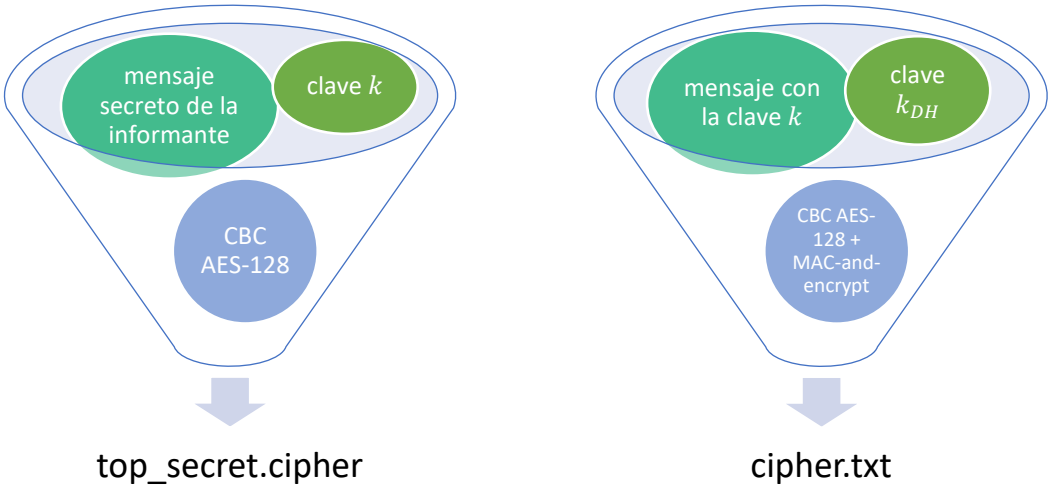
La división de delitos cibernéticos de la Ertzaintza se ha vuelto a poner en contacto con vosotros/as porque han encontrado a una persona con información novedosa sobre el robo ocurrido en *Kutxabank*. Como recordáis, un/a empleado/a (desconocido/a) había robado una gran suma de dinero y la empleó para comprar *cryptocurrency*.

La informante ha enviado un fichero cifrado **top_secret.cipher**, y ha decidido mandar la clave (k) utilizada para cifrar top_secret.cipher en un segundo fichero **cipher.txt** utilizando un canal de comunicación muy seguro.



Estas son las especificaciones del canal de comunicación muy seguro utilizado por la informante para el segundo mensaje:

- CBC AES-128, padding #PKCS7.
- Se incluye el iv al inicio del mensaje cifrado.
- Encrypt-and-MAC
- HMAC basado en SHA256.

El cifrado del fichero top_secret.cipher es similar al anterior pero no incluye ningún algoritmo de verificación de la integridad del mensaje cifrado.

Para poder cifrar el mensaje que contiene la clave (k), la informante ha utilizado una clave (k_{DH}) deducida mediante el protocolo Diffie-Hellamn de establecimiento de claves. Esta es la información que tenéis a vuestra disposición para poder hallar (k_{DH}).

Clave pública de la informante:	0x ccb1cf316ef3ea8868481472e8385a7e
Vuestra clave pública:	0x 870d7253bef3e17be12d9738937531dc
Vuestra clave privada:	0x 45451fae9b3a9d5f463ccb756303557c

Pero, en vez de recibir un único mensaje cifrado con la información de la clave k, habéis recibido dos mensajes (**cipher1.txt** y **cipher2.txt**). Parece que un hacker ha interceptado la comunicación y ha intentado modificar el mensaje para que no podamos descifrar el fichero top_secret.cipher. Afortunadamente, el hacker no ha conseguido interceptar el mensaje por completo y hemos recibido el mensaje cifrado original y el mensaje cifrado modificado. **¿Cómo podemos identificar si cipher1.txt o cipher2.txt es el mensaje cifrado original? ¿Qué información contiene el fichero top_secret.cipher?**