Índice:

Temario

Encriptación

- Ver como tanto simétrico como asimétrico logran comunicaciones seguras, asegurando los 3 pilares + el no repudio. Desde un punto de vista teórico-práctico.
- Certificados con OpenSSL.

Seguridad en el Stack TCP/IP

- Y Man in the Middle.

Tunneling y VPN

- Tunneling en Layer 3.
- **IPSec:** Parte teórica (modos de cifrado, capas, Diffie-Hellman, generación de claves, implementación).

Block-chain

- Como funciona a nivel de encriptación.

Forense

- Recuperación de datos.
- Preservación de datos.
- Hacer firmas digitales.
- Un poco de como se hace en dispositivos móviles.

Zero trust

- **Antes:** bastión y río con cocodrilos y chau.
- **Después:** no se puede confiar en nadie porque después del bastión están los humanos. Seguridad en cada micro-servicios.

Criptografía

Definición: Conjunto de técnicas utilizadas para proteger información confidencial de personas no autorizadas.
Sus ramas son:

- **Criptología:** Se dedican al estudio de la escritura secreta, a las formas de codificación.
- **Criptoanálisis:** Busca vulnerabilidades en los sistemas criptográficos y acceder a la información secreta sin disponer de las claves.
- **Criptografía aplicada:** Ver como los algoritmos permiten brindar servicios de seguridad, sin reparar demasiado en la teoría.
  Podemos clasificarlas según su época histórica:
- **Criptografía clásica:** Formas de transformar un mensaje para hacerlo ilegible a un supuesto atacante, en la época previa a la computación. Sus algoritmos se basan en la transposición y la substitución.
- **Criptografía moderna:** A mediados de los 70'. Implementa algoritmos matemáticos computarizados para transformar el texto.

La criptografía hoy en día se usa mucho como la base de las comunicaciones en los datos o en la transferencia de los mismos, sobre todo en Internet. TLS (Transport Layer Security) es una capa criptográfica que asegura la comunicación de protocolos de capa superior (como HTTP).
Se ve criptografía en ambientes como:

- SaaS.
- Herramientas Ofimáticas online.
- Herramientas de Trabajo Colaborativo.
- Plataformas de Compra-Venta online.
- Pasarelas de pago.
- Transacciones con tarjetas.
- Tareas de Sysadmin:

- SSH.
- Túneles VPN.
- Plataformas de observability.

Algunas definiciones:

Seguridad de la información:

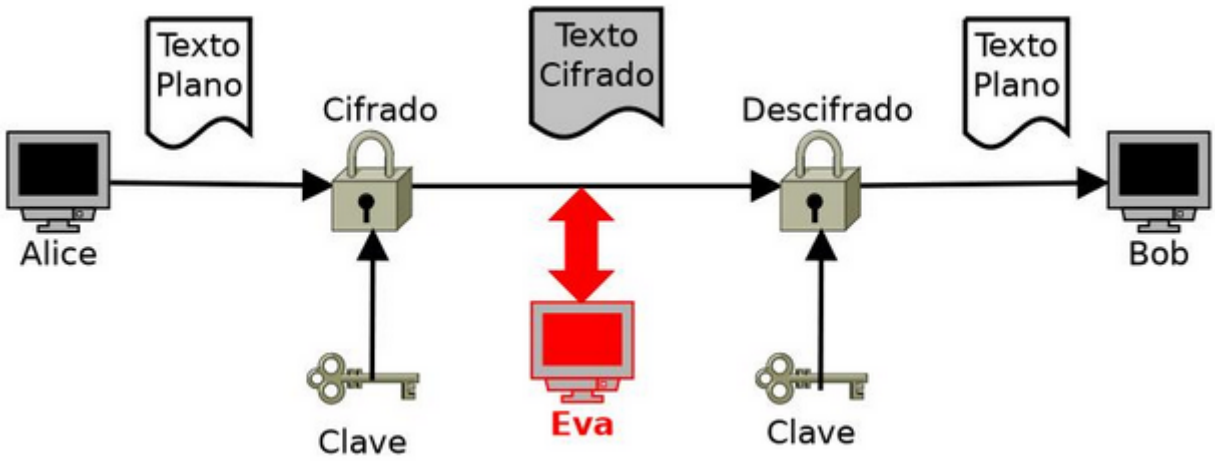
Métodos y procesos destinados a **proteger** los **archivos de información** en general, no necesariamente sobre medio informático.

Seguridad informática:

Métodos y procedimientos técnicos para lograr la **confidencialidad**, **disponibilidad** e **integridad** de la información. Si se trata de comunicaciones seguras en red, puede añadirse otra propiedad: la **autenticación** de la información, y su característica asociada, el **no repudio**. También lo son las prácticas de **prevención de ataques** maliciosos a la infraestructura en cuanto a estaciones de trabajo, servidores, dispositivos activos, redes, dispositivos móviles, sistemas de almacenamiento, etc.

Criptosistema:

Incorpora todos los elementos de un sistema criptográfico necesarios para lograr la seguridad en una comunicación.



Tenemos un emisor, un receptor y un atacante que intenta interceptar la comunicación y vulnerarla.

Seguridad en las comunicaciones:

- Básico para ser segura que tenga:
  - ***Confidencialidad*** → Con cifrado simétrico o asimétrico. Que solamente las entidades autorizadas puedan acceder al contenido de la información.
  - ***Autenticidad / no repudio*** (Que se logran a la vez) → El receptor comprueba que efectivamente recibió un mensaje del emisor (y que ese

emisor quería mandarle un mensaje) y nadie lo está impersonando. Y con no repudio, el emisor no puede negarse a que envió ese mensaje y no puede 'desentenderse' de la situación. Es característica derivada de la autenticación.
    - ***Integridad*** → Verifico si el mensaje se modificó / adulteró por algún error (ej. en el canal de comunicación) o atacante (cambios intencionales).
    - (***Disponibilidad*** → Si se necesita acceder a la información se debe poder hacerlo cuando se la requiera. Es una propiedad más general).
    - (Funciones resumen / hash).[1]
- Para cifrados simétricos se recomienda AES > 256b y en asimétrico RSA > 2048b.
- **La codificación** tiene función inversa y no necesita clave, solo necesitas saber como se hace. Ej. Base64 en correo para mandar binarios (como PDF) que no es carácter, porque el mail solo funciona con caracteres. Envío de mensajes, no secretos.
- **El hash** no tiene inversa y transforma un input en una cadena de largo fijo de bits sin rastro de la información original. Puede haber colisión de hash. Integridad
- **Cifrado:** Tiene función inversa, pero necesita de una clave. Se puede usar 1 clave (cifrado simétrico, para cifrar y descifrar) o 2 claves (asimétrico, una y una). Seguridad

El cifrado asimétrico es muchísimo más lento que el simétrico. El asimétrico se utiliza para intercambiar la clave simétrica → Criptografía hibrida y encapsulamiento de claves

> ¿Qué diferencia hay entre la integridad TCP/IP e integridad en criptografía?
>
> En TCP/IP se utiliza el CRC para ver que la cantidad de bits sea igual a la cantidad de bits enviados, por lo que si coincide, en teoría no habría ningún cambio. El mismo CRC aplica distintos métodos en casos de que no esté la misma cantidad de bits, de tal manera que se pueda corregir el error. La diferencia con la integridad de la seguridad informática es que esta, en caso de que se haya modificado el mensaje, uno se da cuenta de dicha modificación, en cambio, con TCP/IP, no hay nada que te asegure que el dato no haya sido modificado. Ambos sistemas pueden ser atacados por personas(dato a saber).

After break

Hacemos una práctica con OpenSSL:

- Para hacer hashes con md5 o sha3-512

```
echo "hola" | openssl dgst -sha3-512
openssl dgst -sha3-512 /etc/algo.txt
```

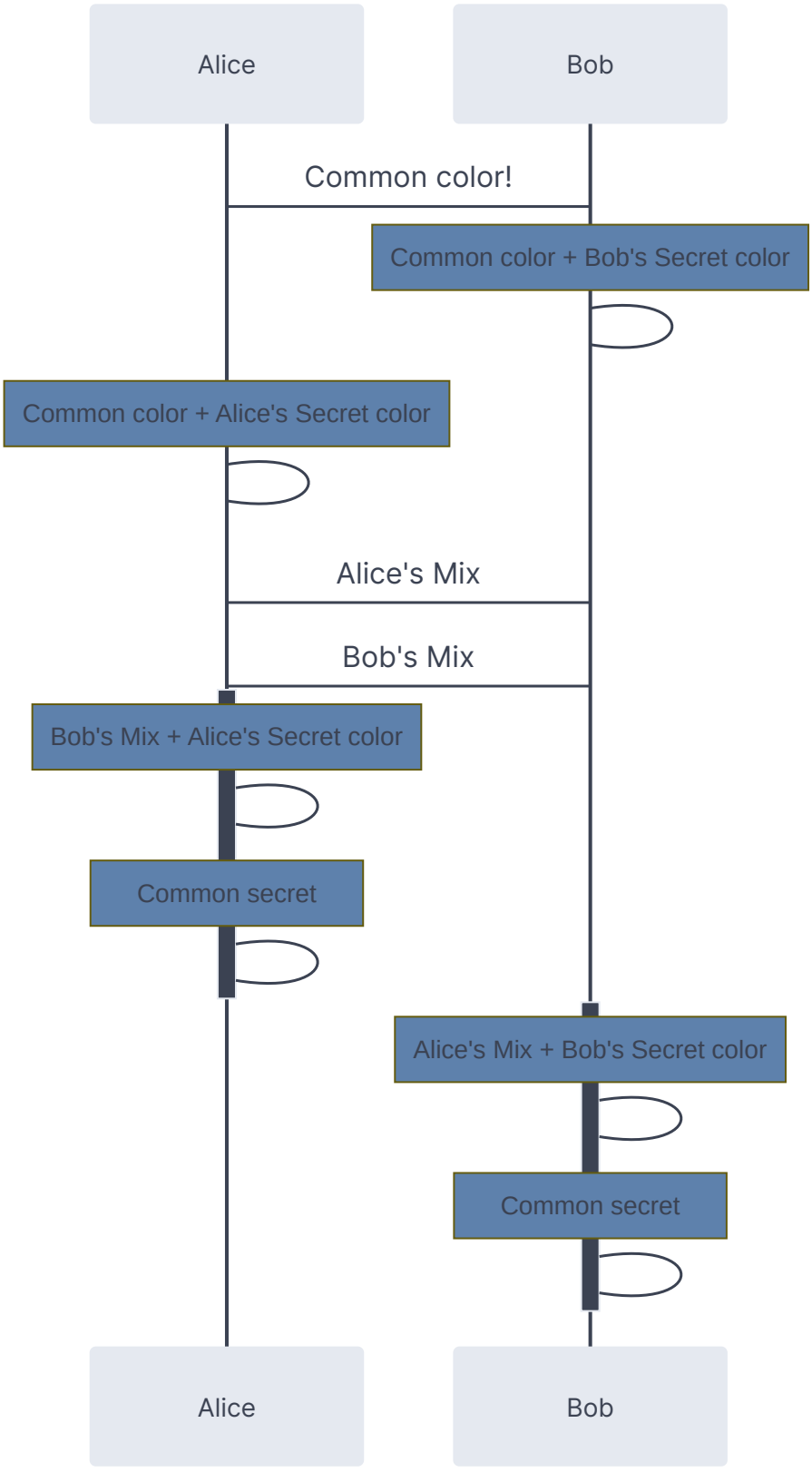
Intercambio de claves:

Si empleamos criptografía simétrica, ¿Cómo hacemos que se intercambien la clave que van a utilizar en un canal inseguro, sin que el atacante se percate?
Ejemplos: Diffie-Hellman, variantes de curva elíptica (ECDH), sincronización de redes neuronales artificiales (criptografía neuronal), algoritmos de computación cuántica (Intercambio de claves cuántico, QKE), etc.

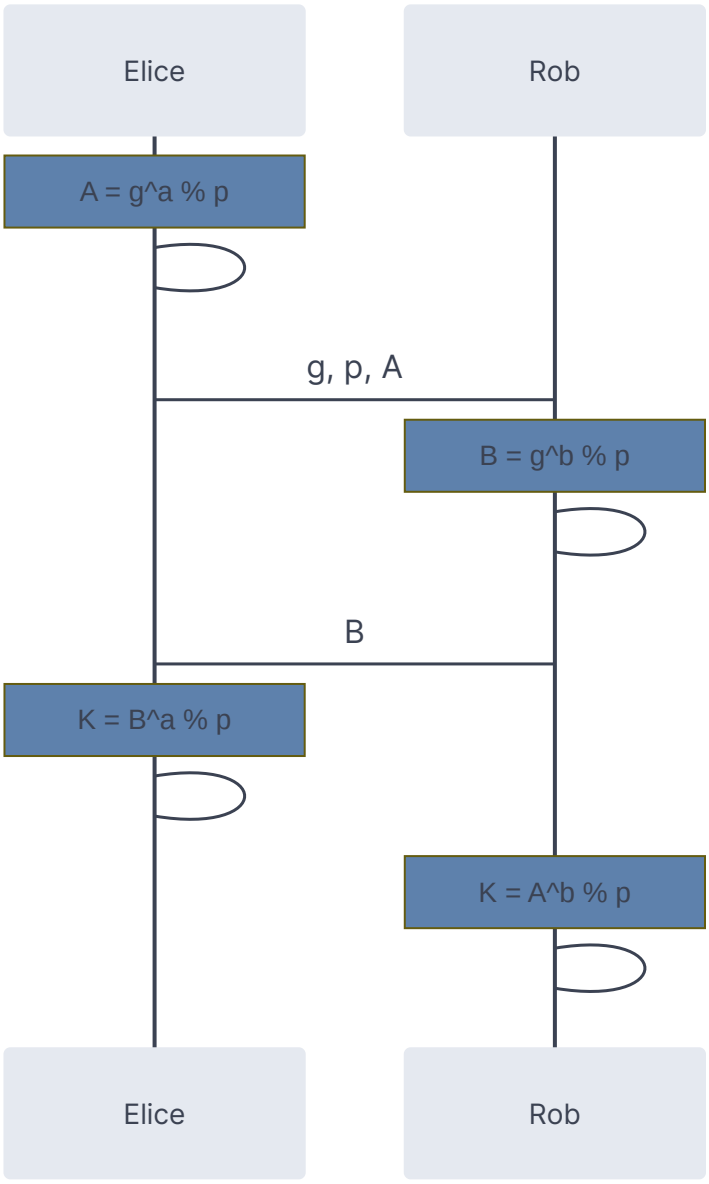
Diffie-Hellman:

Diffie-Hellman
Funcionamiento: Hay dos partes que negocian un

Conceptualmente:



Matemáticamente:



Perfect forward secrecy (PFS): Ir cambiando el cifrado de Diffie-Hellman cada 8 hs (o media si lo querés hacer re seguro) aproximadamente para que aunque nos descubran la clave no importe porque no tienen toda la comunicación/todos los mensajes. Porque si te pasas la contraseña simétrica normal cada cierto tiempo, si te cachan 1 clave, tienen acceso a todas las otras claves de ahí en adelante.

Queda por ver

- Seguridad[2] con criptografía simétrica (HMAC).
- Seguridad con criptografía asimétrica (Firma digital).
- Infraestructura de clave pública (PKI) (x509, CA).

Continúa en: 2022-08-17

---

1. Los () hacen mención a que no son lo que hacer a una comunicación segura, pero es necesario o para que se dé la comunicación o para proveer integridad.↩
2. Seguridad = **3 pilares** (confidencialidad, autenticidad, integridad) **+ no repudio**. También llamado servicios de seguridad↩