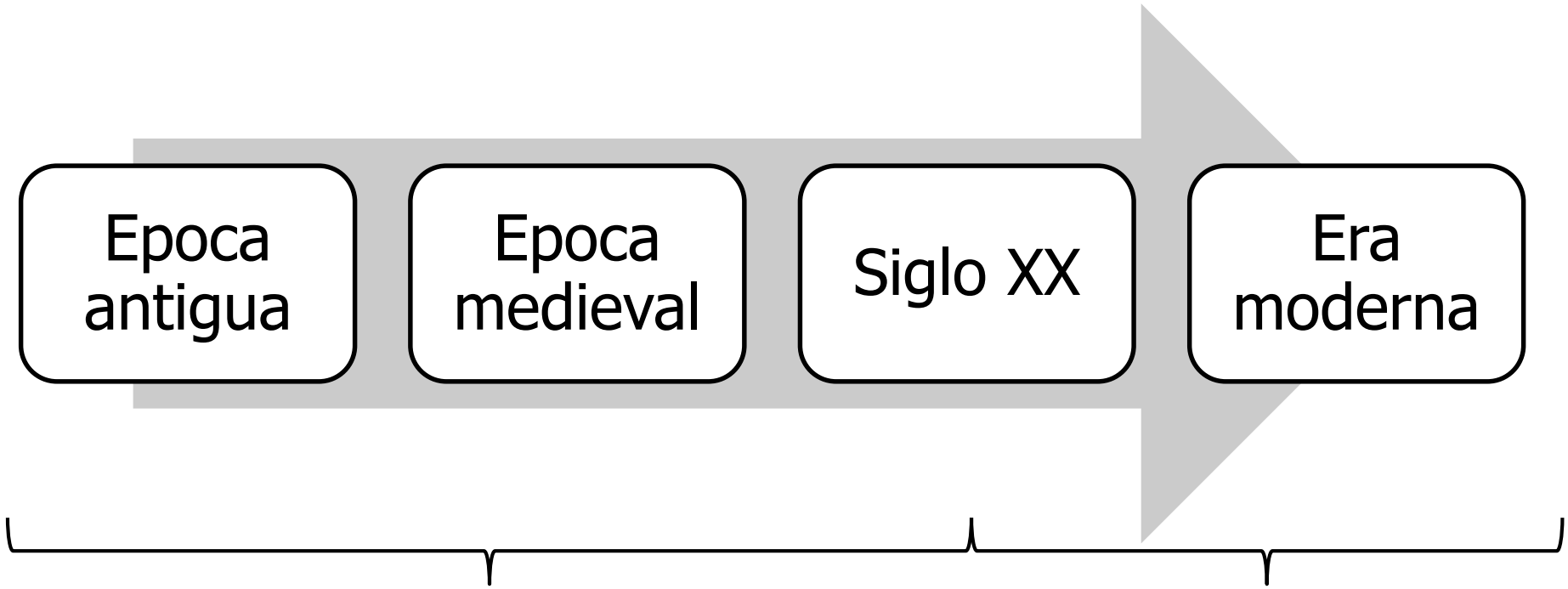
Seguridad práctica

- No se puede romper con los recursos disponibles

Conocimiento del sistema



Distintas épocas

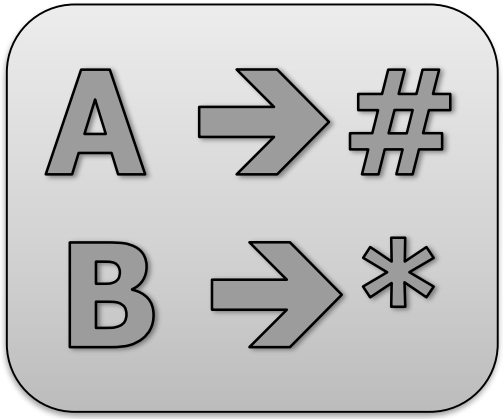


Sistemas clásicos	Sistemas modernos
- Basados en el secreto del método	- Basados en el secreto de la clave
- Se cifran letras	- Se cifran bits

Sistemas clásicos – Técnicas

- Sustitución
  - Correspondencia entre un símbolo y otro
  - Puede atacarse por análisis de frecuencias
  - Principio de confusión (Shannon)

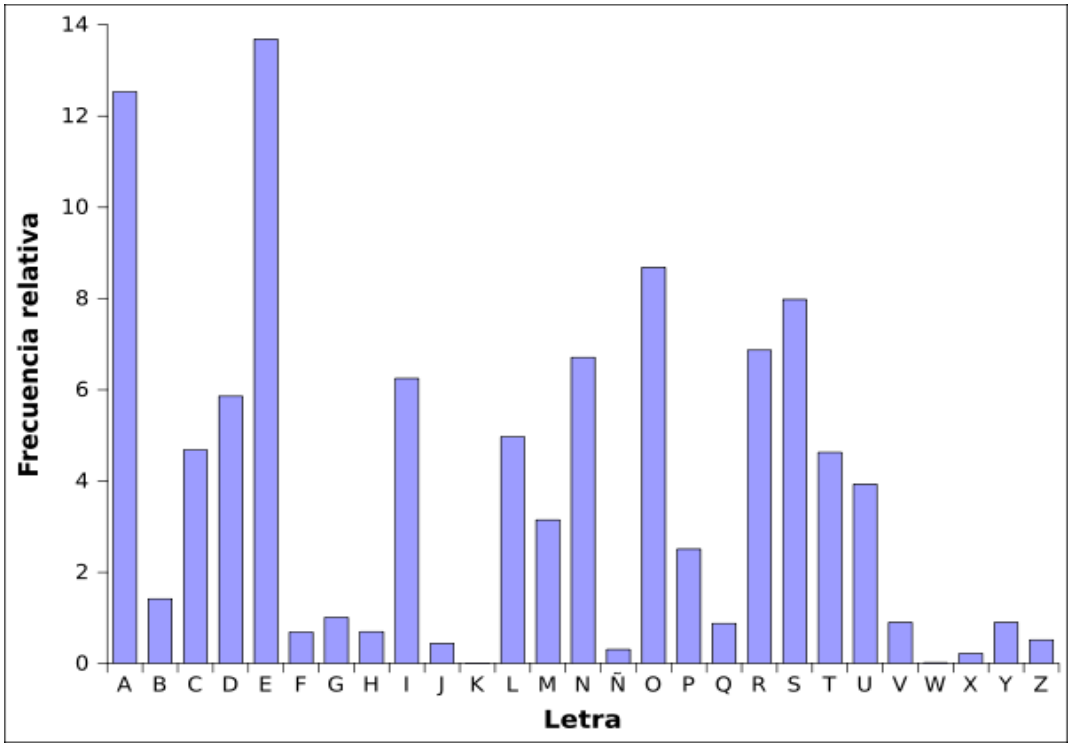
- Transposición
  - Los símbolos se redistribuyen sin modificarlos y según reglas
  - Principio de dispersión (Shannon)



Sistemas clásicos – Ataque por frecuencias

- Se relaciona los elementos más frecuentes del criptograma

- El texto debe tener una longitud considerable



Sistemas clásicos – Alfabetos de cifrado

- En el español:
  - Solo mayúsculas (módulo 27)
  - Mayúsculas y números 0-9 (módulo 37)
  - Mayúsculas y minúsculas (módulo 54)
  - Mayúsculas, minúsculas y números (módulo 64)
  - Todos los caracteres imprimibles ASCII (módulo 224)

- El espacio en blanco presenta una frecuencia de casi un 20%

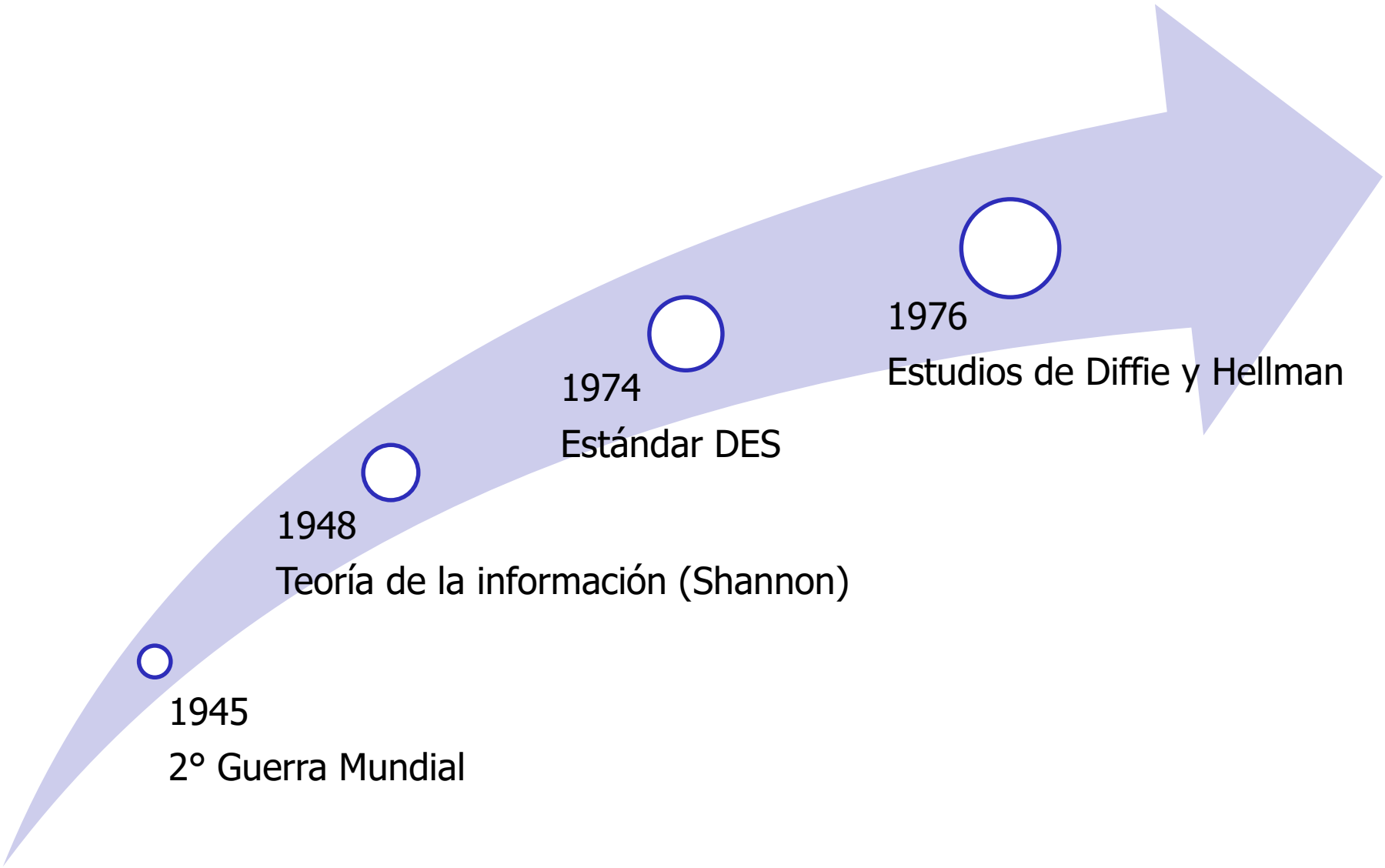
ABC abc 123 */?

Sistemas clásicos – Uso de alfabetos

- Sistemas monoalfabeticos: utilizan un solo alfabeto transformado
  - Son fáciles de analizar por frecuencia de caracteres
  - Se aprovecha la redundancia del lenguaje (predicibilidad)

- Sistemas polialfabéticos: utilizan más de un alfabeto para el cifrado
  - Si una letra se repite, no se cifra igual (se evitan análisis directos por frecuencia)
  - Existe una periodicidad con la que se repite la misma transformación

Hitos en sistemas modernos



Sistemas Modernos – Clasificación de algoritmos

Según la clave utilizada

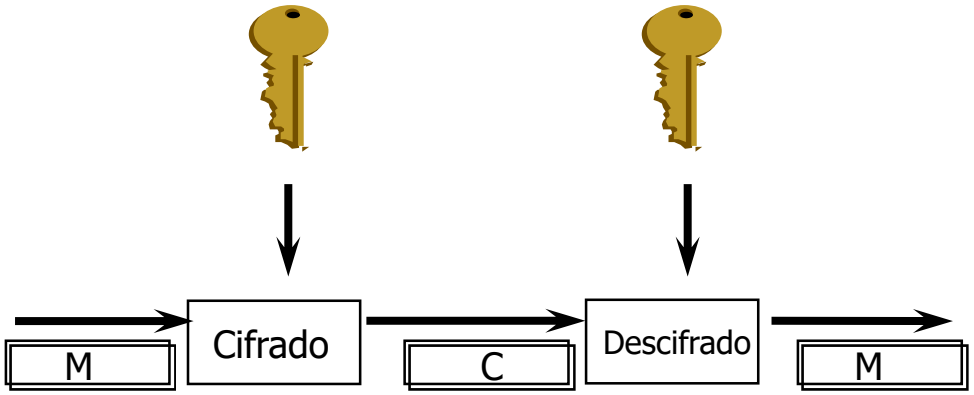
- Simétricos: Se utiliza la misma clave para cifrar y descifrar
- Asimétricos: Se utilizan claves distintas para cifrar y descifrar
- Irreversibles (sin clave): no permitiendo su descifrado

Según los elementos cifrados a la vez

- Bloque: Dividen el texto en fragmentos iguales para cifrar
- Flujo: Cifran símbolo o bit a bit

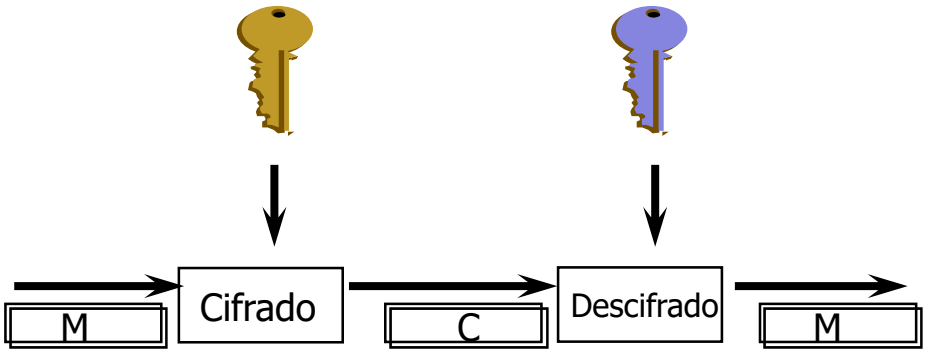
Algoritmos Simétricos

- DES / 3DES
- IDEA
- Blowfish
- RC5
- AES



Algoritmos Asimétricos

- Diffie Hellman
- RSA
- El Gamal
- Curvas Elípticas



Aprender más

```
 /\/\   ___| |_ __ _   __| | ___  ___ _ __ _   _ _ __ | |_ ___  _ __   v1.0
/    \ / _ \ __/ _` | / _` |/ _ \/ __| '__| | | | '_ \| __/ _ \| '__|
/ /\/\ \  __/ || (_| | (_| |  __/ (__| |  | |_| | |_) | || (_) | |
\/    \/\___|\__\__,_|\__,_|\___|\___|_|   \__, | .__/ \__\___/|_|
                                             |___/|_|

Core Commands
=============

       Command         Description
       -------         -----------
       -h              Help
       -author         Author
       -credit         Credits
       -hex            Decode hexadecimal
       -b64            Decode base64
       -caesar         Break caesar cipher
       -vigenere       Break vigenere cipher
       -affine         Break affine cipher
       -reverse        Decrypt reverse cipher
       -bacon          Decrypt bacon cipher
       -morse          Decrypt morse cipher
       -pediaphone     Decrypt pediaphone cipher
       -transpose      Decrypt transpose cipher
       -friedman       Is monoalpabetical or polyalphabetical?
```

Algoritmos de Hash

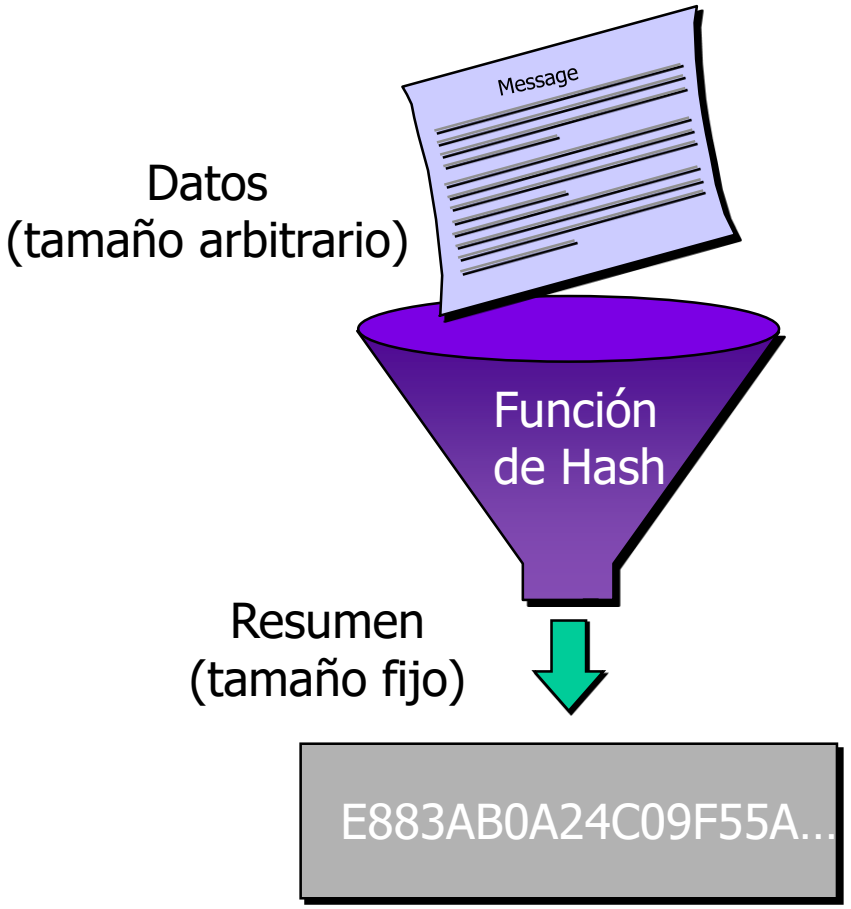
- Se aplica una función sobre un conjunto de datos variables, se obtiene un resumen
  - Se obtiene como resultado el "resumen" (digest o hash)
  - El resumen tiene tamaño fijo e independiente del original
  - Está asociado unívocamente a los datos iniciales

- Es muy difícil encontrar dos mensajes distintos que tengan hash idéntico
  - Es posible pero la probabilidad de "colisión" es muy baja

- Aplicaciones
  - Contraseñas , Firma Digital, Integridad y Autenticación

Algoritmos de Hash

- MD5
- SHA-1
- RIPEMD-160
- HAVAL



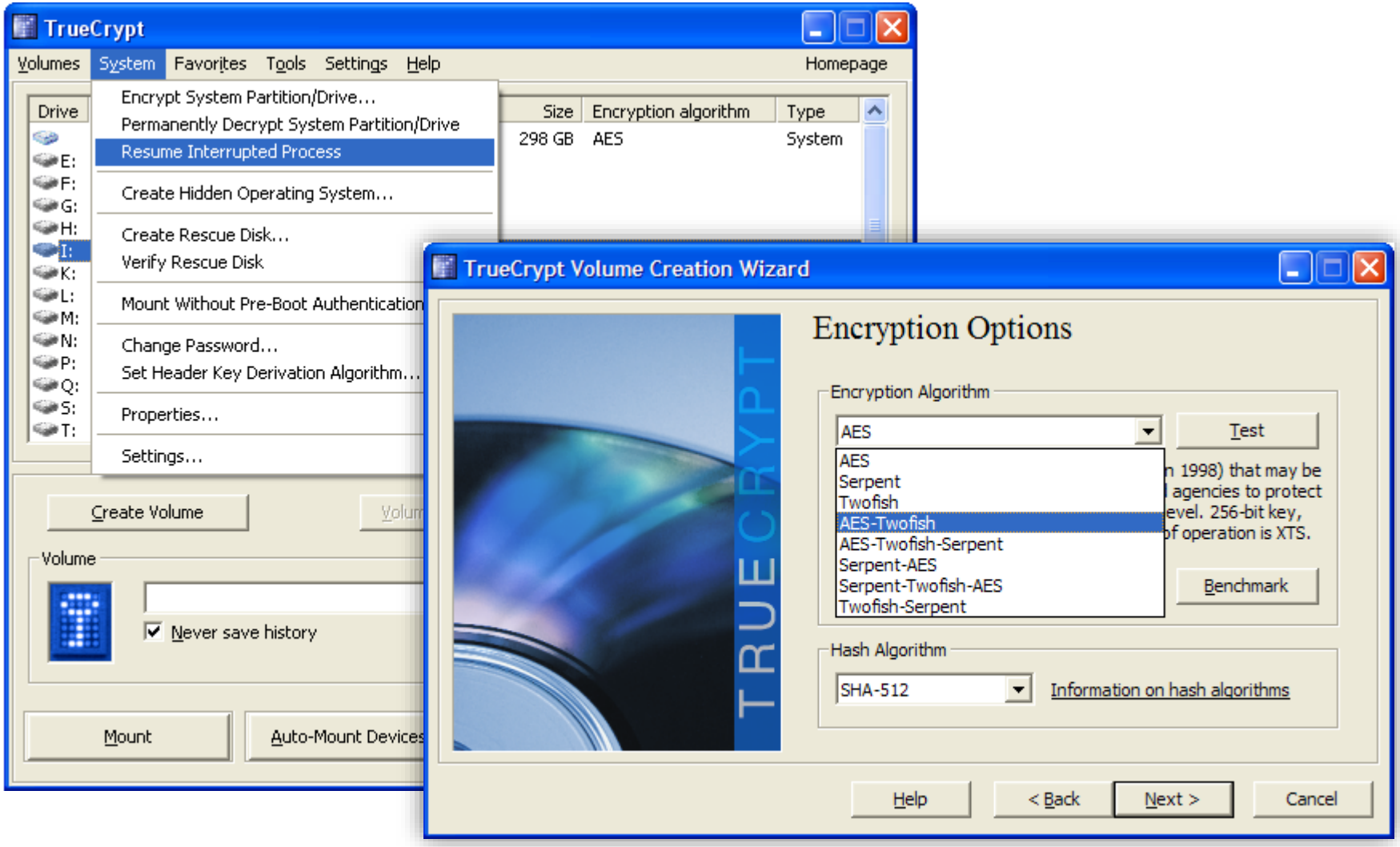
Esteganografía y estaganálisis

- Esteganografía: Técnica para ocultar información dentro de otra información
  - Los formatos más utilizados son fotografías, audio y video
  - La efectividad es muy alta
- Esteganálisis: Técnica de detección de mensajes esteganografiados
  - Identificar datos sospechosos, determinar si contienen información, y recuperarla
  - La complejidad es muy alta y nunca se puede garantizar la inexistencia
    - El archivo sospechoso no tiene nada raro
    - Si hay algo oculto puede estar encriptado
    - Puede haber datos de "ruido" en el archivo

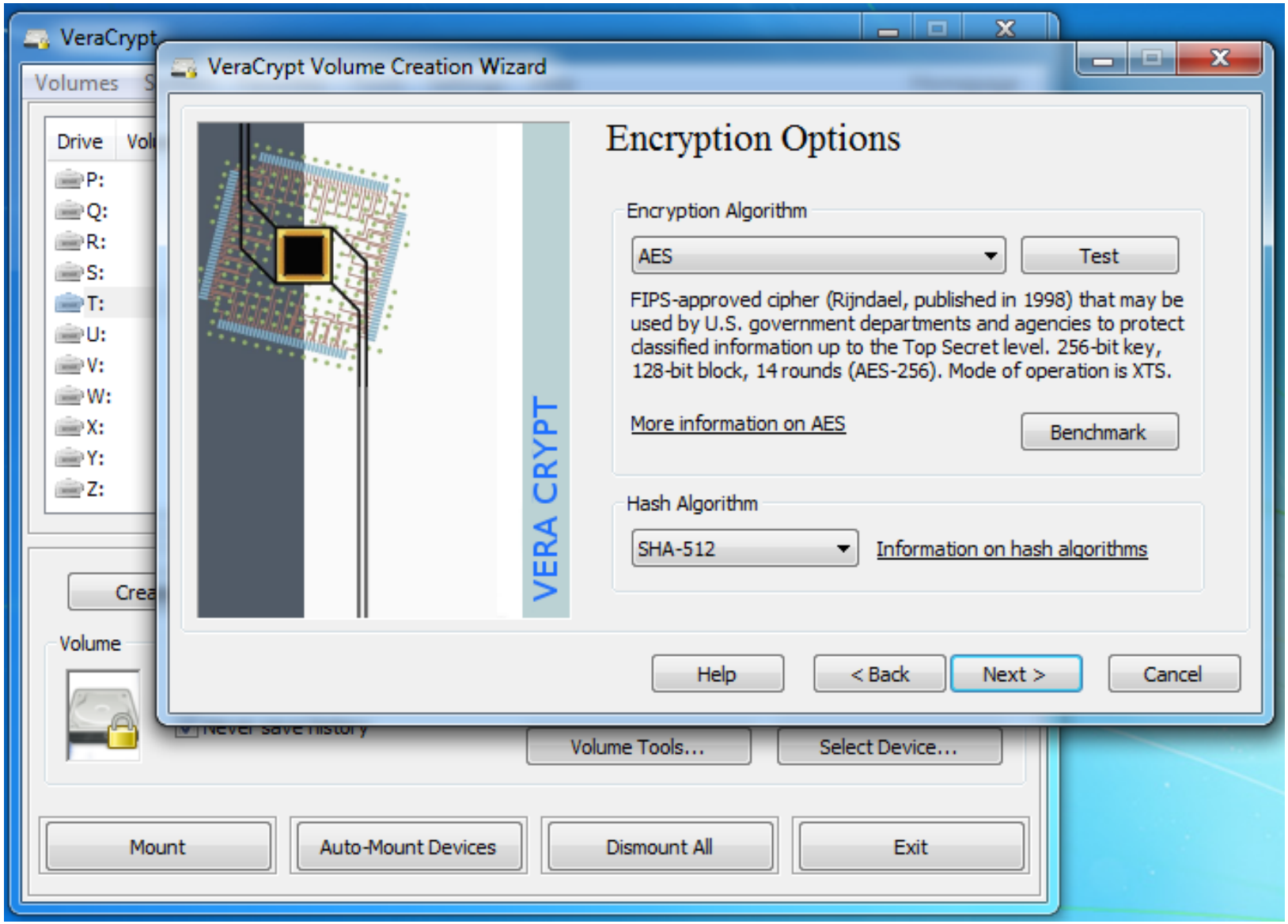
Ejemplos de protocolos criptográficos

- PGP / GPG
- SSH
- SSL / TLS
- Kerberos
- DSS

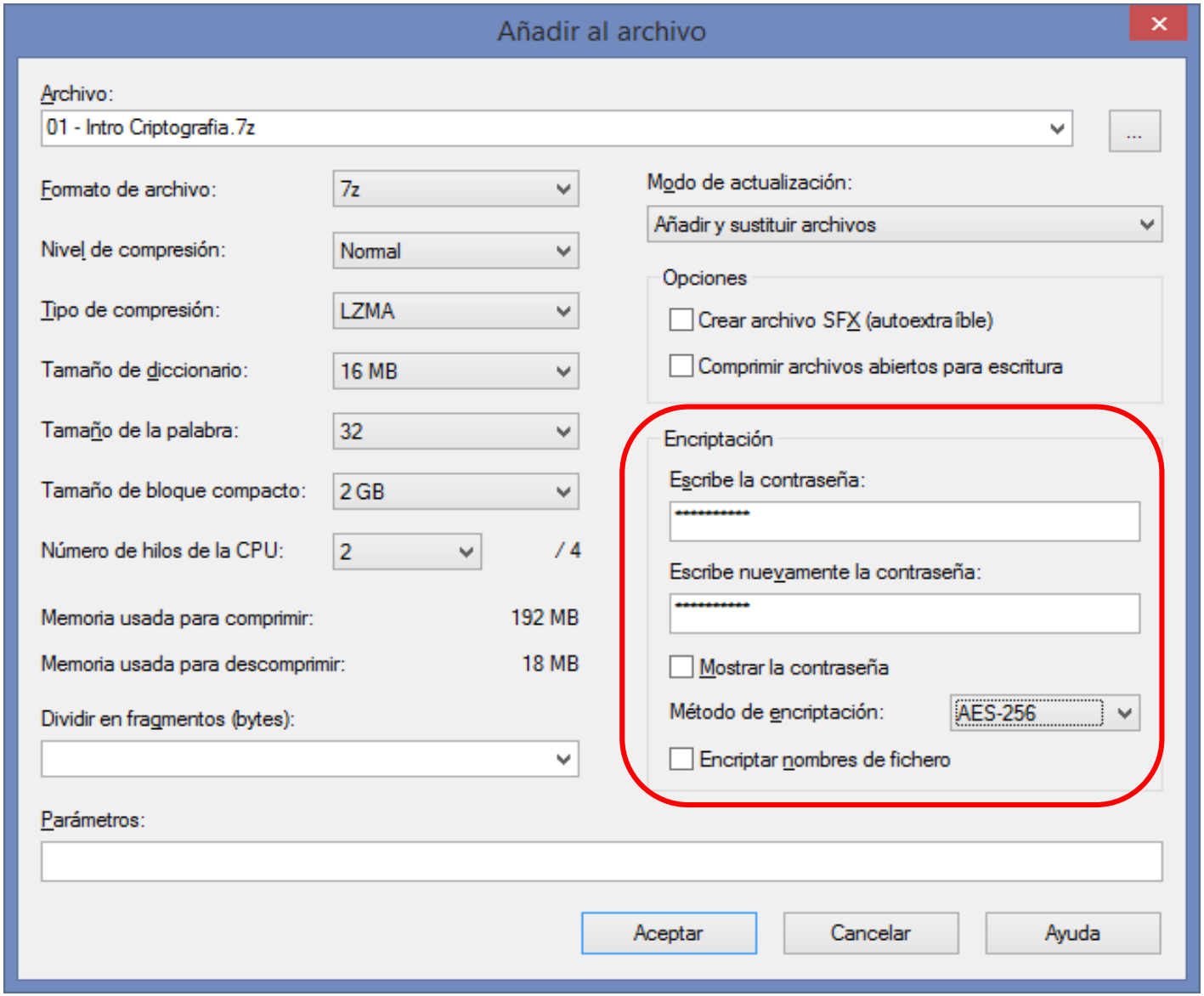
Ejemplo: Truecrypt



Ejemplo: Veracrypt



Ejemplo: 7z para compresión y cifrado



Criptografía en USA

- Prohibición de enseñar criptografía a extranjeros
  - La ley caducó en 2002
  - Se liberó la longitud de las claves

- ¿Dónde estaba el truco?
  - Ya estaban haciendo la captura de claves

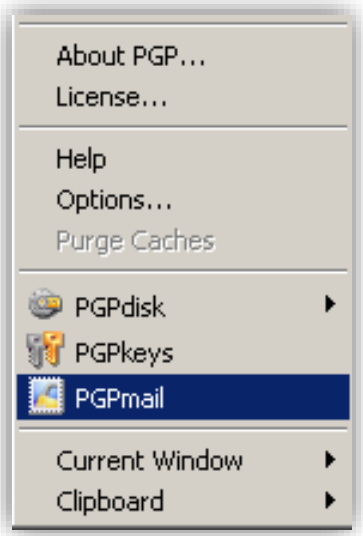
El rebelde

1991	• Crea PGP (Pretty Good Privacy)
1993	• Acusado de crimen federal
1995	• MIT Press lo publica en papel

Phil Zimmermann

PGP (Pretty Good Privacy)

- Protocolo para proteger la información local y para distribuir
- Facilita la autenticación de documentos con firmas digitales
- Utiliza cifrado simétrico y asimétrico
- El standard IETF es OpenPGP (RFC 4880)
- La versión libre es GPG (GNU Privacy Guard)



GnuPG (Gnu Privacy Guard)

- GnuPG es un reemplazo completo y libre para PGP
- Sin restricciones de uso al no incluir algoritmo IDEA (patentado)
- Cumple con el estándar OpenPGP (RFC 2440)
- La versión 1 fue publicada el 7 de septiembre de 1999
- Se distribuye bajo licencia GPL (www.gnupg.org)

Tipos de ataque según los elementos conocidos

Ciphertext-only attack (COA)	• El atacante solo tiene el texto cifrado
Known-plaintext attack (KPA)	• El atacante conoce un texto plano correspondiente
Chosen-plaintext attack (CPA)	• El atacante conoce un texto plano a elección
Chosen-ciphertext attack (CCA)	• El atacante conoce un texto cifrado a elección

Tipos de ataque según su naturaleza

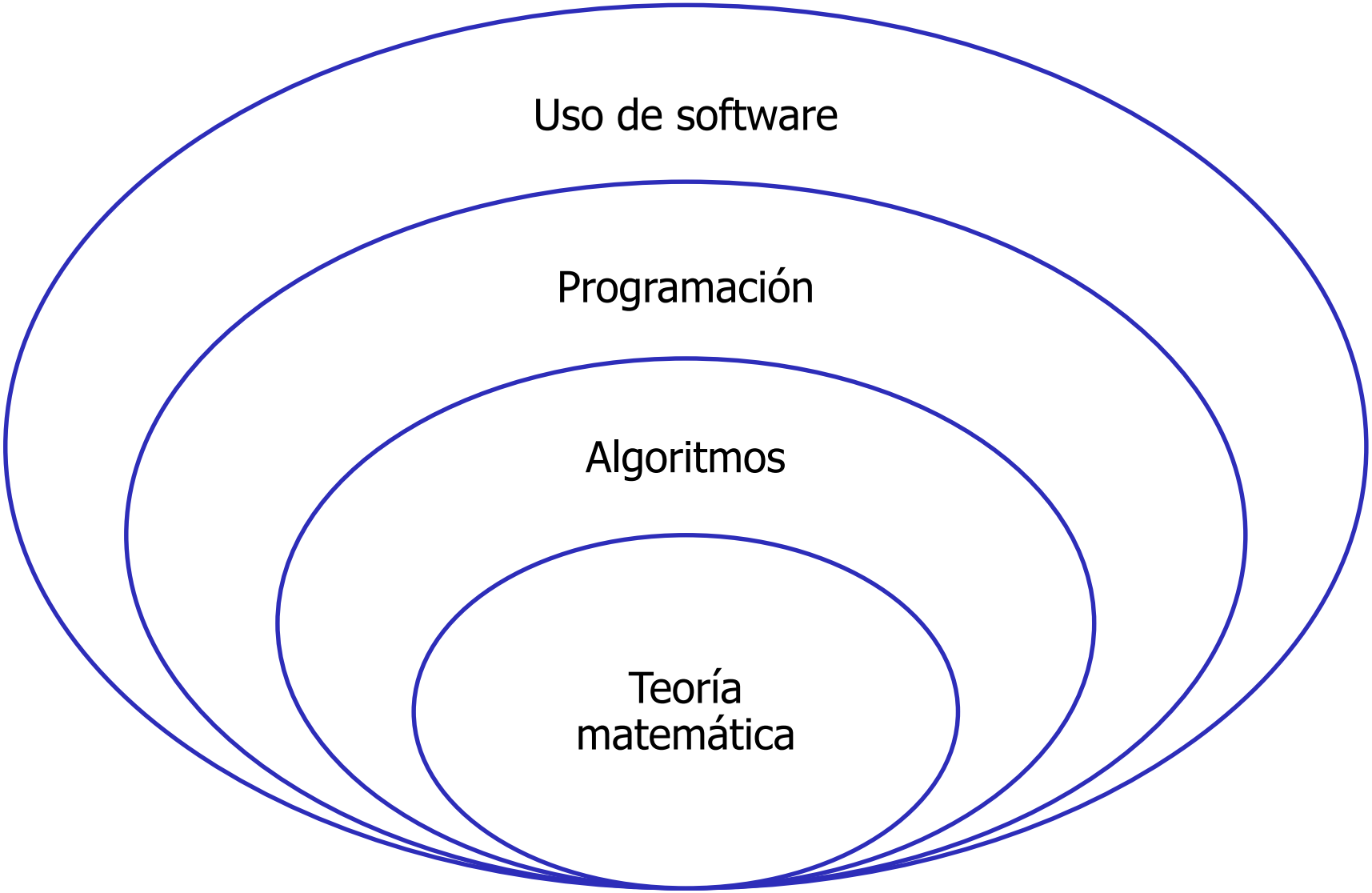
Fuerza bruta	• Se prueban todas las claves posibles
Analíticos	• Manipulación algebraica para reducir complejidad
Estadísticos	• Utilizan debilidades estadísticas del diseño
Implementación	• No atacan el algoritmo sino como fue implantado

Dudas razonables

- No sabemos si los sistemas están quebrados
  - Única opción: usar criptosistemas propios
  - Dos mundos: científico (todo público) y servicios de inteligencia (todo secreto)

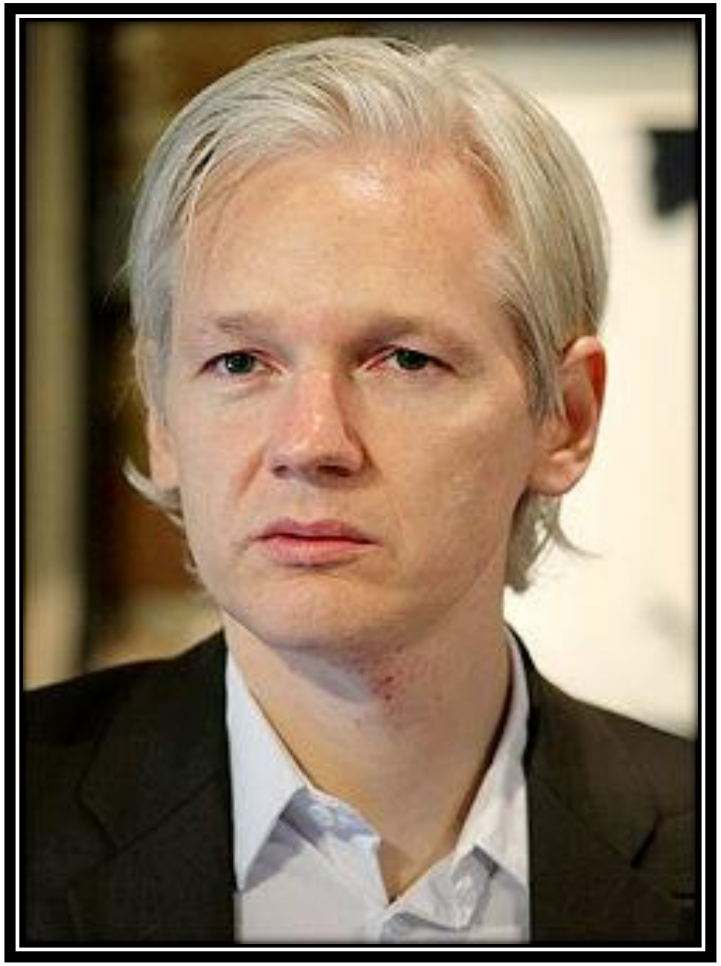
- No sabemos qué tan vulnerable es el software
  - Backdoors
  - Bugs + Exploits
  - Fuerza bruta

De la teoría al usuario: aspirar al buen uso



Criptografía y privacidad

"Lo único que puede devolver la privacidad a Internet es la criptografía"



Julian Assange

Resumen y conclusiones

- La criptografía permite transformar un dato legible en un criptograma
- Para descifrar un dato debe conocerse el algoritmo y la clave
- Se pueden proteger tanto los datos almacenados como en tránsito
- Existen distintos tipos de algoritmos dependiendo del uso
- La esteganografía permite ocultar datos dentro de otros datos
- Es fundamental el uso consciente de la criptografía

¿Preguntas?

Federico Pacheco

 @FedeQuark

 www.federicopacheco.com.ar

 info@federicopacheco.com.ar