Coversheet for centrally scheduled online non-invigilated exams

Exam information	
Course code and name	**COMS4507/7507** Advanced Topics in Security
Semester	Semester 1, 2020
Exam type	Online, non-invigilated
Exam date and time	Please refer to your personalised timetable
Exam duration	Working time (90 minutes) + additional online allowance of 30 minutes. TOTAL exam duration: **2 hrs** from exam commencement time
Exam window	You must commence your exam at the time listed in your personalised timetable. The exam will remain open **only** for the duration of the exam.
Reading time	Reading time has not been formally allocated for online exams, however students are encouraged to review and plan their approach for the exam before they start. The total exam time should be sufficient to do this.
Additional time	30 minutes additional time has been incorporated in recognition of the online environment and the different circumstances that students face in their home environments. This includes allowances for network or connection issues.
Weighting	This exam is weighted at the percentage of your total mark for this course as shown below COMS4507: 50% COMS7507: 60%
Permitted materials	This is an open book exam – all materials permitted.
Required/recommended materials	Recommended materials: calculator, bilingual dictionary (if required)

Instructions	The exam consists of three parts, which are all to be done online as a Blackboard test. (There will be **NO** file upload.) **Part A** (20 marks) consists of 10 Multiple-Choice questions (2 marks each) on the lecture content **(Questions 1 - 10)**. Answer all questions in Part A. **Part B** (20 marks) consists of 5 Short Answer questions (4 marks each) on the lecture content **(Questions 11 – 15)**. Answer all questions in Part B. **Part C** (30 marks) consists of questions on **seminar** presentations **(Questions 16 – 20)**. • IN THIS PART, THERE ARE 4 STANDARD QUESTIONS AND 1 EXTRA QUESTION. • **SELECT 3 QUESTIONS** TO BE ANSWERED OUT OF THE 4 STANDARD QUESTIONS, IF NONE OF THE STANDARD QUESTIONS ARE ON A TOPIC THAT YOU HAVE PRESENTED AS A SEMINAR. • IF ONE OF THE 4 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. • IF A STUDENT ANSWERS MORE THAN 3 OF THE SEMINAR QUESTIONS, THE FIRST 3 ANSWERED SEMINAR QUESTIONS WILL BE MARKED AND COUNTED TOWARDS THE EXAM MARKS. **Total Exam Marks: 70**
Who to contact	*Given students may not all undertake the online exam at the same time, or in the same time zone, and that some questions may be randomised, responding to student queries and/or relaying corrections to exam content during the exam will not be feasible.* At the end of the exam, there is a free text box field (Question 21, with 0 marks). Please use this to specify any assumptions you have made in completing the exam, in case you thought there was some degree of ambiguity, and which questions those assumptions relate to. If you experience any **technical difficulties** during the exam, contact the Library AskUs service for advice. You should also ask for an email documenting the advice provided so you can provide this to the course coordinator immediately at *initial.surname@uq.edu.au*.>

Important exam condition information	This is an open book exam. You will have access to your own notes, course texts, and other materials. The normal academic integrity rules apply. • You cannot cut-and-paste material other than your own work as answers. • You are not permitted to consult any other person – whether directly, online, or through any other means – about any aspect of this assessment during the period that this assessment is available. If it is found that you have given or sought outside assistance with this assessment then that will be deemed to be cheating and will result in disciplinary action. By undertaking this online assessment you will be deemed to have acknowledged UQ's academic integrity pledge to have made the following declaration: *"I certify that my submitted answers are entirely my own work and that I have neither given nor received any unauthorised assistance on this assessment item"*.

Preview Test: COMS4507/7507 Semester One Final Examination 2020

Test Information

Description	COMS4507/7507 Final Exam
Instructions	Please refer to the Exam Cover Sheet for important details about the exam.
Timed Test	This test has a time limit of 2 hours.This test will save and submit automatically when the time expires. Warnings appear when **half the time**, **5 minutes**, **1 minute**, and **30 seconds** remain. *[The timer does not appear when previewing this test]*
Multiple Attempts	Not allowed. This test can only be taken once.
Force Completion	This test can be saved and resumed at any point until time has expired. The timer will continue to run if you leave the test.

QUESTION 1 **2 points** Save Answer

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

- ○ A. The Bitcoin scripting language ("Script") is a simple, stack based and Turing complete programming language.
- ○ B. Bitcoin uses the Istanbul Byzantine Fault Tolerant (IBFT) consensus protocol.
- ○ C. Bitcoin transactions need at least one input.
- ○ D. None of the other statements is correct.
- ○ E. Bitcoin is a public permissioned blockchain.

QUESTION 2

2 points Save Answer

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

- A. None of the other statements is correct.
- B. eCash is a Blockchain-based payment system.
- C. eCash uses digital signatures to verify the identity of users.
- D. For the bank to link a coin serial number to a customer, it needs to find a 32-bit SHA256 pre-image.
- E. Blind Signatures are used to prevent double spending.

QUESTION 3

2 points Save Answer

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

- A. In a Blockchain, a trusted third party is responsible for verifying the account balances of the unspent transaction outputs (UTXOs), which avoids double spending.
- B. One of the main inherent security benefits of a Blockchain is data privacy.
- C. None of the other statements is correct.
- D. A Blockchain is binary tree with linear (O(N)) search time.
- E. A hash pointer to the last block (head) of a blockchain protects the integrity of all the blocks in the in chain.

QUESTION 4

2 points Save Answer

Which one of the following statements regarding Merkle Trees is correct? (choose the best answer)

- A. Merkle Trees are named after the German Chancellor Angela Merkel.
- B. A Merkle Root is calculated as the hash of the two concatenated hash values of its two child nodes.
- C. In Merkle Trees, proofing membership is provided by showing a Merkle Path, which requires O(N) steps, i.e. the cost is linear in the number of nodes in the tree.
- D. The Merkle Root protects the authenticity of all the information stored in the tree.
- E. None of the other statements is correct.

QUESTION 5

2 points Save Answer

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

- A. Given a fixed amount of mining power, joining a mining pool increases the expected (average) mining revenue.
- B. On average, a new Bitcoin block is mined every 15 seconds.
- C. The total amount of available Bitcoin gradually increases, with 657,000 BTC being added every year.
- D. None of the other statements is correct.
- E. The Bitcoin mining reward consists of two parts, transaction fees and block rewards, which are provided in coinbase transactions.

QUESTION 6

2 points Save Answer

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. None of the other statements is correct.

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

D. 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.

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

QUESTION 7

2 points Save Answer

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

A. Bitcoin uses an "ASIC-resistant" Proof of Work algorithm.

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

C. The solution to a Bitcoin mining puzzle is a 32-bit integer.

D. None of the other statements is correct.

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

QUESTION 8

2 points Save Answer

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

- A. 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.
- B. Ethereum's transaction throughput can be improved by increasing the mining difficulty, as is the case in Bitcoin.
- C. Contract Accounts in Ethereum can send transactions and are controlled by a private key.
- D. None of the other statements is correct.
- E. 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.

QUESTION 9

2 points Save Answer

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

- A. The difference between the sum of the inputs and the sum of the outputs in a Bitcoin transaction represents the Block Reward.
- B. None of the other statements is correct.
- C. Bitcoin sent to a transaction "change address" represent a transaction fee, which is given to the node that mines the corresponding block.
- D. A transaction locking script requires the successful verification of the corresponding public key certificate.
- E. Inputs to a Bitcoin transaction consist of zero or more unspent transaction outputs (UTXOs).

QUESTION 10

2 points Save Answer

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

A. None of the other statements is correct.

B. Pay-to-pubkey-hash (P2PKH) addresses allow the implementation of complex transactions, e.g. “multisig” transactions.

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

D. Bitcoin addresses are represented in Base64 encoding.

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

QUESTION 11

4 points Save Answer

It is claimed that Isaac Newton invented Calculus in the late 1600s but he never published it. It is assumed that Gottfried Wilhelm Leibniz sometime later independently invented Calculus, and published the results. A major dispute followed between the supporters of the two mathematicians as to who was the inventor of Calculus (the “Calculus Controversy”).
Imagine that you are in a similar position to Newton, and that you have made a great discovery, e.g. you have invented a new algorithm that can efficiently factor large integers. For some unspecified reason, you do not want to publish or patent the algorithm at this point in time. However, you want to be able to proof at a later point in time, e.g. in 10 years’ time, that you knew the algorithm at the current time, i.e. on 8/7/2020.
Discuss if and how you could use a blockchain, e.g. Ethereum, to achieve this. Describe the mechanism, as well as the assumption you would have to make for this scheme to be secure and trustworthy.

QUESTION 12

4 points Save Answer

a) [2 marks] Explain the concept of function modifiers in Solidity. Considering the Solidity code of the '*Purchase*' smart contract shown below, discuss the use and impact of the modifier '*condition*' in the *confirmPurchase()* function.

b) [2 marks] Explain the concept of '*events*' in Solidity, and discuss their use in the '*Purchase*' smart contract shown below.

```
pragma solidity >=0.4.22 <0.7.0;

contract Purchase {
    uint public value;
    address payable public seller;
    address payable public buyer;
    enum State {Created, Locked, Inactive}

    State public state;

    constructor() public payable {
        seller = msg.sender;
        value = msg.value / 2;
        require((2 * value) == msg.value, "Value has to be
even.");
    }

    modifier condition(bool _condition) {
        require(_condition);
        _;
    }

    modifier onlyBuyer() {
        require(
            msg.sender == buyer,
            "Only buyer can call this."
        );
        _;
    }

    modifier onlySeller() {
        require(
            msg.sender == seller,
            "Only seller can call this."
        );
        _;
    }

    modifier inState(State _state) {
```

```
        require(
            state == _state,
            "Invalid state."
        );
        _;
    }

    event Aborted();
    event PurchaseConfirmed();
    event ItemReceived();


    function abort()
        public
        onlySeller
        inState(State.Created)
    {
        emit Aborted();
        state = State.Inactive;
        seller.transfer(address(this).balance);
    }


    function confirmPurchase()
        public
        inState(State.Created)
        condition(msg.value == (2 * value))
        payable
    {
        emit PurchaseConfirmed();
        buyer = msg.sender;
        state = State.Locked;
    }


    function confirmReceived()
        public
        onlyBuyer
        inState(State.Locked)
    {
        emit ItemReceived();

        state = State.Inactive;

        buyer.transfer(value);
        seller.transfer(address(this).balance);
    }
}
-----------------------------------------
```

QUESTION 13

4 points Save Answer

Satoshi Nakamoto, the pseudonym of the inventor of Bitcoin, is known to have mined the first block (genesis block), containing a single Coinbase transaction. As can be seen on the blockchain (e.g. using any Bitcoin blockchain explorer), the corresponding 50 BTC block reward has not been spent yet to this day. Over the years, a number of people have claimed to be Satoshi Nakamoto, without providing any convincing proof. If you were the inventor of Bitcoin, describe how you could convincingly proof to the world that you are indeed Nakamoto.

QUESTION 14

4 points Save Answer

Assume that you bought yourself a Dragonmint T16 ASIC Bitcoin miner, which can do 16 TH/s (16 * 10^12 hashes per second). Also assume that, at the current level of difficulty, solving the Bitcoin PoW (Hashcash) puzzle requires to find a nonce value that results in a hash value with the first 76 bits being '0'. (Answer both parts of the question, i.e. a) and b), in the corresponding text box. Show your work.)

a) [2 marks] What is the expected (average) time in days for you to solve a puzzle using your Dragonmint miner?

b) [2 marks] If the total Bitcoin hash rate is 100 Exa hashes per second (100 * 10^18), including your own modest contribution, what is the probability that you will be successful in mining the next block, i.e. that you will find a solution to the hash puzzle first?

QUESTION 15

4 points Save Answer

Discuss the differences between the Proof-of-Work (PoW) and Proof-of-Stake (PoS) blockchain consensus mechanisms. In particular, list the advantages and disadvantages of each approach.

QUESTION 16

10 points Save Answer

Seminar: Paper/Topic #68: Side-Channel Leaks in Web Applications

- Explain what side channel attacks are in general?
- Explain how side channel attacks on Web Applications work, if all communication is encrypted via TLS/SSL. Explain how information can be extracted?
- Discuss potential mitigation approaches against these types of Side-Channel Leaks.

QUESTION 17

10 points Save Answer

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.

QUESTION 18

10 points Save Answer

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/cryptocurrency.

QUESTION 19

10 points Save Answer

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 DNSLink in IPFS.
- Explain how integrity is protected for data stored on IPFS.
- Explain the use of Distributed Hash Tables (DHTs) in IPFS.

QUESTION 20

10 points Save Answer

This is an EXTRA Seminar Question. You can only choose this question if one of the other 4 (regular) Seminar Questions is on the topic that you presented.

Paper/Topic #71: Anonymous connections and onion routing

- What is Onion Routing trying to achieve? What type of attacks is it trying to prevent?
- How does Onion Routing work? Describe the high-level concepts.
- What information can an attacker gain by compromising a single Onion Router?

QUESTION 21

0 points Save Answer

This text box can be used to make any comments about assumptions that you made for answering any questions in Part A (Questions 1-10), if you feel that there is any ambiguity in the question formulation. For all the other questions, the relevant comments can be made in the corresponding answer text box.