Assignment 2 Report

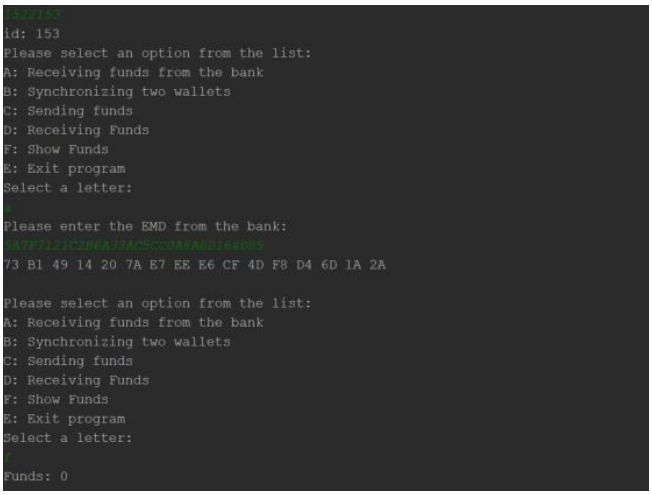
Names: Caleb Lohrmann, Terence Ho

Introduction:

For assignment two we created and finished all features of the banking app. The only thing to take note when compiling is that It asks for the full 7 digit student ID if you are testing the banking send money functionality use the 7 digit else you can use the 3 digit wallet id. If you use the 7 digit the wallet still has the three digit id from the end of the student id.

Case 1: Bank Sending money

The first picture on the left is when the correct EMD is used and paired with the correct has you can see that for our case the bank sent us 215 dollars. The second picture shows what happens if it is the incorrect EMD as you can see it shows the failed decrypted string and the amount is not updated.



Case 2: Synchronization of two wallets

This case shows the synchronization of two wallets. The first picture shows the first wallet create the synchronization for the second wallet. The next picture shows the successful decryption and synchronization. Then in the third picture the second wallet creates the synchronization token for first wallet and the last picture shows the successful decryption and synchronization of the first wallet with the second. This creates a successful synchronization,

```
Please enter the walletID to synchronize with:
123
created string: 00000153000001230000000000000000
encrypted token: 0D 25 B2 AD C2 4E 5D 65 9A 45 97 96 7F B5 7D CA
0D25B2ADC24E5D659A4597967FB57DCA
00 00 01 53 00 00 01 23 00 00 00 00 00 00 00 00
00000153000001230000000000000000
Token is for your wallet
```

```
Please select an option from the list:
A: Receiving funds from the bank
B: Synchronizing two wallets
C: Sending funds
D: Receiving Funds
F: Show Funds
E: Exit program
Select a letter:
d
Please enter the receiving token:
A19A40445AE8338C483FA2B456ED3F1F
00 00 01 23 00 00 01 53 00 00 00 00 00 00 00 00
153
153
Token is for your wallet
walletID:123 amount:0 counter: 1
Funds received
```

```
Please enter the walletID to synchronize with:
153
created string: 00000123000001530000000000000000
encrypted token: A1 9A 40 44 5A E8 33 8C 48 3F A2 B4 56 ED 3F 1F
A19A40445AE8338C483FA2B456ED3F1F
00 00 01 23 00 00 01 53 00 00 00 00 00 00 00 00
00000123000001530000000000000000
Token is for your wallet
```

```
Please select an option from the list:
A: Receiving funds from the bank
B: Synchronizing two wallets
C: Sending funds
D: Receiving Funds
F: Show Funds
E: Exit program
Select a letter:
d
Please enter the receiving token:
[redacted]
00 00 01 53 00 00 01 23 00 00 00 00 00 00 00 00
123
123
Token is for your wallet
walletID:153 amount:0 counter: 1
Funds received
```

Case 3: Sending funds

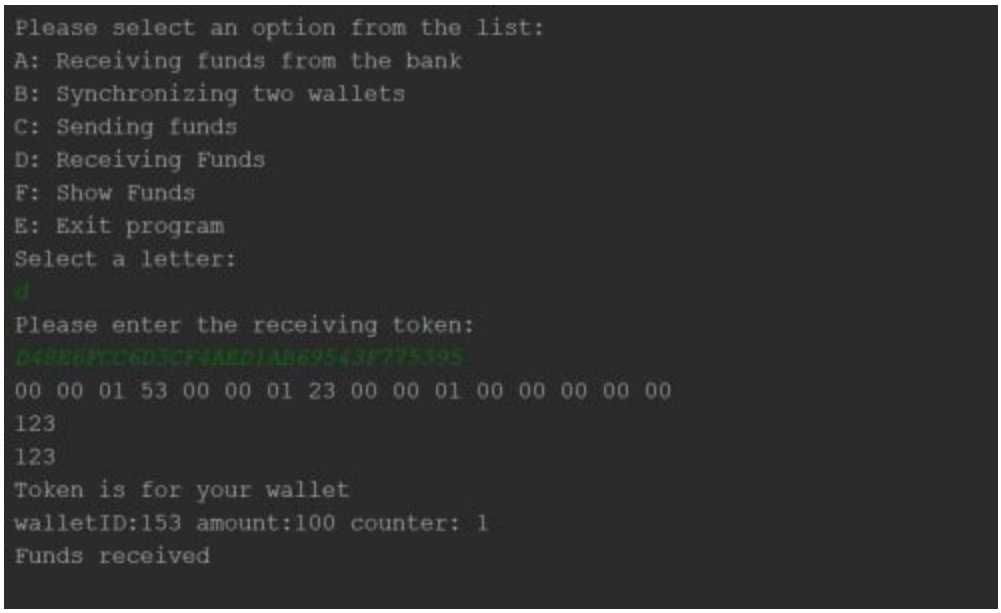
Use case 3 and 4 sort of go together as it shows to total of the same send and receive. The first picture shows a successful encryption token for wallet 123 of 100 dollars and that the amount has been updated.

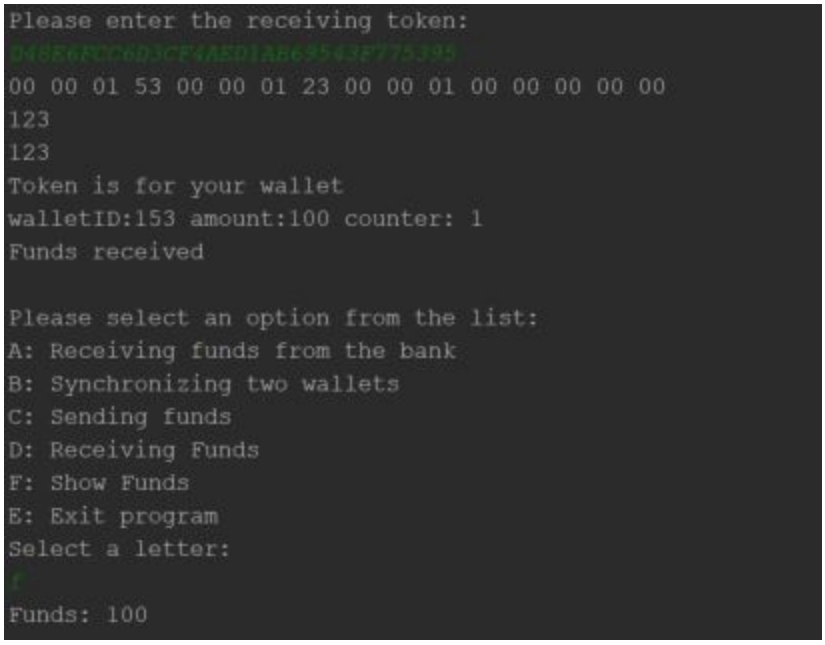
```
Select a letter:
C
Please enter the walletID of the receiver:
123
Please enter the amount being sent:
100
created string: 00000153000001230000010000000000
encrypted token: D4 8E 6F CC 6D 3C F4 AE D1 AB 69 54 3F 77 53 9
to:123 amount:100 counter: 1
100 funds sent to Wallet@1035e27

Please select an option from the list:
A: Receiving funds from the bank
B: Synchronizing two wallets
C: Sending funds
D: Receiving Funds
F: Show Funds
E: Exit program
Select a letter:
f
Funds: 115
```

Use Case 4: Receiving Money

This shows a successful receive of money from a different wallet. This uses the exact token that was created in use case 3. As you can see from the first picture, it depicts the token was decrypted and since it was synched up it added 100 dollars to the amount. The second picture shows that addition.





Please indicate two possible vulnerabilities in the current design and propose modifications to close such risks:

1. One vulnerability to the current design is the ability to use a generic AES256 for a encryption with no padding for encrypting the token. This could make the key vulnerable to cryptanalysis.
    a. One way of closing the risk is to utilize an additional key during encryption, using salt and secret initialization vectors for the encryption process that is only known by the bank's system.
2. Another vulnerability in the current design is that if you find the bank's secret key, you could brute force the counter and allow any token that contains your wallet's id to become valid.
    a. One way of closing this risk is to utilize a public bank key to encrypt for the bank and private bank key for the bank to decrypt the token. This would only allow the bank to decrypt and verify that the token is valid.
3. The internal table is also not encrypted and could potentially be used to backtrack in order to find wallet IDs and balances. Paired with the ability access a wallet using the wallet ID. This could be a way for someone to access someone else's wallet.
    a. The internal table could be encrypted in order to avoid people from being able to access that information.