Fangyang Cui
Problem Set 1

1. a. The transaction ID is 3a83b9f6504c4617730918f0a4b8a4290edb63e8f4f0519aa05aaf4fcab9c3c4.
b. The transaction fee was .0001 BTC or approximately $0.02.

c. The block containing my transaction contained 1,649.102 BTC of transactions.

d. My transaction was received on September 3rd at 12:23 AM according to blockchain.info. Counting the block that contains my transaction as the first confirmation, the third confirmation block was mined at 12:54 AM. Therefore, the taken was 31 minutes.

2. a. Some addresses of other students are
1EEwCjPdxHPBGX3puriE7eVBnd1j1gRipW
1MeR6TjdB4yZqh3tPCDomrEDsKDTZMTYzL
1CN1KrUpBVpmWi1nyBkM397N9t6vLmeQXE

b. The source of the bitcoins I received traces back to the address 1AVcWkJzfCUKorNA5SjY1KJcSCEaCtyMsQ. This is likely an address controlled by a bitcoin exchange. Although I don't know for sure what exchange the address belongs to, I would guess it is coinbase since that is the easiest option to buy bitcoins in the United States.

c. The transaction was relayed by 208.66.68.127 which is owned by InterWeb Media, a Canadian company.

3. a. The developer could send the private keys of all addresses generated by the wallet to his computer. This would allow him to take the coins at any time he wants and not raise suspicion until after the theft is completed. The developer could have the program do this automatically when the balance reaches a certain amount.

b. I am confident my money is safe in my wallet since I only have a small amount that is not worth stealing. In addition, other people online have used the same wallet without any issues. If I was going to store more money in it, I would have to review the source code to make sure the wallet contains no malicious code and compile the wallet from the source.

4. Converting to base 16,
$2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 = 16^{64} - 16^8 - 2*16^2 - 16^2 - 8*16 - 4*16 - 16 - 1$.
16^{64} is a 1 followed by 64 zeroes so the hexadecimal representation can be found starting from that and subtracting.
16^8 = 1 0000 0000
$3* 16^2$ = 0300
13*16 = D0
1 = 1

Subtracting these amounts from 16^{64} results in
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFC2F.

5. In order to trust the key generated by keypair.go with a large amount of bitcoins, I would need to trust that the random number generator does generate random numbers. Therefore, the address I generate will not be the same as someone else's generated address. I need to trust that the private and public keys are generated correctly without a calculation error. I need to trust that the keys being generated are not being logged anywhere so that only I know the private key.

6.

```
func generateVanityAddress(pattern string) (*btcec.PublicKey, *btcec.PrivateKey) {

	// Generate a private key, with a vanity address
	priv, err := btcec.NewPrivateKey(btcec.S256())
	pub := priv.PubKey()
	addr := generateAddr(pub).String()
	found, regexperr := regexp.MatchString(pattern, addr)

	if err != nil || regexperr != nil{
			// There was an error. Log it and bail out
			log.Fatal(err, regexperr)
	}

	for !found {

		priv, err = btcec.NewPrivateKey(btcec.S256())
		pub = priv.PubKey()
		addr = generateAddr(pub).String()
		found, regexperr = regexp.MatchString(pattern, addr)
		if err != nil || regexperr != nil{
			// There was an error. Log it and bail out
			log.Fatal(err, regexperr)
		}

	}

	return pub, priv
}
```

This function keeps generated keys until an address that matches the pattern is found.

7.

```
F:\crypto cabal stuff\PS1>go run vanity.go
This is a private key in hex:   [6b7f3e5fc96e2284e5df6f5c93aae589d8580700108803f
1e3e681438f513586]
This is a public key in hex:    [03d17c425bc84dfe91a5ded6fe373c41551d4c4f6243525
54364ba646ec367f17e]
This is the associated Bitcoin address: [1BTCz9VHTscXr5P2qRkpQbx8bQ2rXS6y5]
```

8. The vanity address is just as secure as the first address that was generated. Because of the properties of cryptography, an attacker gains no additional information by knowing that the address contains a unique string. Finding the private key will be just as difficult.

9. Transaction ID : f623cd14bf7627dbfc797bf471fc1f16281ec962fda9db0043f1fbcef4a5729e

10. The transaction ID that sent bitcoin from my vanity address to another student's address is 5bc842024ed8eb684e4b5c0821e5cce34671e9bf00383a9a8e596f264ff1ef44.

11.

Transaction ID: 9444de49dcc417c2e317320c99c8bf91a2efa12b72e6e07b98eba2467663f875

Here, I send a transaction from my 1BTC vanity address worth 50,000 satoshis total back to my primary bitcoin address. The vanity address contained 100,000 satoshis to start with.