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, 2019

COMS4507/7507 Advanced Computer and Network Security

This paper is for St Lucia Campus students.

Examination Duration: 90 minutes

Reading Time: 10 minutes

Exam Conditions:

This is a School Examination

This is an Open Book Examination

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)

Calculators - Any calculator permitted - unrestricted

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.
Choose and answer 3 questions in Part B.

Total Marks: 55

For Examiner Use Only

Question	Mark

Total _____

Part A – Short Answer Questions and Problems
8 Questions (25 Marks)

ANSWER ALL QUESTIONS IN PART A

MARKS PER QUESTION AS INDICATED

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

1) [3 marks]
Traditional consensus algorithms for distributed systems, such as PBFT etc., have been around for quite some time before Bitcoin. What is the key innovation and key differences in the way in which Bitcoin achieves consensus, compared to the traditional distributed systems consensus approaches?

2) [3 marks]
Consider the eCash system, as discussed in the lecture.

a) [1 mark] How does eCash prevent double-spends?

b) [2 marks] Discuss the differences of eCash and Bitcoin in regards to transaction anonymity.

3) [4 marks]
Consider a Blockchain system with a HashCash-based Proof of Work (PoW) system, similar to the one used in Bitcoin. The PoW system requires finding a partial pre-image for a block header, which includes a 256-bit nonce field. To solve the PoW puzzle, we can try different values for the nonce, hash the block, and check if we get the desired result. The current difficulty of n=40 means the first 40 bits of the hashed block header have to be zero.

a) [2 marks] Using his desktop computer, it takes Bob on average 1 hour to find a valid solution to the PoW puzzle. If the difficulty is changed to n=52, how long would it take Alice on average to find a valid solution, if the hash rate of her computer is 100 greater than Bob's?

b) [2 marks]
Assume that all block header fields, except for the nonce, are fixed and cannot be changed in order to find a solution to the puzzle. Assuming a difficulty of n=40, discuss the impact of changing the size of the nonce field to 32 bits. What is the probability that a solution can be found for a given block?

4) [4 marks]
Bitcoin and Public Key Cryptography

a) [2 marks] Explain how and for what purpose Public Key Cryptography is used in Bitcoin.

b) [2 marks] In traditional Public Key Cryptography systems, we use Certificate Authorities (CAs) and Public Key Certificates to guarantee the authenticity of public keys. Explain how this is achieved in Bitcoin.

5) [3 marks]
List the key differences between Bitcoin's and Ethereum's current consensus mechanisms.

6) [3 marks]
Explain what a Merkle Tree is, and how it is used in Bitcoin.

7) [3 marks]
Alice, Bob, Charlie and Dave are using Shamir's method to implement a (3, 4)-threshold secret sharing scheme, to share a secret message *M*.

Their respective shares are as follows:

Alice: $(x_A, y_A) = (1, 4512)$
Bob : $(x_B, y_B) = (2, 4521)$
Charlie: $(x_C, y_C) = (-1, 4506)$
Dave : $(x_D, y_D) = (-233, 107879)$

Using these shares, reconstruct the secret *M*.

8) [2 marks]
Explain the purpose of Gas in Ethereum.

Part B – Questions on Seminar Presentations

Answer 3 out of (4+1) QUESTIONS (30 MARKS)

10 MARKS PER QUESTION

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 (13) IN YOUR POOL OF QUESTIONS FROM WHICH YOU CAN CHOOSE YOUR QUESTIONS.

ALL QUESTIONS IN PART B HAVE AN EQUAL WEIGHT OF **10 MARKS**.

9) Topic/Paper #57 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.

10) Topic/ Paper/Topic #40 *Lest We Remember: Cold Boot Attacks on Encryption Keys*

- Describe the basic concept of a Cold Boot Attack and the underlying physical effects.
- Describe the process of recovering encryption keys.
- Discuss how the attack can be used on disk encryption systems.

11) Topic/Paper #52: Honeywords: Making password-cracking detectable

- What is the key problem that the paper is trying to address? What is the attack scenario that it considers?
- What are the benefits of using Honeywords?
- Describe the role of the Honeychecker.

12) Paper #46: Chip and PIN is Broken

- What is the purpose of the EMV protocol discussed in the paper?
- Explain the basic concept of how the EMV protocol works and briefly describe the 3 protocol phases.
- Explain the basic flaw in the EMV protocol that allows the attack described in the paper.
- Explain the key steps of the attack.

Extra Question

13) Topic/Paper #75: Password Cracking, Approaches and Tools

- Explain the basic concept of password cracking.
- Discuss the different types of password cracking approaches.
- Explain how Context Free Grammars (CFGs) can be used for password cracking.

END OF EXAMINATION