1.

a. 1d7155155e54d07b56d484f0aab57b94ed864bf28bc5165f74385fde67644190

b. .0001 BTC, $0.02

c. .108282 BTC

d. 15:14:37 -> 15:17:16 -> 15:17:59 -> 15:33:05
It took roughly 18:24 for the transaction to be followed and confirmed by 3 blocks.

2.

a. 1MDjCqjwnKmMWPxawpgN1UuDfbMUUgqnWw
1LeXjaxMbugBveWusTRpbFtx13N5HamcE4
15j1jdJsMa4vR71gcZ6FCfYeAWJdPwpn7W

b. It comes back to address 14J6ep326owXDpc1waViGJNB1onSFy9eou, bought on 8/26/15 at 4:51:05 pm

3.

a. Increase the “fees” a user has to pay in a transaction by padding the fee displayed and keeping the extra amount.
Lie about exchange rates, implying the BTC you have is worth less than its actual value.

b. Fairly confident, as it was recommended by the instructor (and hopefully he wouldn’t lead us astray). It also appears to be fairly popular online, so either it’s duped a good number of people or it’s legitimate.
Calculate the various fees yourself and compare them to what the wallet says.
Independently verify exchange rates.

4. Used the fromHex function from btcec.go, converted and printed out num := fromHex(“FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFC2F”) = 115792089237316195423570985008687907853269984665640564039457584007908834671663

Computed $2^{256} - 2^{32} - 2^{9} - 2^{8} - 2^{7} - 2^{6} - 2^{4} - 1$ = 115792089237316195423570985008687907853269984665640564039457584007908834671663

5. Nobody knows what the seed was when the private key was chosen.
keypair.go didn’t send the key information anywhere.
Nobody was able to monitor the output on my computer.
Nobody has solved the discrete logarithm problem.

6.

```
func generateVanityAddress(pattern string) (*btcec.PublicKey, *btcec.PrivateKey) {
  priv, err := btcec.NewPrivateKey(btcec.S256())
  if err != nil {
    // There was an error. Log it and bail out
    log.Fatal(err)
  }

  addr := generateAddr(priv.PubKey())

  bool, err := regexp.MatchString(pattern, addr.String())

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

  }

  return priv.PubKey(), priv
}
```

7. 1Ryan2d1mWxdsmtbh9vTbmSdMa8grian4
8. Still secure, as it having specific characters doesn’t give more information about the private key.
9. 0c485c0de6dcf00e332d0d48fc38de376cbdf4bafc8880107555a17808deb6a4
10. -privkey "17225eb8ea21fc1d50aee0155bcb70c4122deeffe3d123d90a3c880e7ed22f62" -toaddress "15j1jdJsMa4vR71gcZ6FCfYeAWJdPwpn7W" -txid "0c485c0de6dcf00e332d0d48fc38de376cbdf4bafc8880107555a17808deb6a4" -vout 0
11. See additional file (spend.go)
12. I get a “The sending api responded with:
    Transaction rejected by network (code -26). Reason: 18: bad-txns-inputs-spent”