- Vemos el temario

Encriptacion

- Ver como tanto simétrico como asimétrico logran comunicaciones seguras, asegurando los 3 pilares + el no repudio. Desde un punto de vista teorico-practico.
- 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).

Blockchain

- Como funciona a nivel de encriptacion.

Forense

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

Zero trust

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

Criptografia

La criptografia hoy en dia se utiliza mucho como la base de las comunicaciiones en los datos o en la transferencia de los mismos.

Seguridad en las comunicaciones:

- Basico que tenga:
  - Confidencialidad → Con cifrado simetrico o asimetrico.
  - Autenticidad / no repudio (Que se logran a la vez) → El receptor comprueba que efectivamente recibio un mensaje del emisor (y que ese emisor queria 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 algun error o atacante.
  - (Funciones resumen / hash).
- Para cifrados simetricos se recomienda AES > 256b y en asimetrico RSA > 256b.
- **La codificacion** tiene funcion inversa y no necesita clave, solo necesitas saber como se hace. Ej: Base64 en correo para mandar binarios (como pdf) que no es caracter, porque el mail solo funciona con caracteres. Envio 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 informacion original. Puede haber collision 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 (asimetrico, una y una). Seguridad

El cifrado asimetrico es muchisimo mas lento que el simetrico. El asi se usa para intercambiar la clave simetrica.

After break

Hacemos una practica con openssl:

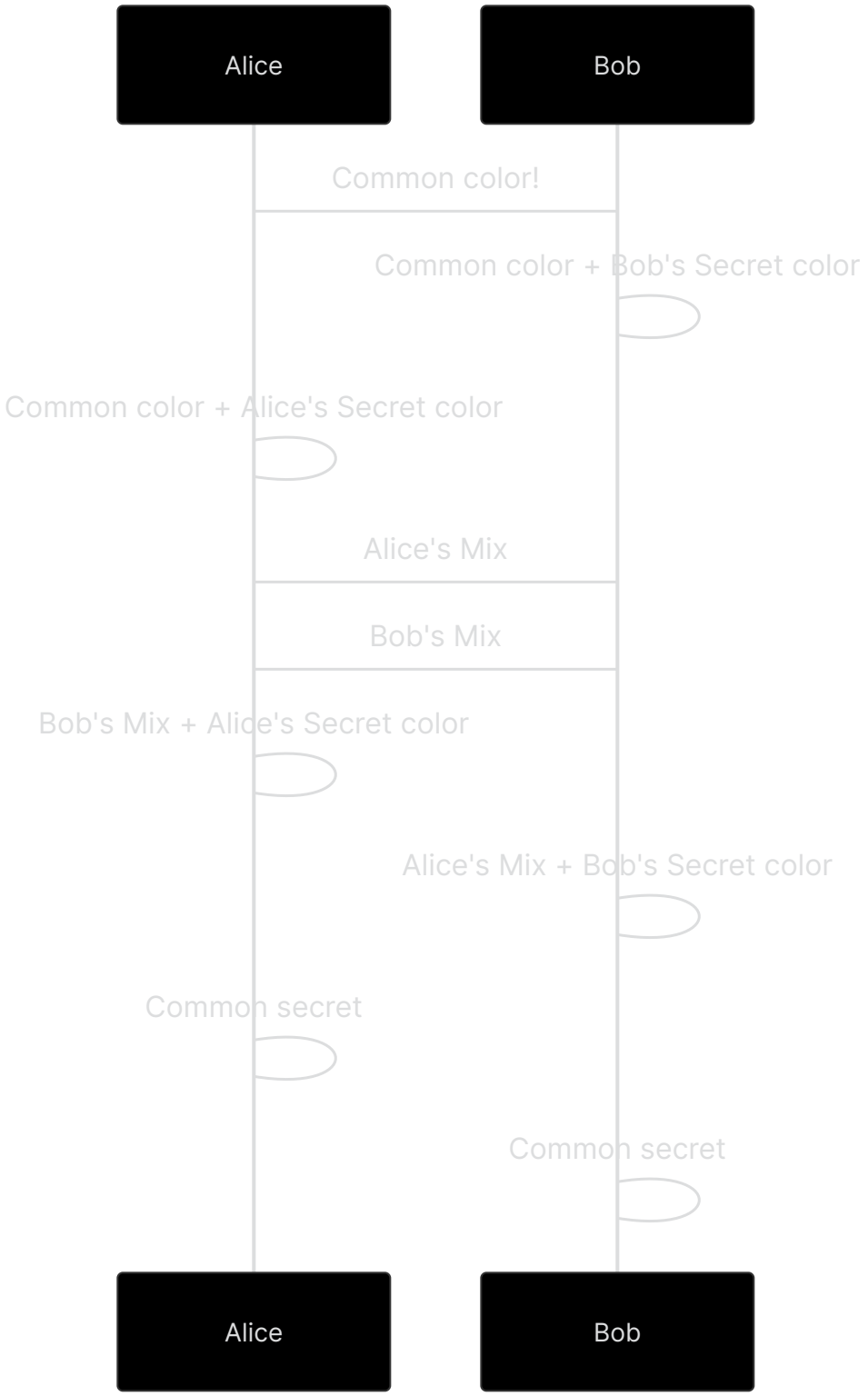
- Para hacer hashes con md5 o sha3-512

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

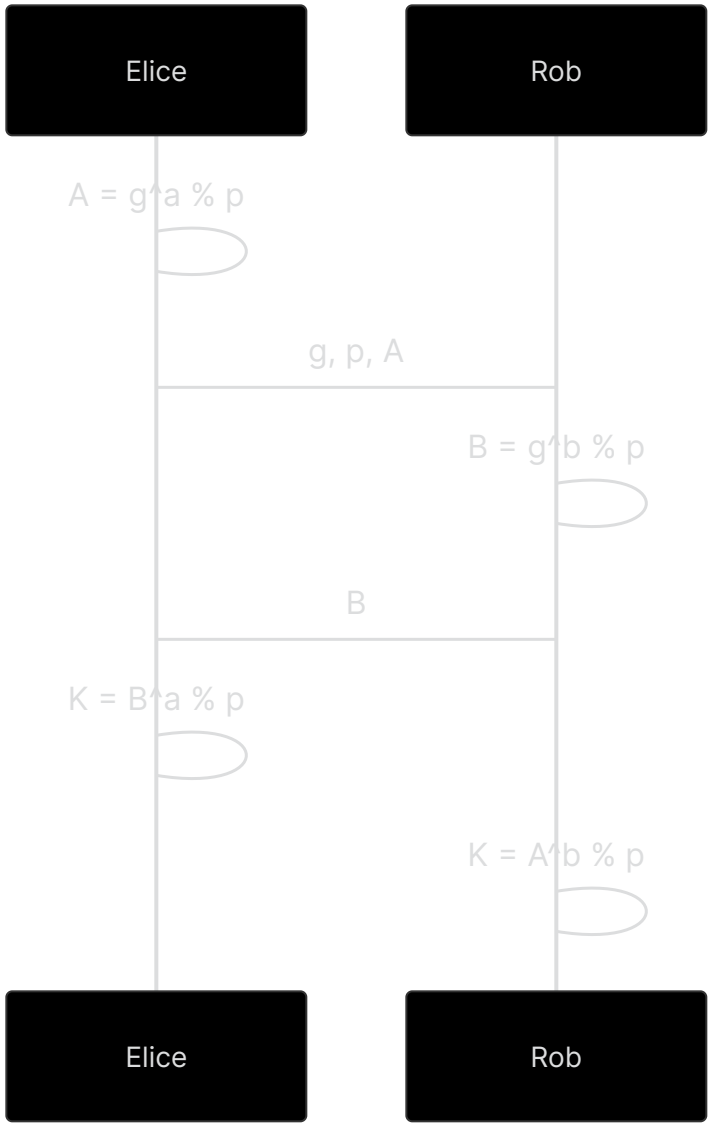
Vemos el funcionamiento de Diffie-Hellman:

- Funcionamiento:
  Hay dos partes que negocian un

Conceptualmente:



Matemáticamente:



Perfect forward secrecy (PFS): Ir cambiando el cifrado de Diffie-Hellman cada 8hs (o media si lo querés hacer re seguro) aprox 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 ahi en adelante.

Queda por ver

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

Nota: Seguridad = 3 pilares (confidencialidad, autenticidad, integridad) + no repudio. Tambien llamado servicios de seguridad