¿QUÉ ES LA CRIPTOGRAFÍA?

Sofía Celi

¿QUIÉN SOY?

- Investigadora e implementadora de criptografía en Brave
- Trabajo en algoritmos post-quánticos, verificación formal y más!

https://sofiaceli.com/

AGENDA

- ¿Qué es la criptografía?
- Ejemplos de propiedades
- Ejemplos de aplicación
- El futuro en la criptografía

¿QUÉ ES LA CRIPTOGRAFÍA?

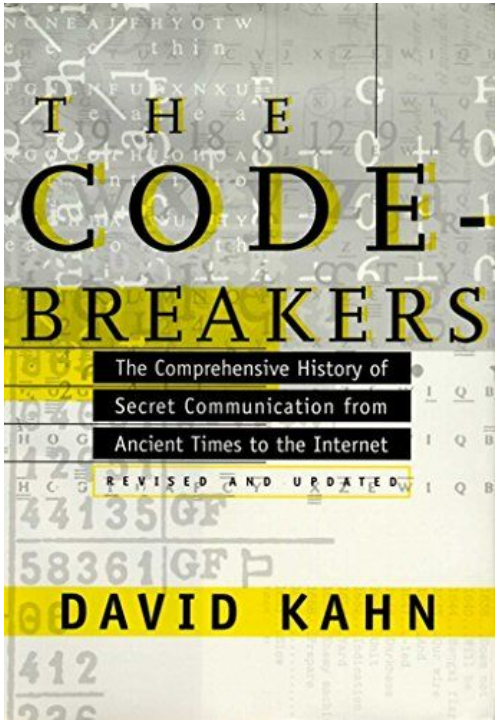
- Criptografía es la ciencia que **estudia** las **técnicas** para **hacer seguras** las **comunicaciones digitales** en **presencia de adversarios**

- **Estudia:** desde la teoría hasta la práctica
- **Técnicas:** algoritmos y protocolos
- **Hacer seguras:** no solamente seguridad en sí -> privacidad, integridad
- **Comunicaciones digitales:** cualquier data que es transmitida -> identidad, mesajes, metadata
- **Presencia de adversarios:** activos o pasivos -> ajenos a la comunicación

¿QUÉ ES LA CRIPTOGRAFÍA?

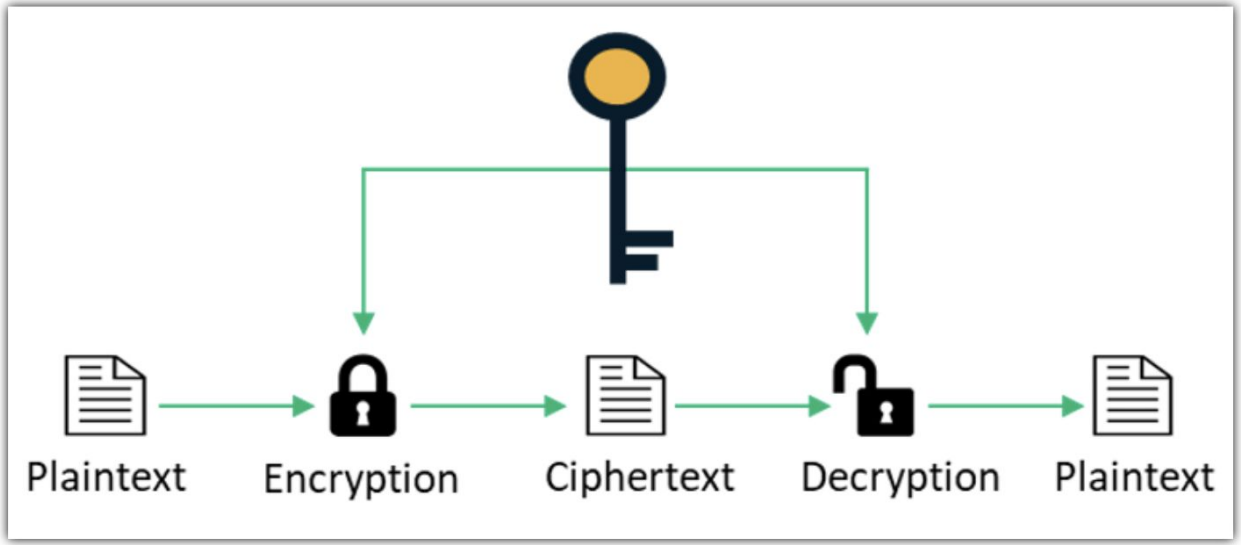
- En la antigüedad: encriptación para canales confidenciales

- “Code breakers”
  —-David Kahn, 1996



Criptografía simétrica

- Las llaves que tienen los participantes son las mismas.



Criptografía simétrica

- Las llaves que tienen los participantes son las mismas.

Alicia: K -> *cifrado := Enc(K, “hola”)*

Roberto: K -> *“hola” := Dec(K, cifrado)*

Criptografía simétrica

- Cifrado de sustitución

Alicia: K -> *cifrado := Enc(K, “hola”)*

Roberto: K -> *“hola” := Dec(K, cifrado)*

K := h -> t, o -> r, l -> q, a -> p

trqp := Enc(K, “hola”)

hola := Dec(K, “trqp”)

Criptografía simétrica

- Cifrado de César: desplazar 3 lugares (mod 26)

K := h -> k, o -> r, l -> o, a -> d

krod := Enc(K, “hola”)

hola := Dec(K, “krod”)

cifrado = Enc(x) = (x + n) mod 26

Criptografía simétrica

- Cifrado de César: desplazar 3 lugares (mod 26)
- Cuál es la letra más común en español?

K := a -> d, l -> o

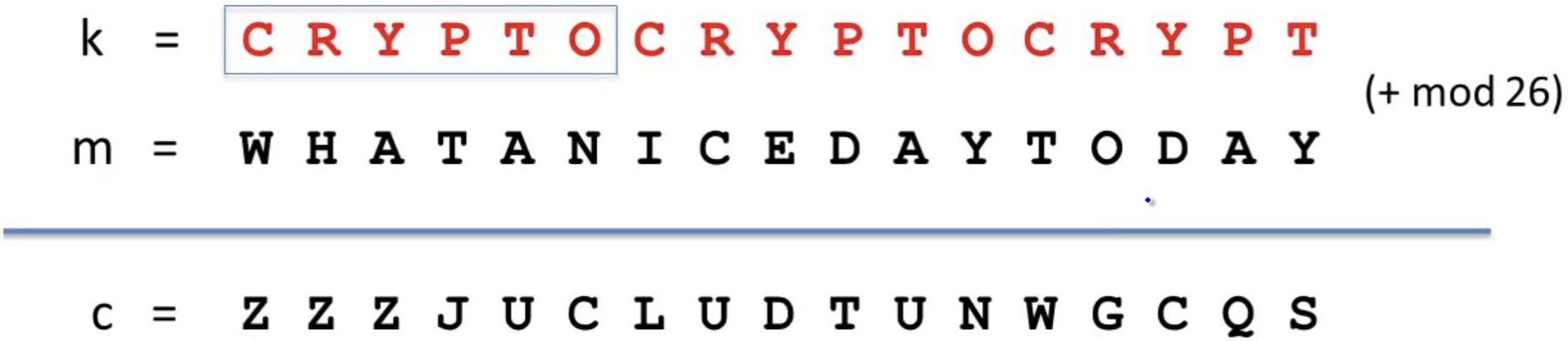
od pdqcdqd := Enc(K, “la manzana”)

la manzana := Dec(K, “od pdqcdqd”)

cifrado = Enc(x) = (x + n) mod 26

Criptografía simétrica

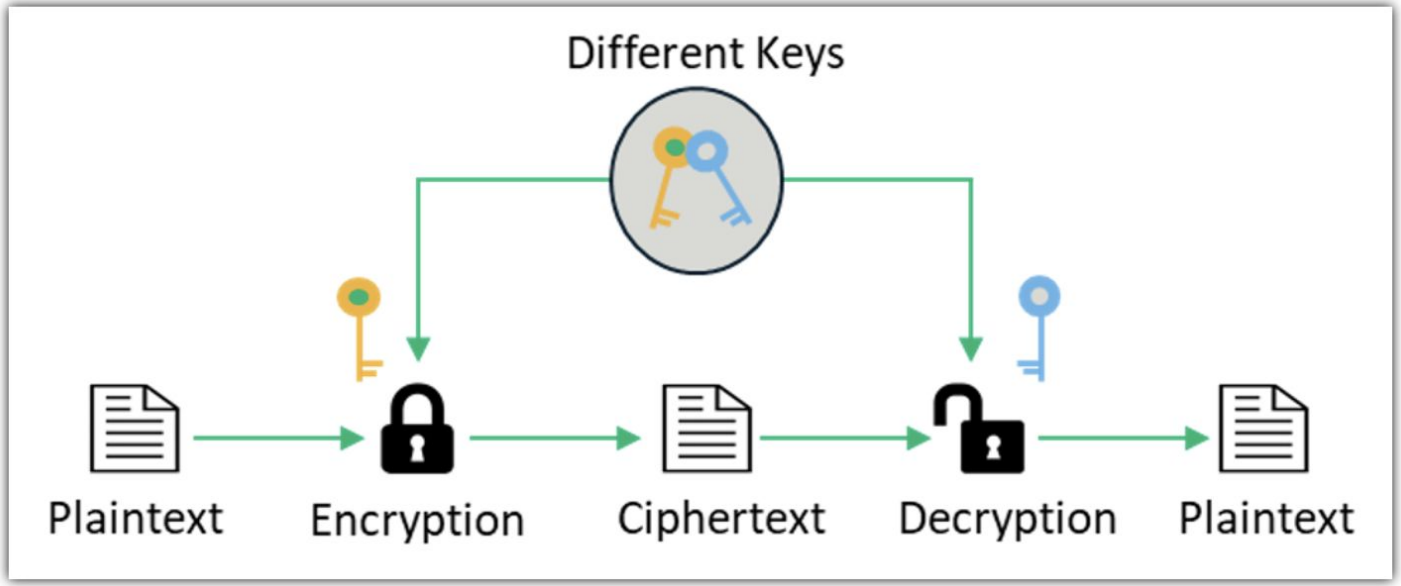
- Cifrado de Vigenère



Dan Boneh, History of Cryptography

Criptografía asimétrica

- Las llaves que tienen los participantes no son las mismas.



¿QUÉ ES LA CRIPTOGRAFÍA?

- Hoy: no solamente para la encriptación

- Ciencia de probabilidades:
  - Todo esquema puede ser roto pero:
  - se necesita de mucho tiempo y poder computacional

¿QUÉ ES LA CRIPTOGRAFÍA?

- Ahora: no solamente para la encriptación

- Ciencia de probabilidades:
  - Todo esquema puede ser roto pero:
  - se necesita de mucho tiempo y poder computacional
  - Basado en la dificultad del problema

LA COMUNICACIÓN

- Entren **actores/participantes**
- Mandado de **mensajes/metadata**
- A través de un **canal inseguro digital**
- Con un **código en común**

EN QUÉ CONSISTE

- En proveer de comunicación segura
- En poder establecer llaves que sean usadas para dicha comunicación segura

TIPOS DE PROPIEDADES

- **Confidencialidad**

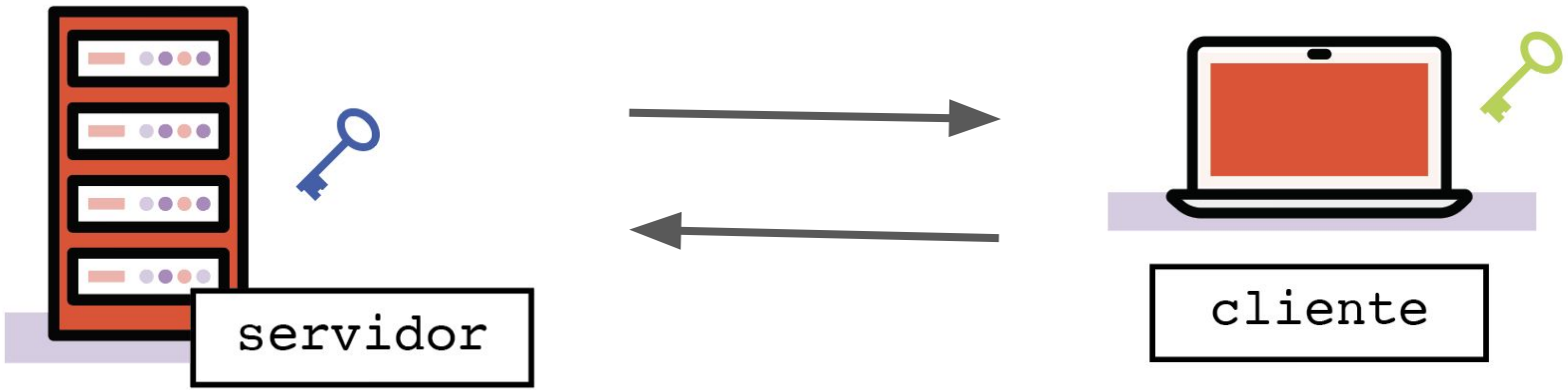
  La data transmitida puede ser solo leída por los participantes de la comunicación

- **Autentificación**

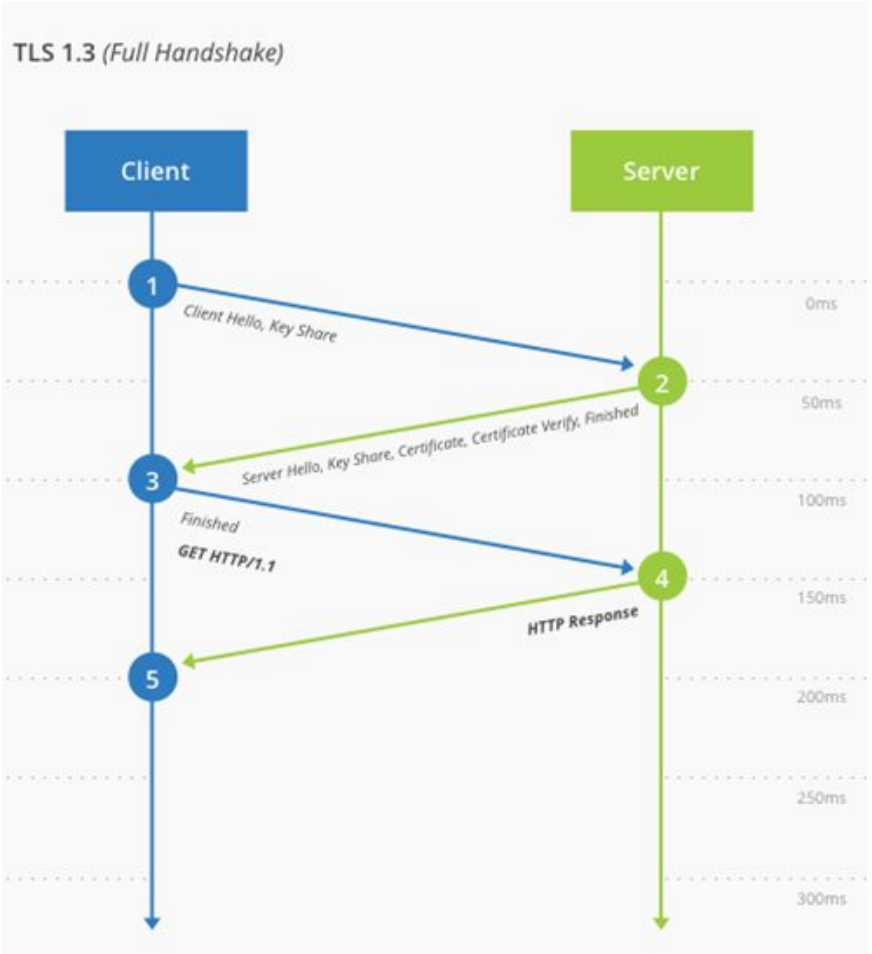
  Garantía de estar comunicándose con el participante adequado

- **Integridad**

  La data transmitida no puede ser modificada


servidor
cliente

UN EJEMPLO: TLS 1.3



UN EJEMPLO: TLS 1.3

- **Confidencialidad**

  mensaje = Desencriptar(cifrado, llave)
  cifrado = Encriptar(mensaje, llave)

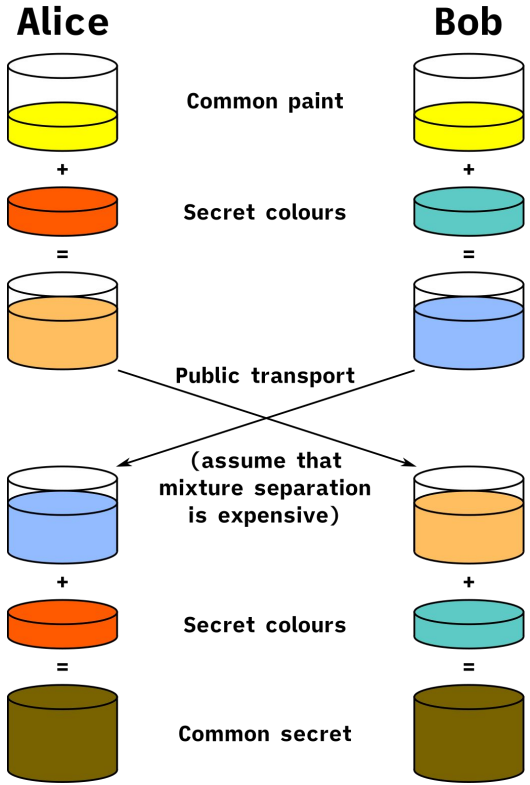
  Desencriptar(Encriptar(mensaje, llave), llave)

  Ejemplos: AES, ChachaPoly

UN EJEMPLO: TLS 1.3

- **Confidencialidad**

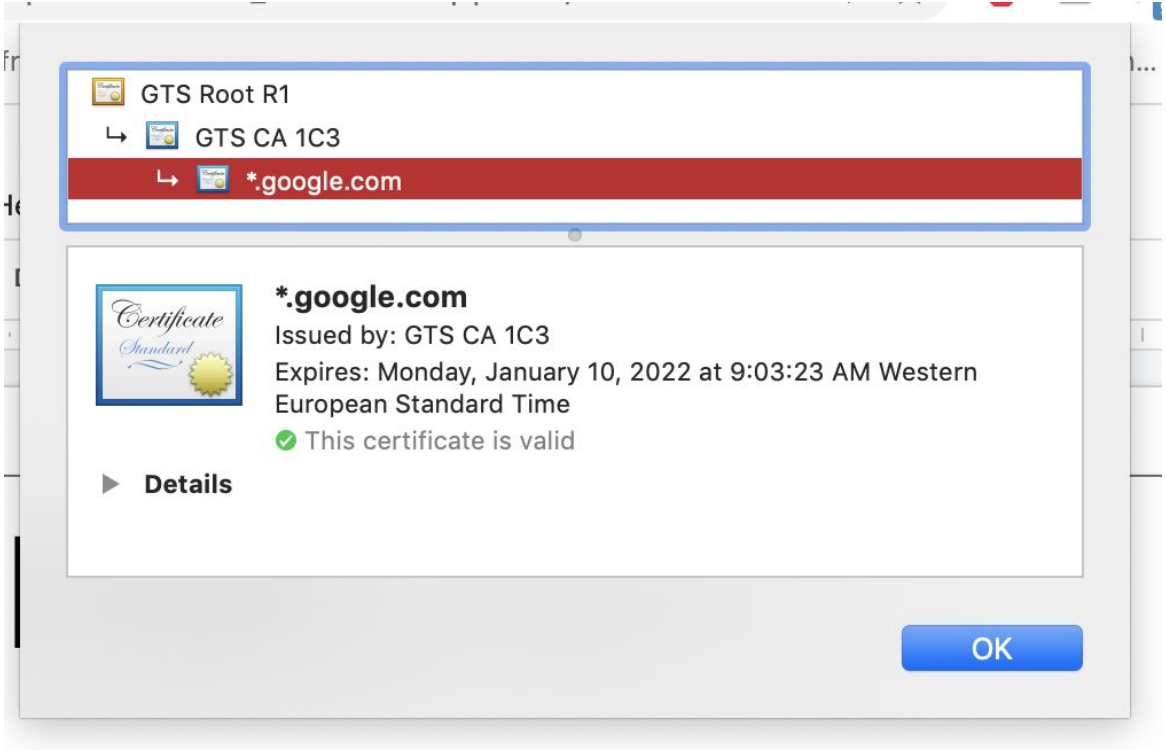
  Cómo se genera esta llave?
  Cómo se distribuye?
  Diffie-Hellman



UN EJEMPLO: TLS 1.3

- **Autentificación**

  Firmas digitales



TRES PASOS

1. Definir el modelo de amenazas: quién es el adversario?
2. Proponer una construcción
3. Provar que romper dicha construcción teniendo en cuenta el modelo de amenazas definido significa que hemos resuelto un problema computacional complicado

La criptografía es una ciencia rigurosa.

PODEMOS HACER MUCHO MÁS

- **Comunicación anónima**
  - **Dinero anónimo** (anonimato y doble gasto)
- **Private Information Retrieval**
- **Multi-Party Computation**
- **Zero-knowledge proofs**

EL FUTURO

Criptografía post-quántica
Privacidad
Implementaciones

GRACIAS!

@claucece