- Vemos el 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

- 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

La criptografía hoy en día se utiliza mucho como la base de las comunicaciones en los datos o en la transferencia de los mismos.

# Seguridad en las comunicaciones:

- Básico que tenga:
  - Confidencialidad -> Con cifrado simétrico o asimétrico.
  - 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 con no repudio, el emisor no puede negarse a que envió ese mensaje.
  - Integridad -> Verifico si el mensaje se modificó por algún error o atacante.
  - (Funciones resumen / hash).
- Para cifrados simétricos se recomienda AES > 256b y en asimétrico RSA > 256b.
- **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.

---

# After break

Hacemos una práctica con OpenSSL:

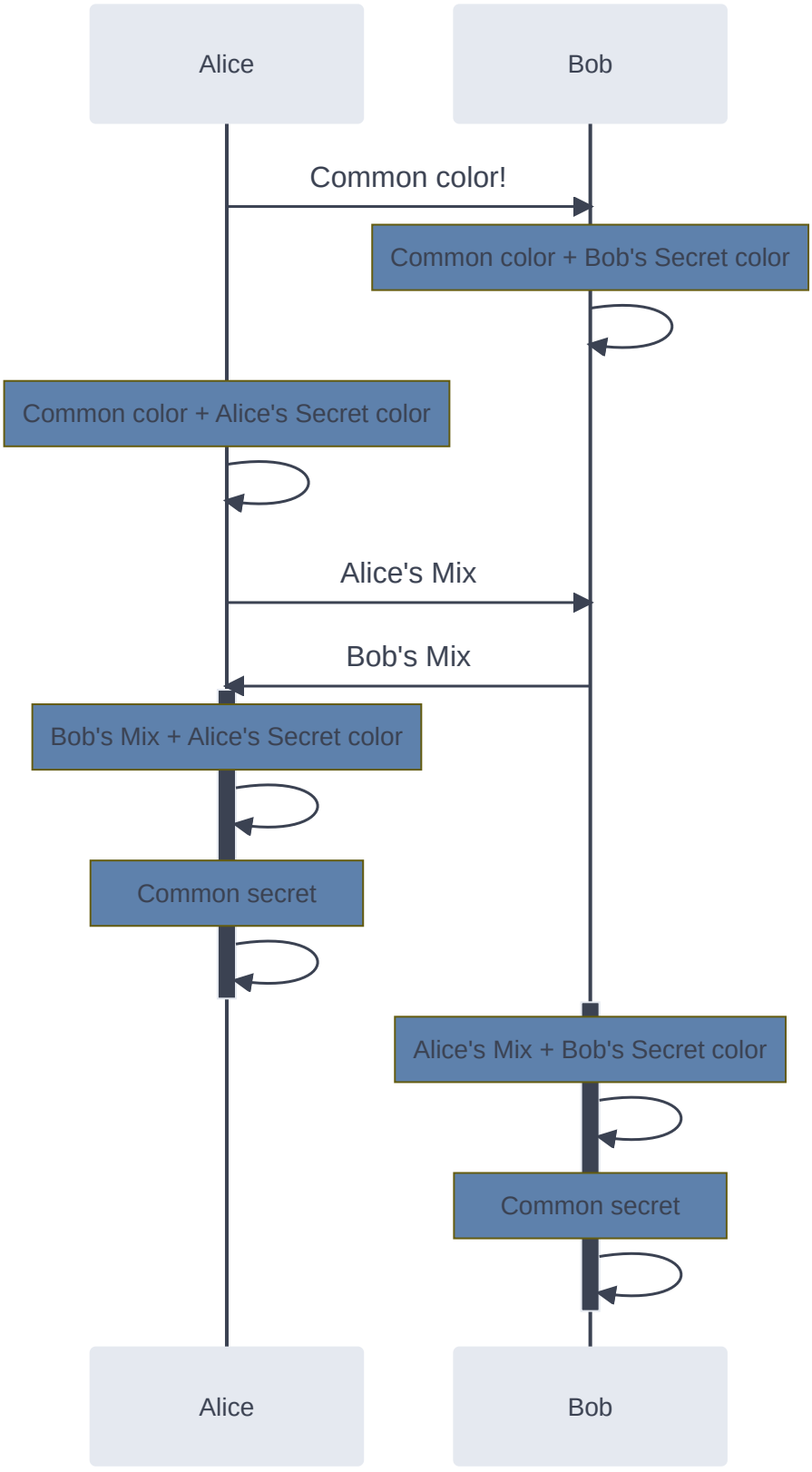
- Para hacer hashes con md5 o sha3-512

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

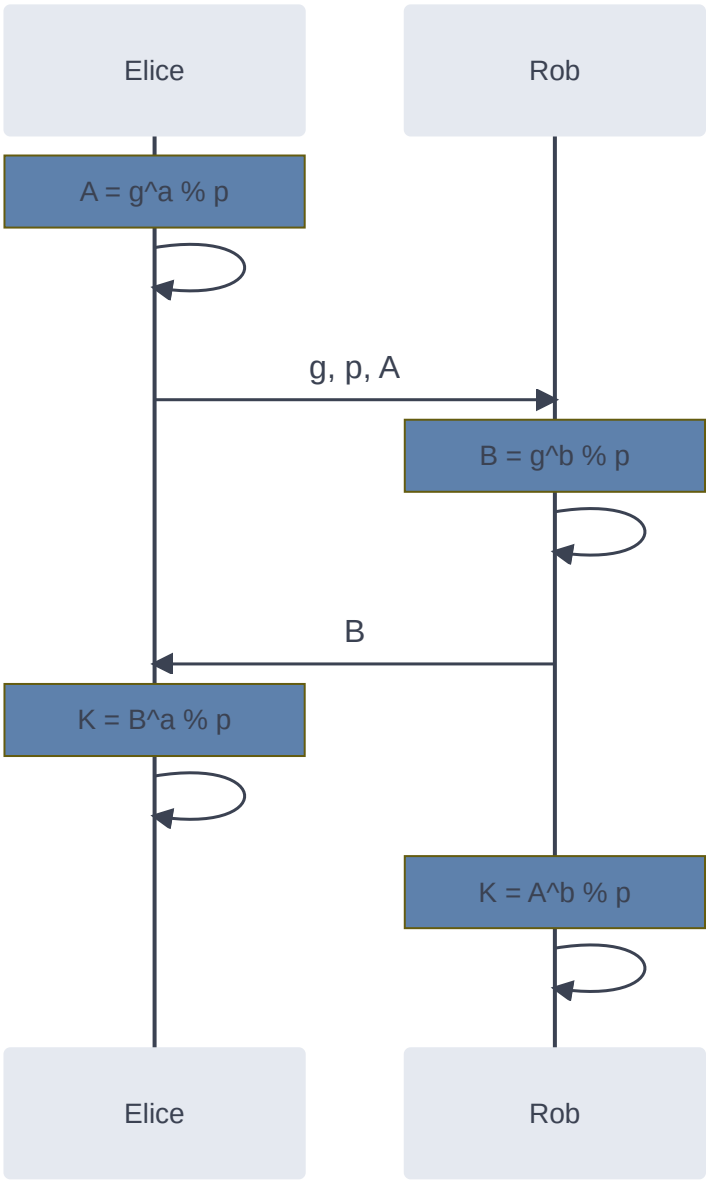
Vemos el funcionamiento de Diffie-Hellman:

- 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) apróx 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[1] con criptografía simétrica (HMAC).
- Seguridad con criptografía asimétrica (Firma digital).
- Infraestructura de clave pública (PKI) (x509, CA).

---

1. Seguridad = **3 pilares** (confidencialidad, autenticidad, integridad) **+ no repudio**. También llamado servicios de seguridad↩