Conceptos

Introducción a la Criptografía y a la Seguridad de la Información

Iván Castellanos

Departamento de ingeniería de sistemas e industrial
Universidad Nacional de Colombia

3 de septiembre de 2019

Conceptos

$$\underset{\text{(secret)}}{\kappa\rho\upsilon\pi\tau o} - \underset{\text{(to write)}}{\gamma\rho\alpha\varphi\iota\alpha}$$

- «*Comunicación en la presencia de adversarios*» Ronald Rivest
- «*Una batalla intelectual entre un creador de código y un rompedor de código*» Simon Singh
- «*Estudio de técnicas matemáticas para lograr los objetivos principales de la seguridad de la información*» Handbook of applied cryptography

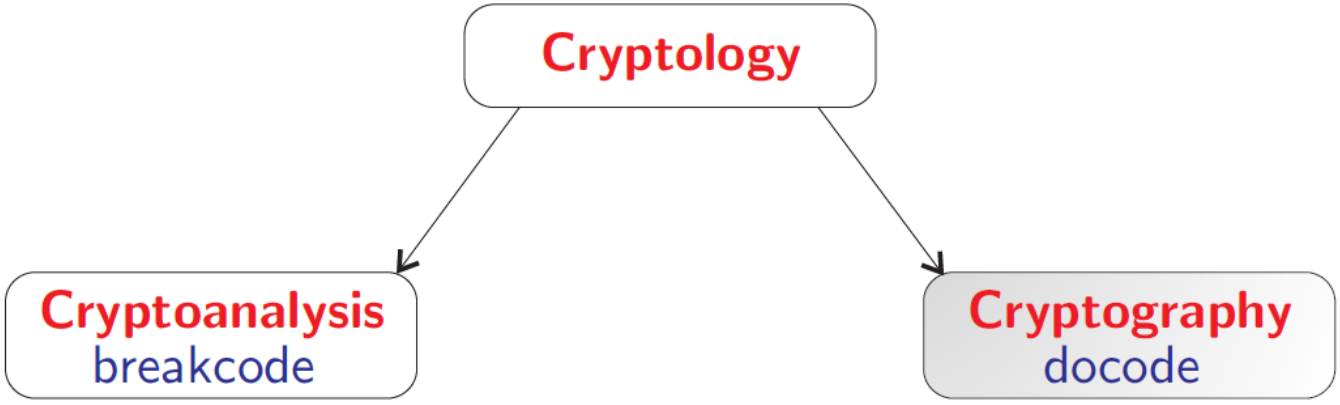
Conceptos

Definición (Criptoanálisis)

Es el arte de descifrar un mensaje encriptado (un secreto escrito)

Definición (Criptología)

Es la ciencia de codificar y decodificar mensajes



Conceptos

- El mensaje a enviar se llama *texto plano* (*plaintext*).
- El proceso de codificar un mensaje para esconder su contenido se llama cifrado (encryption).
- el mensaje encriptado se llama *texto cifrado* (*ciphertext*).
- El proceso de recuperar el texto plano de un texto cifrado se llama descifrado (decryption).
- El cifrado y el descifrado usualmente utilizan una *llave*

Personajes del curso

Existen muchos personajes con diversos roles en literatura sobre criptografía y seguridad de la información. Algunos de los más destacados son:

- *Alice y Bob*: son los chicos buenos, generalmente Alice quiere mandarle mensajes a Bob.
- *Eve*: (eavesdropper) una atacante pasiva, puede ver la comunicación entre Alice y Bob
- *Mallory*: (malicious attacker) también llamada Maggie, es una atacante activa. A diferencia de Eve, Mallory puede modificar mensajes, sustituir mensajes o responder mensajes viejos, entre otros.
- *Peggy*: Un probador
- *Victor*: Un verificador
- *Trudy*: Un intruso

Objetivos

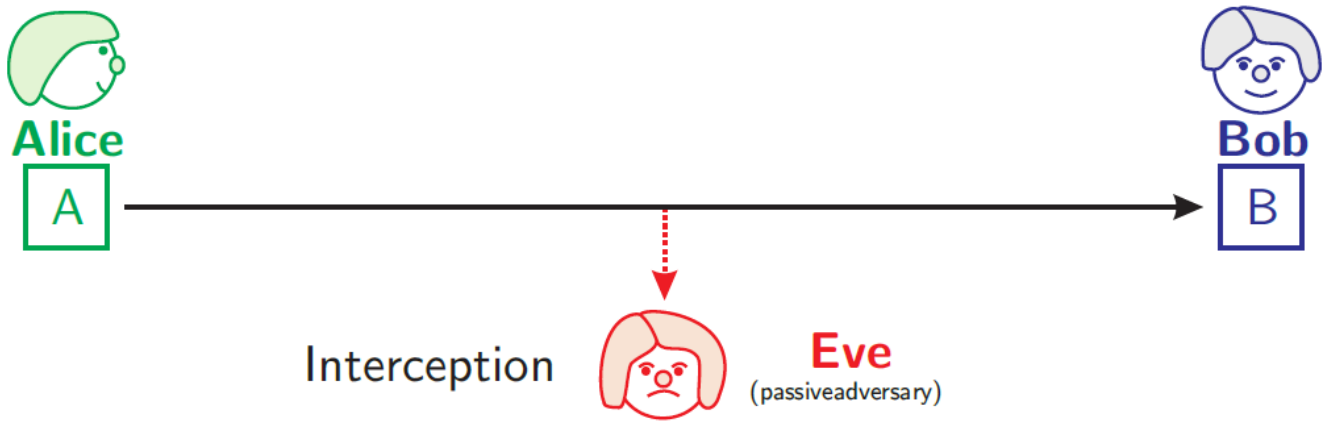
En la seguridad de la información queremos lograr las siguientes cosas:

- *Confidencialidad*: prevenir acceso desautorizado
- *Integridad*: prevenir la modificación de información existente
- *Autenticación*: identificación de entidades u origenes de datos
- *No-Repudio*: Prevenir la negativa de mensajes enviados/recibidos

Nota

Un objetivo principal de la criptografia es manejar estos principios en la teoría y en situaciones prácticas

Confidencialidad

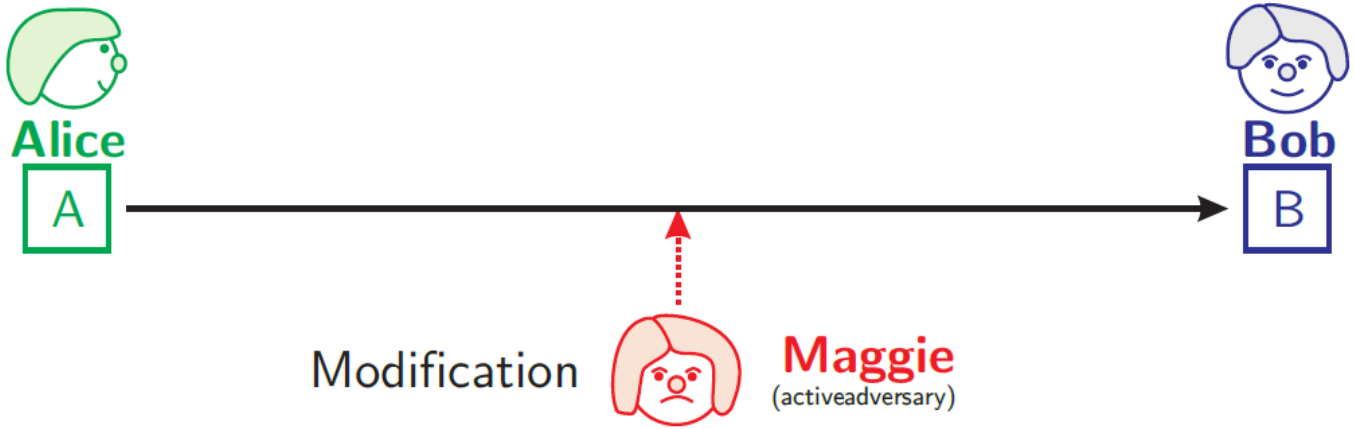


- Ningun observador puede acceder al contenido del mensaje
- Ningun observador puede identificar ni al remitente ni al receptor

Nota

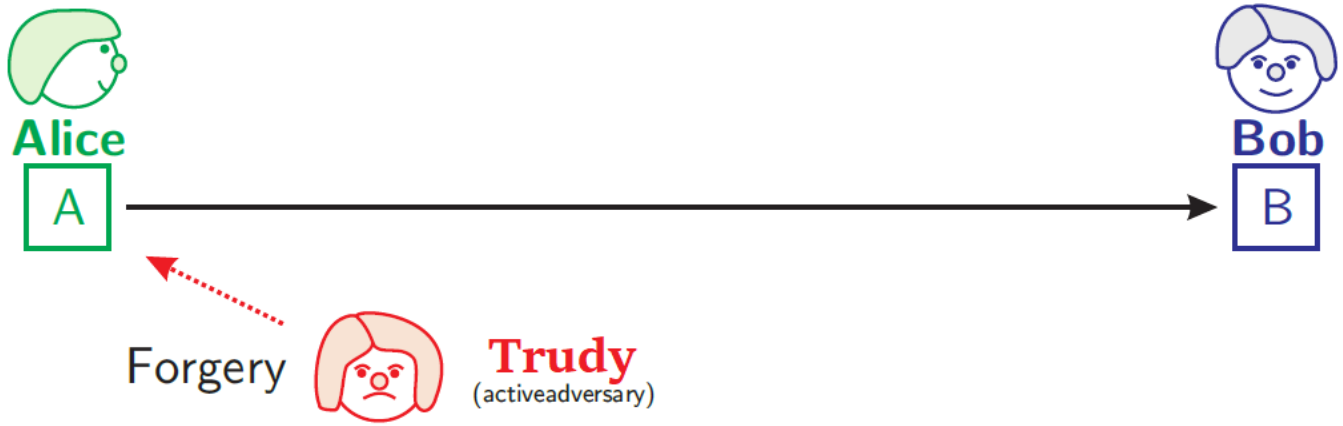
También se usan los términos seguridad y privacidad para esta característica

Integridad



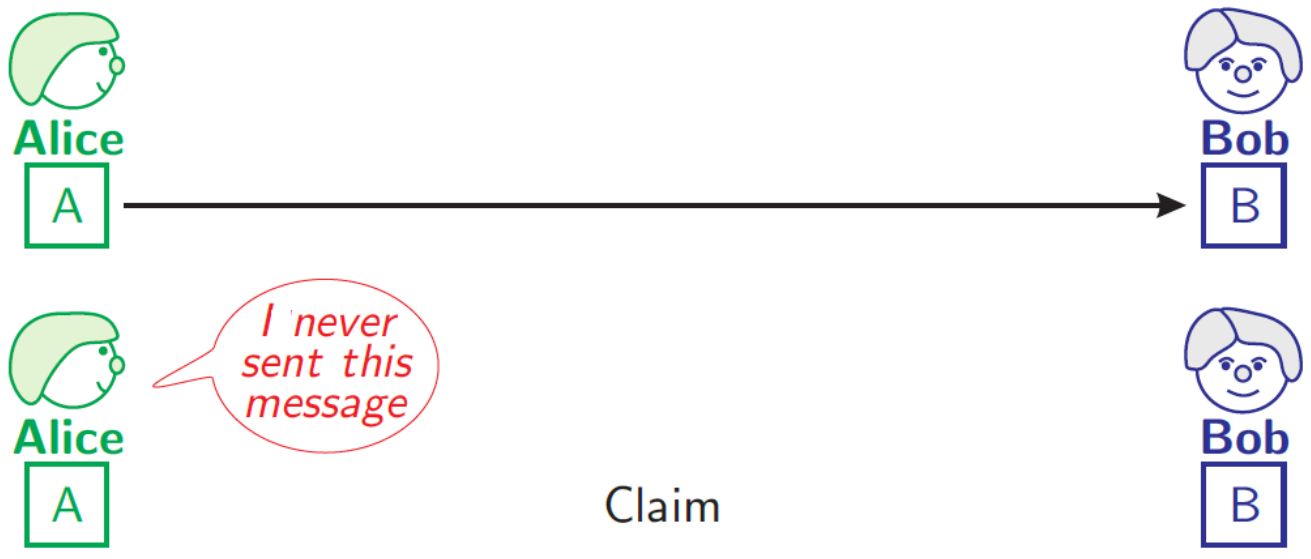
- El mensaje no se puede modificar durante la transmisión
- El mensaje le debe llegar al receptor
- El mensaje no le debe llegar repetidas veces al receptor

Autenticación



- El remitente puede estar seguro que el mensaje le llega únicamente al receptor indicado.
- El receptor puede estar seguro que el mensaje viene del remitente correcto y no de un impostor.

No-Repudio



- El remitente no puede negar que el mensaje fue enviado por él.
- El receptor no puede negar que el mensaje fue recibido por él.

Vulnerabilidades

- Cualquier información que logre tener el atacante puede vulnerar la seguridad de un usuario.

Ejemplo

La fotografia de la llave de una puerta, el sonido de las teclas al digitar una contraseña, información sobre el usuario 'atacado', etc.

Nota

Parte del trabajo de criptografía considera todos estos posibles escenarios.

Métodos de criptografía

- A lo largo de la historia se han desarrollado differentes métodos de cifrado que han sido *rotos* eventualmente.
- La implementación de los métodos de cifrado deben tener en cuenta cualquier vulnerabilidad qcon la que puedan ser *rotos* por un atacante.

Ejemplo

Una buena implementación previene ataques de canal lateral.

Nota

Se recomienda implementar los métodos de cifrado vistos en clase sólo con fines didácticos.

Métodos de criptografía

- Un método de cifrado *seguro* no es aquel que se trate de mantener oculto, sino uno que incluso siendo público sea dificil de romper (Principio de Kerckhoff).
- Cuando no se cumple lo anterior se dice que se tiene *seguridad por oscuridad*
- Lo que debe mantenerse secreto en el uso de los métodos es la llave.

Ejemplo

Sistema de apertura de puertas, sistema de caja fuerte, Sistema AES, etc.