THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

This exam paper must not be removed from the venue

Venue ____________________
Seat Number __________
Student Number |__|__|__|__|__|__|__|__|
Family Name ____________________
First Name ____________________

School of Information Technology and Electrical Engineering

EXAMINATION

Semester One Final Examinations, 2021

COMS4507 Advanced Topics in Security

This paper is for St Lucia Campus students.

Examination Duration: 90 minutes

Reading Time: 10 minutes

Exam Conditions:

This is an Open Book examination
Any calculator permitted - unrestricted
During reading time - write only on the rough paper provided
This examination paper will be released to the Library

Materials Permitted In The Exam Venue:
(No electronic aids are permitted e.g. laptops, phones)

None

Materials To Be Supplied To Students:

1 x 14-Page Answer Booklet

Instructions To Students:

Additional exam materials (e.g. answer booklets, rough paper) will be provided upon request.

Answer all questions in Part A.
Answer all questions in Part B.
Choose and answer 3 questions in Part C.
Total Marks: 65

For Examiner Use Only

Question	Mark

Total _________

Part A – Multiple Choice Questions
10 Questions (20 Marks)

EACH MULTIPLE CHOICE QUESTION CARRIES 2 MARKS
CHOOSE THE BEST ANSWER FOR EACH QUESTION (ONLY ONE)
PLEASE CIRCLE THE CORRECT ANSWER ON THIS PAPER

1) Which one of the following statements regarding eCash is correct? (choose the best answer)

a) eCash is a DLT-based payment system.

b) Blind Signatures are used to prevent double spending.

c) eCash uses digital signatures to verify the authenticity of coins.

d) For the bank to link a coin serial number to a customer, it needs to find a 32-bit SHA256 pre-image.

e) None of the other statements is correct.

2) Which one of the following statements regarding Blockchains is correct? (choose the best answer)

a) A Blockchain is binary tree with linear (O(N)) search time.

b) A hash pointer to the first block (Genesis block) of a blockchain protects the integrity of all the blocks in the in chain.

c) One of the main inherent security benefits of a blockchain is data integrity and immutability.

d) In a Blockchain, a trusted third party is responsible for verifying the account balances of the unspent transaction outputs (UTXOs), which avoids double spending.

e) None of the other statements is correct.

3) Which one of the following statements regarding Bitcoin is correct? (choose the best answer)

a) Bitcoin is a public permissioned blockchain.

b) Bitcoin uses the Tendermint consensus protocol.

c) The Bitcoin scripting language (“Script”) is a simple, stack based and Turing complete programming language.

d) Coinbase transactions need at least one unspent transaction output (UTXOs) as input.

e) None of the other statements is correct.

4) Which one of the following statements regarding Bitcoin addresses is correct? (choose the best answer)

a) Bitcoin addresses are derived as a SHA512 hash of an ECDSA Private Key.

b) Bitcoin addresses are represented in Base64 encoding.

c) Public key certificates are used to guarantee the authenticity of addresses in Bitcoin.

d) Pay-to-script-hash (P2PSH) addresses allow the implementation of more complex transactions, e.g. “multisig” transactions.

e) None of the other statements is correct.

5) Which one of the following statements regarding Bitcoin Mining is correct? (choose the best answer)

a) The most efficient method for Bitcoin mining is via the use of 64-bit Intel CPUs with Thermal Velocity Boost and Intel Dynamic Tuning.

b) Bitcoin uses an “ASIC-resistant” Proof of Work algorithm.

c) The solution to a Bitcoin mining puzzle is a 32 character ascii string.

d) The difficulty of the Bitcoin mining puzzle is chosen dynamically, so that the solve time gradually increases over time.

e) None of the other statements is correct.

6) Which one of the following statements regarding Bitcoin Transactions is correct? (choose the best answer)

a) A transaction locking script requires the successful verification of the corresponding public key certificate.

b) The difference between the sum of the inputs and the sum of the outputs in a Bitcoin transaction represents the Block Reward.

c) Bitcoin sent to a transaction “change address” represent a transaction fee, which is given to the node that mines the corresponding block.

d) Inputs to a Bitcoin transaction consist of zero or more unspent transaction outputs (UTXOs).

e) None of the other statements is correct.

7) Which one of the following statements regarding Bitcoin's Proof of Work based consensus mechanism, also referred to as "Nakamoto Consensus", is correct? (choose the best answer)

a) Proof of Work in Bitcoin requires the factoring of very large integers, which is computationally very expensive.

b) The probability of successfully mining a block in Bitcoin in a given amount of time is proportional to the available hash power of a miner.

c) The mining pool with 25% of the total Bitcoin mining power can expect to mine 6 blocks per hour, on average.

d) The Block Reward for Bitcoin mining decreases linearly, until it reaches a minimum of 1 BTC per mined block.

e) None of the other statements is correct.

8) Which one of the following statements correctly explains how we can prove that a transaction is part of a Bitcoin block? (choose the best answer)

a) Starting at the Merkle Root, traverse the tree until reaching the targeted data hash. The tree traversal path represents the proof of membership.

b) Starting from the hash of the targeted transaction at the bottom of the tree, traverse the tree until reaching the Merkle Root. The path represents the proof of membership.

c) Perform a depth-first search of the binary tree until the transaction is found, i.e. the hash matches.

d) Perform a linear O(n) lookup of the Unspent Transaction Output array.

e) None of the other statements is correct.

9) Which one of the following statements regarding Bitcoin Mining is correct? (choose the best answer)

a) The total amount of available Bitcoin gradually increases, with 657,000 BTC being added every year.

b) The Bitcoin mining reward consists of two parts, transaction fees and block rewards, which are provided in coinbase transactions.

c) On average, a new Bitcoin block is mined every 15 seconds.

d) Given a fixed amount of mining power, joining a mining pool increases the expected (average) mining revenue.

e) None of the other statements is correct.

10) Which one of the following statements regarding Ethereum is correct? (choose the best answer)

a) In Ethereum, new transactions are forwarded over its peer-to-peer network using the Centralised Shortest Widest Path Last Routing protocol (CSWPLR), which relies on Dijkstra's shortest path algorithm.

b) Contract Accounts in Ethereum can send transactions and are controlled by a private key.

c) Ethereum’s transaction throughput can be improved by increasing the mining difficulty, as is the case in Bitcoin.

d) Paying more for Gas in Ethereum has a similar benefit to providing higher transaction fees in Bitcoin, i.e. it generally reduces the time it takes for a transaction being included on the blockchain.

e) None of the other statements is correct.

Part B – Short Answer Questions and Problems
5 Questions (15 Marks)

ANSWER **ALL QUESTIONS** IN PART B

MARKS PER QUESTION ARE AS INDICATED

FOR QUESTIONS THAT REQUIRE CALCULATIONS, YOU NEED TO SHOW THE INDIVIDUAL STEPS OF HOW YOU ARRIVE AT THE RESULT.

11) [2 marks]

Explain the purpose of Gas in Ethereum.

12) [2 marks]

Let's assume you have recently found an efficient algorithm for factoring large integers. You are planning to present the algorithm at a major conference next year (2022). Explain how you can use a Blockchain (e.g. Ethereum) to later prove that you knew the algorithm in 2021, without revealing any details about the algorithm, or even the fact that you have it, prior to its presentation at the conference in 2022.

13) [4 marks]

Bob has bought himself an Antminer S19 Pro Bitcoin miner, which can do 110TH/s (110*10^12 hashes per second). You can assume that, at the current level of difficulty, solving the Bitcoin PoW (Hashcash) puzzle requires finding a nonce value that results in a hash value with the first 76 bits being '0'.

You can assume that the level of difficulty remains constant for the time frame considered in this question.

a) [2 marks]

What is the expected (average) time in days for Bob to solve a puzzle using his Antminer S19 Pro miner?

b) [2 marks]

Let's assume that the total hash rate in Bitcoin is 150 Exa hashes per second (150 * 10^18 hashes per second). Let's also make the simplifying assumption that all Bitcoin mining is done exclusively by Antminer S19 Pro miners. Each Antminer S19 Pro uses 3 kW (3,000 Watt) of power. Let's further assume 1 kWh (kilo Watt hour = 1,000 Watts of power used for the duration of 1 hour) costs $0.20. Finally, we assume that in Bitcoin each block has 2,000 transactions.

Based on these assumptions, calculate the electricity cost in $ per transaction in Bitcoin.

14) [3 marks]

Tendermint consensus uses each validator's deposit as its voting power in selecting the proposer for a round. Here, we assume that there are only two validators, P1 and P2. P1's deposit is twice of P2's deposit. As a result, the voting power of P1 is 2, and the voting power of P2 is 1.

Which validator is selected as the proposer in Round 1, Round 2 and Round 3 respectively? Show the relevant calculations.

Hint: At the beginning of each round, each validator's position in the queue (the initial position is 0) is updated by adding its voting power. The validator at the front of the queue is selected as the proposer. At the end of each round, the proposer's position (priority) in the queue is reduced by the total voting power.

15) [4 marks]

Consider the following Ethereum Smart Contract code.

```
pragma solidity >=0.7.0 <0.9.0;
contract Storage {
    uint256 number;
    function store(uint256 num) public {
        number = num;
    }
    function retrieve() public view returns (uint256){
        return number;
    }
}
```

a) [2 marks]

Write a constructor function for this smart contract to store the creator of the contract into a variable.

b) [2 marks]

Write a modifier and apply the modifier to the function ***store*** to ensure that only the creator of the contract can store values to the variable ***number*.**

Part C – Questions on Seminar Presentations

Answer 3 out of (5+1) QUESTIONS (30 MARKS)

10 MARKS PER QUESTION

IN THIS PART, THERE ARE **5 STANDARD QUESTIONS** AND **1 EXTRA QUESTION**.
SELECT 3 QUESTIONS TO BE ANSWERED OUT OF THE 5 STANDARD QUESTIONS, IF NONE OF THE STANDARD QUESTIONS ARE ON A TOPIC THAT YOU HAVE PRESENTED AS A SEMINAR.
IF ONE OF THE 5 STANDARD QUESTIONS IS ON YOUR SEMINAR TOPIC, YOU CANNOT SELECT THAT QUESTION. HOWEVER, IN THAT CASE YOU CAN ALSO INCLUDE THE EXTRA QUESTION IN YOUR POOL OF QUESTIONS FROM WHICH YOU CAN CHOOSE YOUR QUESTIONS.
ALL QUESTIONS IN THIS PART HAVE AN EQUAL WEIGHT OF **10 MARKS**.

16) Seminar Paper/Topic #31: Eclipse attacks on Bitcoin’s Peer-to-peer Network

- Explain the basic purpose and aim of an Eclipse attack on Bitcoin’s P2P network.
- Explain the key mechanisms and steps that are required for a successful Eclipse attack.
- Describe the possible countermeasures against the attack.

17) Seminar Paper/Topic #33: The Bitcoin Lightning Network

- What are the key limitations of Bitcoin that the Lightning Network is trying to address?
- Briefly explain the concept of micropayment channels.
- Explain the required steps for a payment to be made between two parties.
- What is the purpose of a Hashed Timelock Contract in this context?

18) Seminar Topic/Paper #73 IoT goes nuclear: Creating a ZigBee chain reaction

- Explain the basic flaw in the Philips Hue device that enables the attack described in the seminar/paper.
- Explain the basic concept of Differential Power Analysis (DPA).
- Explain how DPA is used in the attack described in the seminar/paper.
- Discuss the concept of *War Flying*, and how it is used in the attack discussed in the seminar/paper.

19) Seminar Paper/Topic #30: Hijacking bitcoin: Routing attacks on cryptocurrencies

- At a high level, explain the basic aims and methods of routing attacks on blockchains (cryptocurrencies), as discussed in the seminar and the paper.
- Explain the concept of BGP Hijacking in the context of Bitcoin.
- Discuss the potential impacts of a successful routing attack on a blockchain.

20) Seminar Paper/Topic #27: InterPlanetary File System (IPFS)

- What are the aims and claimed advantages of IPFS compared to traditional, centralised data storage?
- Explain the purpose of IPNS (InterPlanetary Name System).
- Explain the use of Distributed Hash Tables (DHTs) in IPFS.

Extra Question

21) Seminar: Topic/Paper #105: Password Cracking, Approaches and Tools

- Explain the attack scenario considered in this paper and discuss the basic concept of password cracking.
- Discuss the different types of password cracking approaches.
- Explain the concept of probabilistic password cracking and discuss how Context Free Grammars (CFGs) can be used for this.

END OF EXAMINATION