Mid-Term Examination
CS577: Introduction to Blockchain and Cryptocurrency
Full Marks: 60 Time: 2 hours

1. Choose the correct answer(s): **(10*1=10 points)**
   a. What is a miner?
      i. A type of blockchain
      ii. An algorithm that predicts the next part of the chain
      iii. A person doing calculations to verify a transaction
      iv. Computers that validate and process blockchain transactions

   b. What is the purpose of a nonce?
      i. Follows nouns
      ii. A hash function
      iii. Prevents double spending
      iv. Sends information to the blockchain network

   c. What is a genesis block?
      i. The first block of a Blockchain
      ii. A famous block that hardcoded a hash of the Book of Genesis onto the blockchain
      iii. The first block after each block halving
      iv. The 2nd transaction of a Blockchain

   d. Blockchain can be stored as which of the following?
      i. A flat file
      ii. A Database
      iii. Both of the above
      iv. None of the above

   e. Which hashing algorithm is used in many blockchain technology
      i. MD2
      ii. MD5
      iii. SHA-512
      iv. SHA-256

   f. Which of the following cryptography type is used in blockchain
      i. Asymmetric-Key Cryptography
      ii. Symmetric-Key Cryptography
      iii. Depends upon the application
      iv. Depends upon the computing power

   g. Which technology does Blockchain uses for storing transactional data
      i. Peer to peer networking
      ii. Data assembly and disassembly

iii. Hashing
iv. None of these

h. What does every non-leaf node of Merkle tree, is labelled with
   i. hash of a data block
   ii. the cryptographic hash of the labels of its parent nodes
   iii. the cryptographic hash of the labels of its child nodes
   iv. None of these

i. What is the output of SHA-256 algorithm
   i. 16 character
   ii. 32 character
   iii. 64 character
   iv. 128 character

j. What does every leaf node of Merkle tree, is labelled with
   i. hash of a data block
   ii. the cryptographic hash of the labels of its parent nodes
   iii. the cryptographic hash of the labels of its child nodes
   iv. None of these

2. Answer the followings: **(3+6+9=18 points)**
   a. What are the basic security principles?
   b. In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M?
   c. Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root a = 7.
      i. If user A has private key XA = 5, what is A's public key YA?
      ii. If user B has private key XB = 12, what is B's public key YB?
      iii. What is the shared secret key?

3. Write the pseudocode of mining process in bitcoin network and describe all steps in detail. Explain how the difficulty level of the mining process is adjusted in bitcoin network. Establish the relation between global hash-rate and the difficulty level. **(10+4+6=20)**

4. Define blockchain. What type of records can be kept in Blockchain and is there any restriction on the same? How does bitcoin network deal with Sybil Attacks and double-spending attacks?
   (2+2+8=12 points)