1. What’re the three major advantages of hash functions to the blockchain? (list at least two instance in which hash functions are used in Bitcoin, and why)
2. Can two different input map to the same hash result?
3. You’re the CTO of facelook. You want to create a login system that will not store the password of your users, instead your system will store only the hashed password. What’s the drawback of such a system? What can you do to strengthen your login system?
4. Each Bitcoin protocol message is composed of X parts. What are they?
5. The message headers is made out of which field (just their name is enough)
6. Look at the following message and in the bitcoin official documentation, and answer the following question:

```
f9beb4d976657273696f6e0000000005c000000e5c76be67e1101000000000000000
000f64b8558000000000000000000000000000312e302e302e373231000000000000002
08d0000000000000000312e302e302e37323100000000000000208d962384230000
00000645584f4249541ed9060000
```

a. What type of message is it? (verAck, Tx, version, ping…?)
b. Is the message a live-net or test-net message?
c. Break the message into its fields (no need to convert them. Leave them in their hexadecimal form).

7. Draw a timeline representing the handshake process.
8. Write the complete bytecode for verAck message on the live-net (tip, sha256(sha256(empty)) = “5df6e0e2761359d30a8275058e299fcc0381534545f55cf43e41983f5d4c9456”)
9. Place the following addresses in the right category:

mfjRUvWr9QZadpiRnbRfHS4UDSxdR9FE75
mi4kMd3HcLUGJSouNdJZ87eUBbi7cNE6C3
1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2
3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy
1BoatSLRHtKNngkdXEeobR76b53LETtpyT

Test net	Main net

10. For the first address (a), what’s the checksum of that address?
11. What’s the rationale for using base58?
12. Can we identify the public key from the address?
    a. What is usually the role of the private key and the public key when encrypting messages? What’s their role in the Bitcoin protocol?
13. How many transaction types are currently recognized in the bitcoin protocol?
14. What’s the main difference between p2pkh and p2p?
15. Alice has five bitcoins; she wants to send three bitcoins to Charlie and give 0.01 bitcoin to the miner as a fee. How many outputs should her transaction contain? What’s the amount of bitcoin that should be associated with each output?
16. Look at the following transactions and answer the following questions

```
01000000014b6220c07d1ab7b91b3d7aa77cf100c374acf8a64835c809d40511a8a8b245f10000
    00006a4730440220666c899ef50909023f19a3a42a68f8fe01b795756da6bf52cf208303c3d9
    900e0220134b3310136fec063a4926ac5b752a4eaa41636beb8fcec720a3983c4d284d38012
    103d5cd182018fe6570e67073b583ead2b205c42dd4a0c8034afc380fed4ca81581ffffffff01d0
    ede50b0000000017a914cab366f0397714fdc0d611370c31dd89246eff188700000000
```

   a. What type of transaction is it? (p2pkh, p2sh, op_return etc.)?
   b. How many inputs and outputs this transaction contains?
   c. Mark the public key of the sender in the transaction.

Look at the following stack, what will be its final result? Prove it by processing it step by step.
<op_push> <3> <op_push> <4> <op_add> <op_mul> <op_push> <4>

18. Multisig can be achieved using two types of scripts.
    a. Which scritps?
    b. What are the advantages and disadvantages of each one?

19. What is the relation between Difficulty and Target?
20. What’s the role of the nbits field in the block header?
21. Draw a merkle tree containing four transactions
22. Draw a merkle tree containing five transactions
23. Alice wants to prove to Bob the existence of transaction #3 in a merkle tree that contains 10 transactions. What is the minimum amount of information she need to provide in order to do so?