Aplicación bancaria.

En esta aplicación, un usuario debe ser capaz de administrar su cuenta bancaria en línea de una manera segura. Cada vez que un usuario desea establecer comunicación con el banco, la aplicación generará una sesión clave entre el usuario y el banco utilizando el protocolo Diffie-Hellman basado en curvas elípticas (ECC). La sesión clave se utilizará para cifrar toda la comunicación entre el usuario y el banco. La sesión clave debe ser adecuada para trabajar con AES (considerando 12 rondas) y un modo de operación (CBC, CTR). Para cada usuario el sistema mantendrá su nombre, un id de 8 dígitos y una contraseña (passwd). Un usuario accederá al sistema usando su id y contraseña, ambos datos deben viajar cifrados siempre que un usuario desee establecer comunicación con el banco. El sistema almacenará h (passwd), donde h será SHA-1. Para gestionar la información los usuarios y sus cuentas mantendremos una base de datos. Habrá dos tipos de cuentas:

* **Cuenta de ahorro**. Para esta cuenta habrá un número de cuenta, el saldo, retiros y depósitos y las fechas correspondientes.
* **Cuenta de crédito**. Para esta cuenta el sistema almacenará el número de la tarjeta de crédito, el crédito total que el usuario tiene, el saldo, los pagos y los cargos hechos a la tarjeta de crédito, y las fechas correspondientes

Cualquier usuario debe tener al menos una cuenta de ahorro y, como mucho, una cuenta de ahorro y una cuenta de crédito. Él debe ser capaz de hacer lo siguiente:

* Verificar las transacciones en un período de tiempo de sus cuentas.
* Hacer la transferencia entre sus propias cuentas
* Para realizar la transferencia a otros usuarios en el mismo banco, para ello necesitará el número de cuenta o el número de tarjeta de crédito y el nombre del propietario