Criptografía para desarrolladores

Todo lo que necesitas saber para no fallar

Héctor Patricio (@hectorip)

Agenda

De qué hablaremos

1. ¿Por qué es **importante** la criptografía?
2. **Conocimiento básico** que todos los desarrolladores deberían tener
    a. **Conceptos** básicos
    b. **Primitivas** criptográficas
    c. **Protocolos** criptográficos
3. Cómo hacer que las **cosas salgan mal**
4. ¿Qué sigue para ti?

Uno de los **pilares del éxito** de un producto de software es su **seguridad**

Aprender a cómo y cuando usar las **herramientas criptográficas** te dará un punto de vista **ventajoso**

¿Por qué es importante la criptografía?

¿Qué es y por qué existe la criptografía?

Criptografía
Definición

- Viene del griego:
  - ***Kryptós*** *- oculto*
  - ***Graphein*** *- escritura*

  “Escritura Oculta”

- *El **arte de esconder** información*

“La criptografía es la antigua disciplina de hacer seguras situaciones problemáticas que tienen **actores maliciosos**”

David Wong - Real World Cryptography

La ciencia de defender protocolos **contra saboteadores**.

David Wong - Real World Cryptography

Siempre deberías estar pensando en quién está **interesado en robar tu información**.

La criptografía ha decido el resultado de **batallas** y ha hecho caer a **Reyes y Reinas**

Actualmente, nuestra **seguridad digital y autenticidad** de nuestras operaciones depende completamente de ella.

Nosotros, como constructores del mundo digital, estamos **obligados** a entender lo mínimo de lo que hace seguro un desarrollo.

“La vida es difícil, pero es más difícil si eres estúpido”

Conocimiento Básico

Tres Conceptos Importantes

¿Cómo puedo asegurarme que algo es lo que afirma ser?

Autenticidad

Verificar la identidad de alguien o algo.

No quiero que personas que tienen derecho se enteren de mi información. ¿Cómo le hago?

Confidencialidad

Ocultar información de entidades que no tienen derecho a saberla

(Find the lizard)

¿Cómo sé que nadie modificó la información que estoy recibiendo?

Integridad

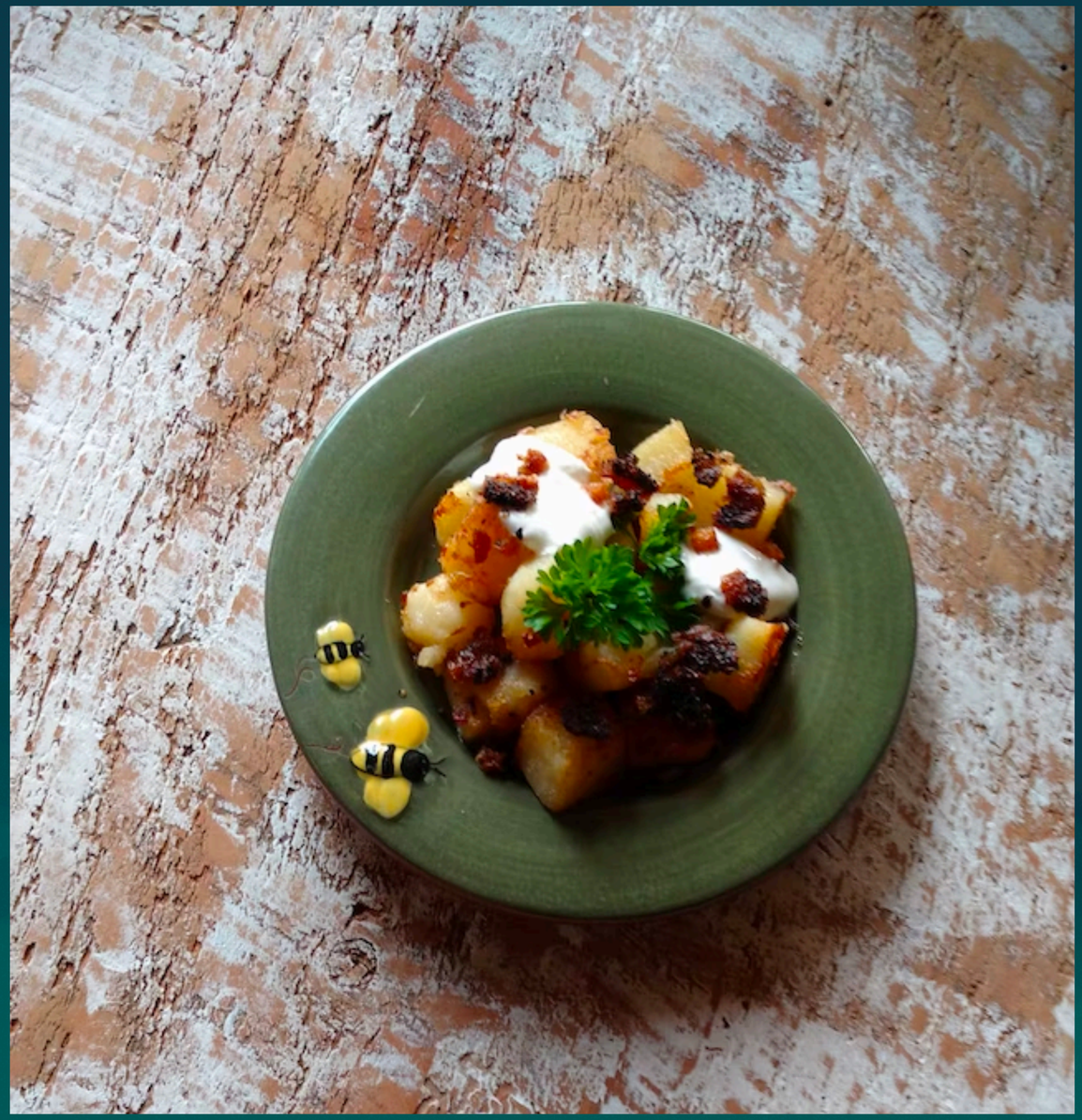
Saber que la información llegó exactamente como se mandó.

Primitivas Criptográficas

Funciones Hash

La navaja suiza de la criptografía.

- Funciones de un sólo sentido
- Normalmente devuelven salidas de tamaño fijo para cualquier entrada
- Se usan para construir protocolos y primitivas más complejas
- Son rápidas y mientras más rápidas, mejor



SHA3-256

Password Hashing

Si trabajas con usuarios, las necesitarás

- Mientras más lentas o costosas, mejor
- Deben ser difíciles de atacar usando software/hardware especializado
- Customizable
- Proveen mejor DX, al dar un buen conjunto de defaults que tienen sentido

Argon2 or bCrypt

Key Exchanges

Cómo compartir secretos con otros

- Permite generar secretos compartidos con un tercero
- Usados por todo internet

Cifrados simétricos

Los cifrados más fuertes

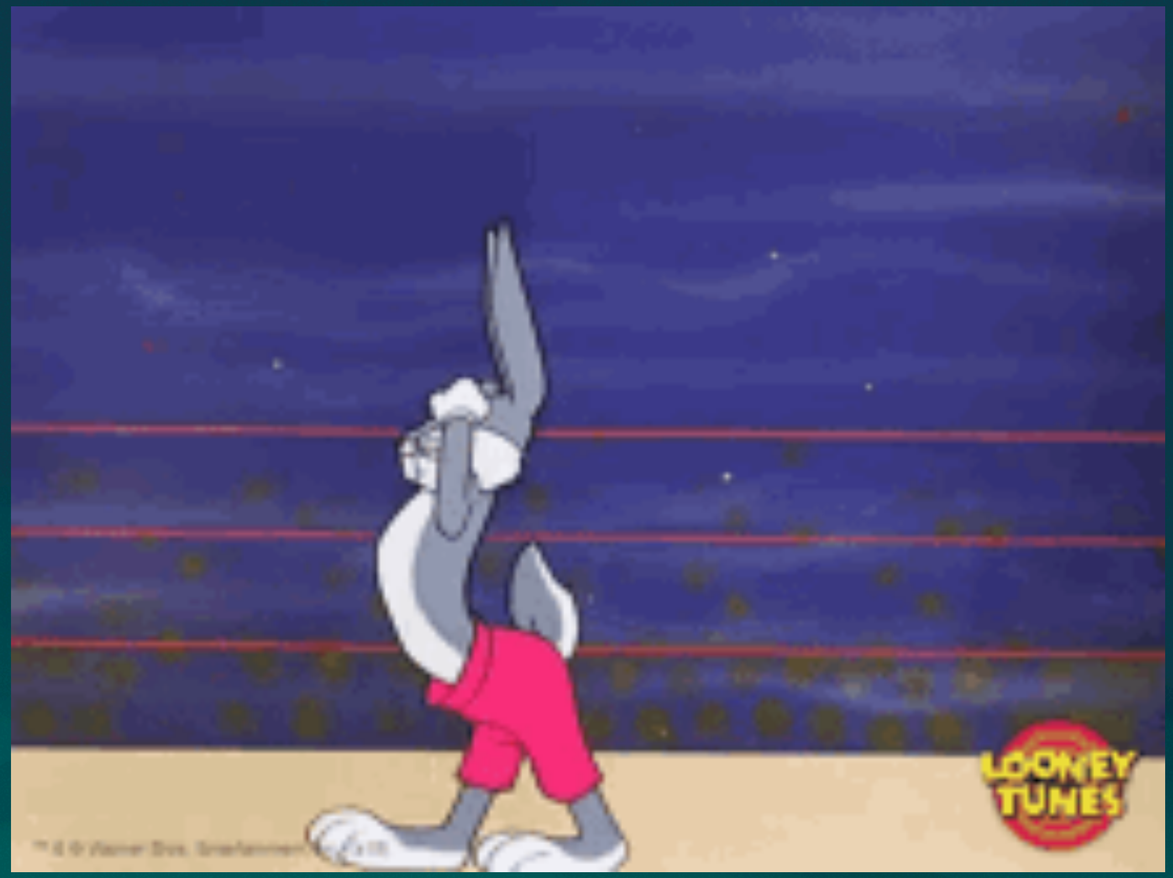
- Existen cifrados de bloque y de flujo
- El cifrado y descifrado se hacen usando la misma llave
- La seguridad depende de qué tan difícil es **encontrar la llave.**

AES-256

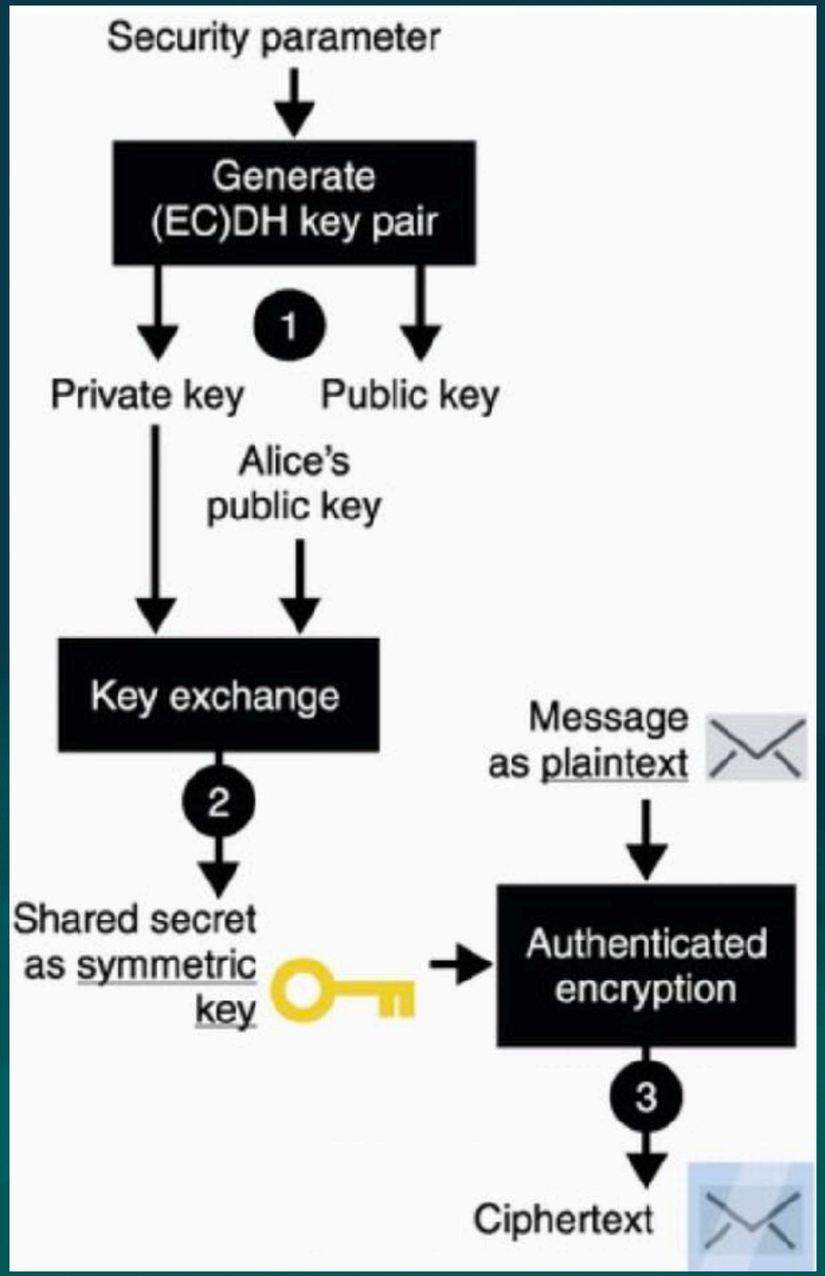
Cifrado asimétrico

Los cifrados más convenientes

- También se conocen como cifrados asimétricos
- Se usa una llave para cifrar y otra llave para descifrar
- Para dar la misma seguridad que un **cifrado simétrico** necesitan llaves mucho más grandes (ej. 2096)



RSA-OAEP
-
ECIES


Security parameter
Generate (EC)DH key pair
1
Private key
Public key
Alice's public key
Key exchange
2
Shared secret as symmetric key
Message as plaintext
Authenticated encryption
3
Ciphertext

Cifrado Autenticado

El más seguro y útil en la realidad

- Provee los tres valores: integridad, confidencialidad y autenticidad
- Es el tipo de algoritmos más usados para transmitir información en internet
- Combinan un tag de autenticación, el texto cifrado y a veces, datos asociados

AES-GCM
ChaCha20-Poly1305

Firmas digitales

Cómo compartir secretos con otros

- Funcionan como si fueran firmas en papel
- Garantizan autenticidad
- Con una firma digital puedes saber exactamente con quién estás hablando

ECDSA
EdDSA

¿Cómo te pueden salir mal las cosas?

Usando una fuente mala de **aleatoriedad**

Usando mal los algoritmos

Usando el algoritmo o protocolo incorrecto

¿Qué sigue para mi?

Real-World Cryptography

David Wong

MANNING

Serious Cryptography

A Practical Introduction to Modern Encryption

Jean-Philippe Aumasson

Foreword by Matthew D. Green

no starch press

RETO: Cryptopals Crypto Challenges