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, 2018

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 - Casio FX82 series or UQ approved (labelled)

Materials To Be Supplied To Students:

1 x 14 Page Answer Booklet

Instructions To Students:

Answer all questions in Part A.
Choose and answer 3 questions in Part B.

All questions are to be answered in the provided answer booklet.

Marks per question are as indicated.

Total exam marks: 55

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

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]

John, Bob, Karl and Charlie use Shamir's method to implement a (3, 4)-threshold secret sharing scheme to share the secret K. Computations are done in GF(11), i.e. modulo 11.

Bob's, Charlie's and Karl's shares are as follows:
Bob: $(x_B, y_B) = (3, 5)$
Charlie: $(x_C, y_C) = (5, 4)$
Karl: $(x_K, y_K) = (9, 7)$

Compute the shared secret K.

2) [3 marks]

Consider the following XOR based secret sharing scheme. The secret to be shared is a 100-bit message M. In the scheme, we generate 4 shares as follows:

X1: random
X2: random
X3: X1 XOR X2
X4: choose so that M = X1 XOR X2 XOR X3 XOR X4

('XOR' represents the bitwise Exclusive OR operation.)

Discuss if this approach is secure, i.e. if it meets the requirements of secret sharing schemes as discussed in the lecture. Explain your answer.
(Tip: A value XOR'ed by itself is 0, which is the neutral element of the XOR operation.)

3) [4 marks]

Explain the distributed consensus mechanism in Bitcoin and its key components.

4) [3 marks]

Explain what a Merkle Tree is, and how it is used in Bitcoin.

5) [2 marks]

Explain how Bitcoin prevents the counterfeiting of coins, i.e. the creation and spending of fake coins.

6) [3 marks]

Consider the following proof of work puzzle as an alternative to the current hash-cash based approach in Bitcoin.

Solving the puzzle consists of multiplying two very large integers, e.g. with thousands of digits each.

Discuss pros and cons of this proof of work approach in the context of Bitcoin.

7) [2marks]

Explain the purpose of blind signatures in David Chaum's eCash system.

8) [5 marks]

a) [2 marks]

Assume the entire Bitcoin network has a total hash rate of 30 Exa hashes per second ($30 * 10^{18}$ hashes per second).

Alice has bought herself a new Dragonmint 16T ASIC miner for $3,000, with a hash rate of 16 TH/s ($16 * 10^{12}$ hashes per second).

We assume a block is mined every 10 minutes (on average), the block reward is 12.5 BTC (Bitcoin), and one BTC is worth $10,000. To keep things simple, we also assume the total hash rate and the mining difficulty remain constant.

On average, how much revenue (in $) can Alice expect to receive from her mining operation in a period of one month (30 days)? You can ignore transaction fees in your calculation.

b) [2 marks]

What is the expected time for Alice to solve a Bitcoin mining puzzle?

What is the probability that it will take Alice more than 10 years to find a solution to a puzzle?

c) [1 mark]

Considering the results in questions a) and b), what is the key benefit of joining a mining pool?

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) Paper #30: *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.

10) Paper #44: The Web never forgets: Persistent tracking mechanisms in the wild

- Describe the general concept of persistent tracking.
- Explain the concept, aim and mechanisms of cookie respawning.
- Explain how canvas fingerprinting works and what it is trying to achieve.
- Discuss potential defences against canvas fingerprinting.

11) Paper #42: 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 #36: 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) Paper/Topic #38: Side-Channel Leaks in Web Applications

- Explain what side channel attacks are in general?
- Explain how side channel attacks over Web Applications that are secured via TLS/SSL can work. What is the main mechanism by which information is leaked?
- Explain how the *autocomplete* or *autosuggest* feature increases the vulnerability to this kind of attack.

END OF EXAMINATION