Exercise 1 (Bitcoin Script)

Alice wants to protect her bitcoins with a password. She chooses a strong password and locks them in a bitcoin transaction output with the following scriptPubkey

```
OP_SHA256
<sha256 of the password>
OP_EQUALVERIFY
```

1. Why is that not a safe way to store bitcoins?

   In order to spend her coins, Alice has to broadcast her spending transaction with the password as scriptSig. Thus the password becomes publicly known. Eve can now compose a transaction stealing Alice's coins. Eve's transaction has to race Alice's, so Eve would e.g. put a larger fee to make her tx more profitable for miners to include.

2. Would it be safe to use Pay-to-script-hash to achieve this goal?

   In a pay-to-script-hash output, the above script would be the redeem script, the lock script would contain the hash of the redeem script, and the unlock script would be the password followed by the redeem script. So, here we have the same problem as before – once Alice broadcasts her spending transaction, the password and the redeem script become publicly known and can be used by Eve.