Writeup Homework 2

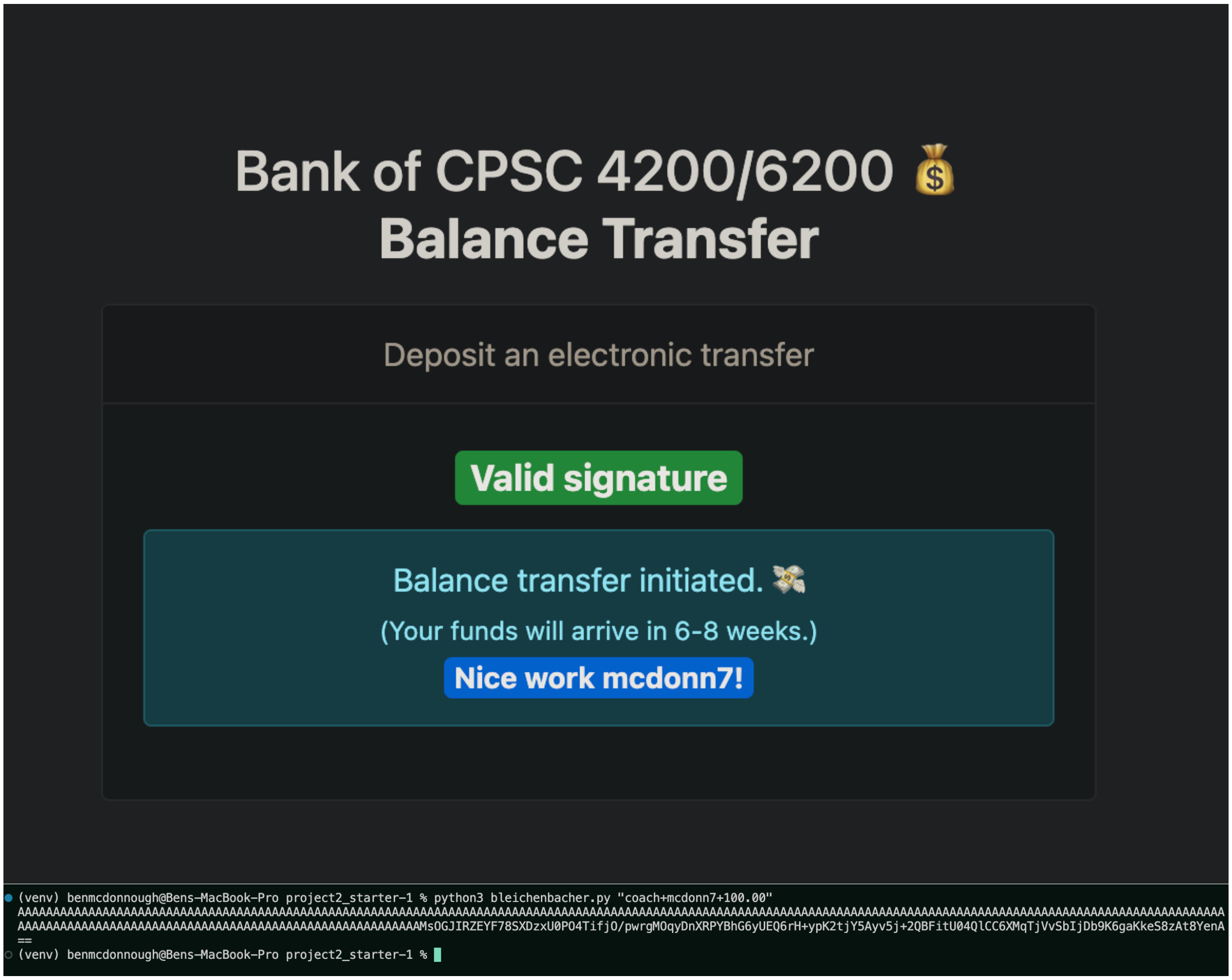
Benjamin McDonnough
I worked on my own on this assignment.

Question 1:

This attack uses the fact that the oracle tells the user if the padding is valid or not. The attack can use this information and being able to manipulate the IV to figure out the plain text without knowing the key for the decryption. To do this, I first split the message into workable blocks. Then, for each block, I set the current block and the previous block. Then for all the bytes going from right to left. I calculate the padding value based off of how many bytes are left. For example, if the program is working on byte 10, all of the padding behind it would be \x05. I then XOR all of the bytes already figured out with the padding value to make sure they stay valid. The the program tries all of the current values for the byte it is currently on to try and find a valid byte. It takes all of these bytes, throws them into an array that is then checked by the oracle so it checks all values at once instead of going through all 255, on at a time. If the padding is valid, it adds the XOR of the correct byte and the padding value to the Decrypted text and takes that value, XOR's it with the same byte of the previous block and stores it in the plaintext. It then takes the plaintext from all the blocks, concatenates them, and prints it out the terminal.

Question 2:

The Bleinchenbacher attack is used to show the vulnerabilities of RSA signatures. To implement this attack, I first took the message and hashed it using SHA256. I also set the ASN1 to the correct bytes. From there, I created the full "block" of data by combining these values with the starting bytes followed by one \xFF and \x00. I then calculated the amount of garbage padding to add to the end of the message using knowledge that the whole thing is 2048 bits. Then, using the public key e = 3, I extracted the signature without needing the private k, d, because of the weak encryption that allows for $c = m^{1/3}$ while also checking to make sure that c is not rounded down too much. This is done by ensuring that $c^e >= m$.


Bank of CPSC 4200/6200 💰
Balance Transfer
Deposit an electronic transfer
Valid signature
Balance transfer initiated.
(Your funds will arrive in 6-8 weeks.)
Nice work mcdonn7!
(venv) benmcdonnough@Bens-MacBook-Pro project2_starter-1 % python3 bleichenbacher.py "coach+mcdonn7+100.00"
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMsOGJIRZEYF78SXDzxU0PO4TifjO/pwrgMOqyDnXRPYBhG6yUEQ6rH+ypK2tjY5Ayv5j+2QBFitU04QlCC6XMqTjVvSbIjDb9K6gaKkeS8zAt8YenA
==
(venv) benmcdonnough@Bens-MacBook-Pro project2_starter-1 %