UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Introducción al curso

Alan Reyes-Figueroa

Criptografía y Cifrado de Información (Aula 01) 08.julio.2021

Motivación

Este curso es una introducción al estudio de los métodos de criptografía, criptoanálisis y cifrado de la información.

En esta materia, estudiaremos de manera introductoria los principales métodos y protocolos actuales de cifrado, así como su correcta implementación computacional.

Objetivos del curso:

- Aprender cómo funcionan los diferentes métodos criptográficos principales.
- Aprender a usarlos correctamente. (Esto es importante porque la aplicación incorrecta conlleva brachas de seguridad).

Herramientas auxiliares

Esta es un área que integra varias ramas de la matemática y de la computación. Por ejemplo, haremos uso extensivo de

- álgebra lineal (matrices)
- teoría de números (divisibilidad, primos, congruencias)
- estadística
- probabilidd discreta
- teoría de la información
- algoritmos y estructuras de datos
- operaciones con bits
- protocolos de comunicación

Criptografía en todas partes

Comunicaciones seguras:

- tráfico web: HTTPS
- tráfico *wireless*: 802.11i WPA2, GSM, Bluetooth

Encriptamiento:

- de archivos: EFS, TrueCrypt

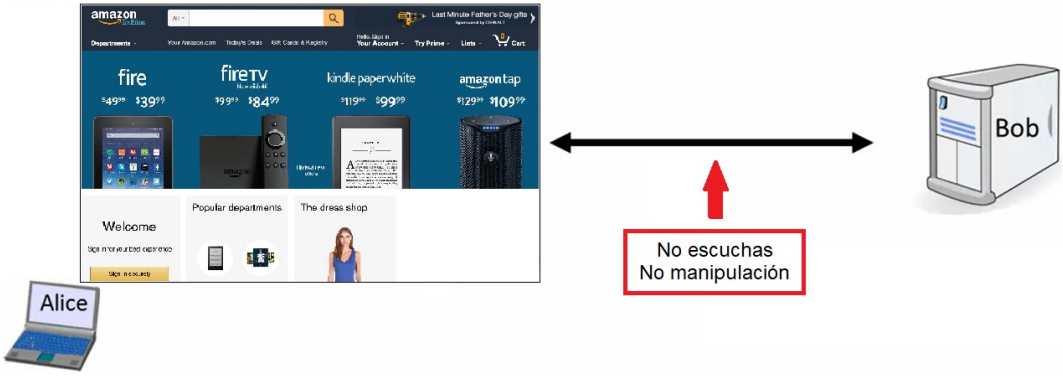
Protección de contenido:

- DVD Blu-ray
- CSS, AACS

Autenticación de usuarios:

- firmas digitales: DSA, TLS/SSL certificate

Criptografía en todas partes



Esquema de un protocolo criptográfico entre Alice y Bob: por ejemplo una laptop comunicándose con un *web server* mediante el protocolo HTTPS (SSL/TLS).

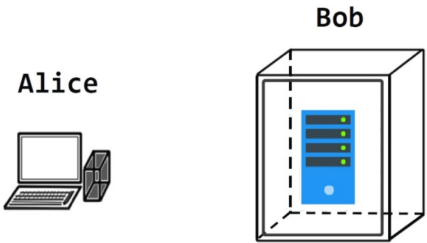
Criptografía en todas partes

SSL/TLS (Secure Sockets Layer):

Consta de dos partes:

1.

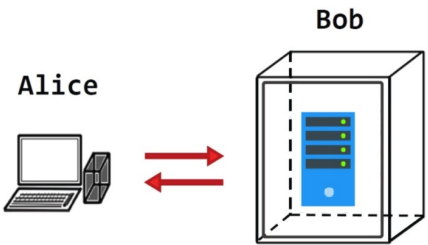
2.



Criptografía en todas partes

Consta de dos partes:

1. Protocolo de intercambio (*Handshake Protocol*), en el cual se establece una clave secreta **k** común usando métodos de criptografía de clave pública (2a. parte del curso).
2.



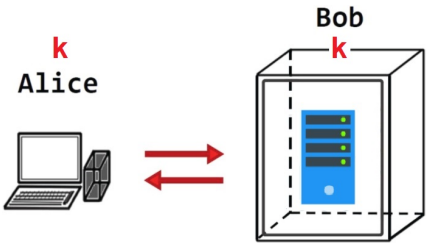
Handshake Protocol

Criptografía en todas partes

Consta de dos partes:

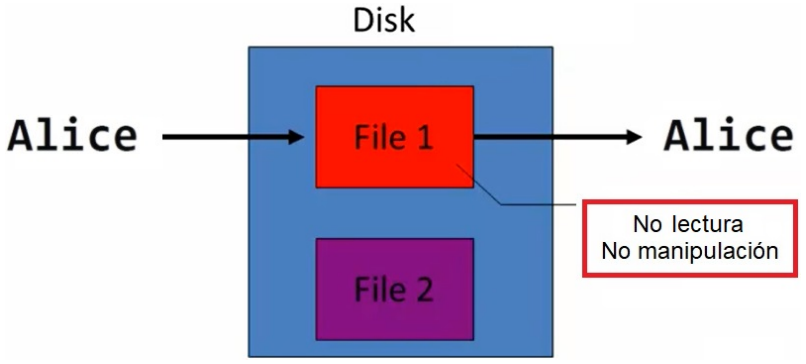
1. Protocolo de intercambio (*Handshake Protocol*), en el cual se establece una clave secreta **k** común usando métodos de criptografía de clave pública (2a. parte del curso).

2. Envío de información, donde se transmiten datos usando la clave compartida **k**, asegurando la integridad y confidencialidad del mensaje (1a. parte del curso).



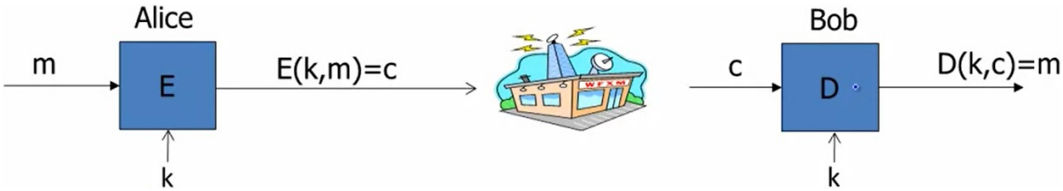
Establecen clave común **k**

Criptografía en todas partes



Esto es análogo a una comunicación segura entre dos partes, *e.g.*:
si Alice de hoy le envía un mensaje a la Alice del futuro.

Encriptado Simétrico



- (E, D) es el cifrado. $E = E(k, m)$ y $D = D(k, c)$ son funciones.
  E se llama la función de encriptado (*encrypter*), D la función de descriptado (*decrypter*).
- $m =$ mensaje plano (*plaintext*), $c =$ mensaje cifrado (*ciphertext*),
- $k =$ es la clave privada (*key*).

- Los algoritmos de encriptado son públicos.
- **Nunca usar métodos de encriptado propios!!!**

Formas de Uso

Claves de un solo uso: (*one-time keys*)

- La clave se usa una única vez para encriptar un mensaje.
- Ejemplo: *Email encryption*

Claves de uso múltiple: (*many-time keys*)

- La clave se usa para encriptar múltiples mensajes.
- Ejemplo: *File encryption*
- Este tipo de claves requieren una maquinaria más sofisticada y compleja para asegurar la seguridad del cifrado.

Criptografía en todas partes

Importante recordar:

Criptografía es:

- una herramienta muy útil
- la base para muchos mecanismos de seguridad

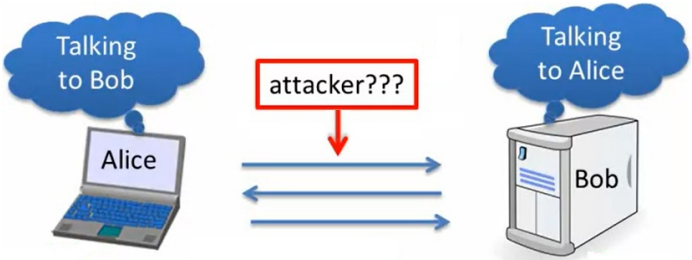
Criptografía no es:

- la solución a todos los problemas de seguridad (*sotfware bugs*, ataques de ingeniería social)
- confiable, a menos que se implemente y se use correctamente (*e.g.* WEP para comunicaciones Wifi)
- algo que debes tratar de inventar por tí mismo (muchos muchos ejemplos de implementaciones *ad-hoc* deficientes).

Aplicaciones

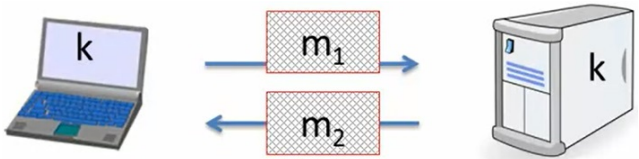
- Intercambio de claves **k**

- Asegurar comunicaciones



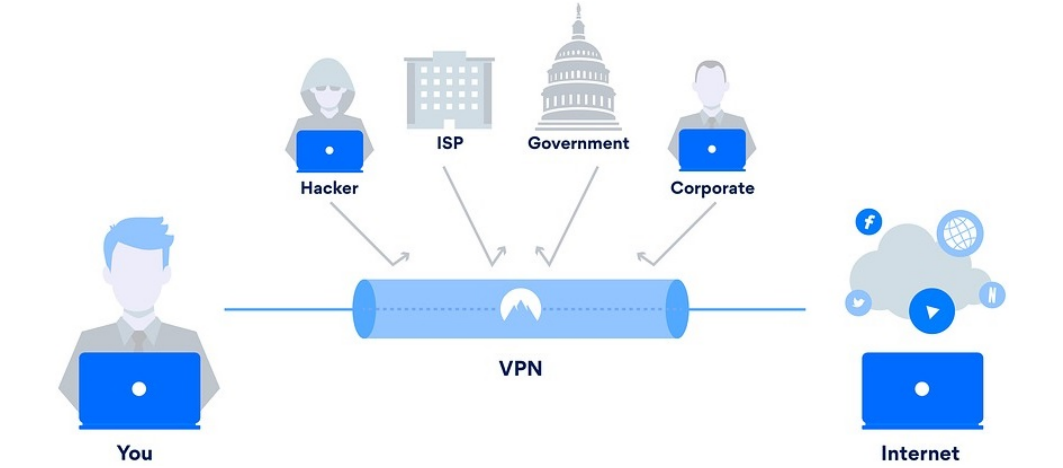
Aplicaciones

- Asegurar comunicaciones



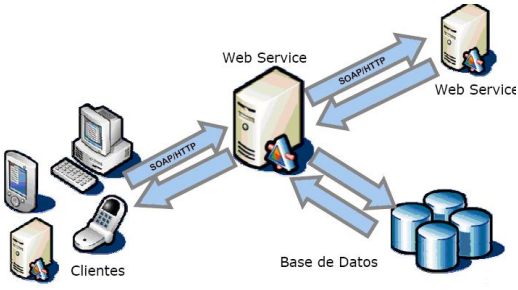
Aplicaciones

- Asegurar comunicaciones



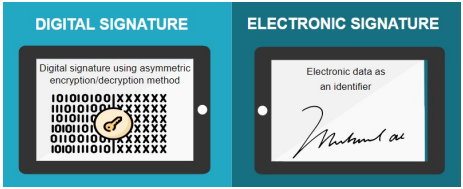
Aplicaciones

- Seguridad de información



Aplicaciones

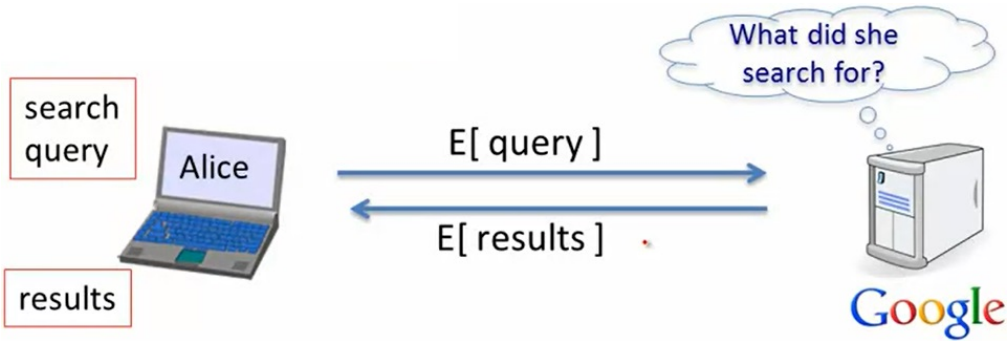
- Firma digital



- Comunicación anónima

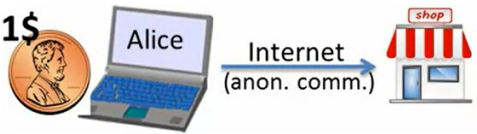
Aplicaciones

- Comunicación anónima (*privately outsourcing computation*)



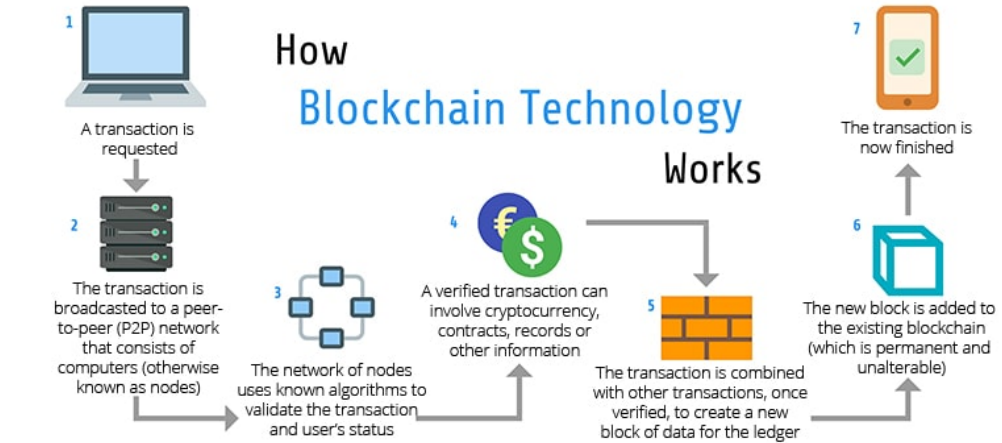
Aplicaciones

- pago digital
  - gastar/pagar dinero de forma anónima
  - prevenir doble uso de moneda



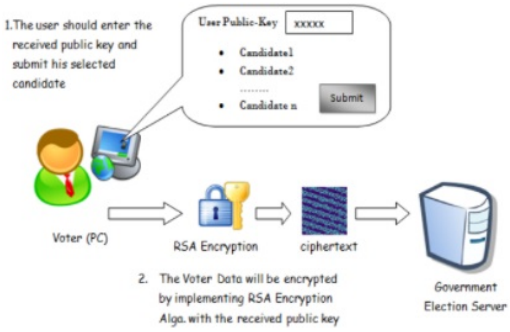
Aplicaciones

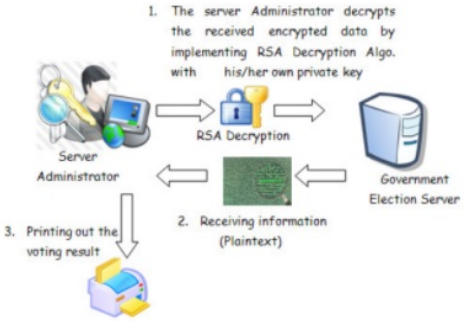
- pago digital



Aplicaciones

- Sistemas de elecciones
- Subastas





Aplicaciones

Estos son casos particulares de lo que se conoce como “computación segura de múltiples partes” (*secure multi-party computation*).

- partes: $x_1, x_2, \ldots, x_n$
- queremos calcular $f(x_1, x_2, \ldots, x_n)$, pero nada más
- uso de una **autoridad confiable** (*trusted authority*).

Teorema

Todo lo que se puede hacer mediante una autoridad confiable, se puede hacer sin ella.

En lugar de ello, las partes se comunican sin revelar información, mediante protocolos criptográficos. Al final de que todos se comunican, se conoce $f(x_1, x_2, \ldots, x_n)$.

Criptografía

La criptografía es una ciencia rigurosa. Típicamente, proponer un nuevo método o protocolo criptográfico implica tres pasos:

1. Especificar con precisión un modelo de amenaza.
2. Proponer una construcción.
3. Demostrar (matemáticamente/algorítmicamente) que romper la construcción bajo el modelo de amenaza, equivale a resolver un problema difícil (NP hard).