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

SAMPLE EXAM

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 NOT 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

Rough paper

Materials To Be Supplied To Students:

1 x 14 Page Answer Booklet

Rough Paper

Instructions To Students:

Total Marks: 70 Part A: 30 Marks - Answer ALL Questions Part B: 40 Marks - Answer 4 of 5 Questions FOR QUESTIONS THAT REQUIRE CALCULATIONS, YOU NEED TO SHOW INDIVIDUAL STEPS OF HOW YOU ARRIVED AT THE RESULT

For Examiner Use Only

Question	Mark

Total ________

Part A – Short Answer Questions and Problems
6 Questions (30 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) [4 marks]
Alice, Bob, Charlie and Debbie use Shamir's method to implement a (2, 4)-threshold secret sharing scheme to share the secret K. Computations are done in GF(7), i.e. modulo 7.

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

Compute the shared secret K.

2) [6 marks]

Answer the following questions regarding Man-in-the-middle attacks in wireless networks.

a) [3 marks] Describe how a wormhole attack is conducted against a multi-hop wireless network and describe the potential impact.

b) [3 marks] Describe in detail how temporal packet leashes can be used to detect a wormhole attack.

3) [4 marks]

Briefly describe the general concept and purpose of Blind Signatures. Explain how the blinding operation can be performed in RSA.

4) [4 marks]
In a Shamir secret sharing scheme, the secret is the constant term *c* of a polynomial of degree 4. Computations are done in GF(991), i.e. modulo the prime 991.

Suppose Alice, Bob and Susie have the following three shares: (2, 197), (4, 874), (13, 547).

How many possibilities are there for the secret? How much information can be gained from the three shares? Explain your answer.

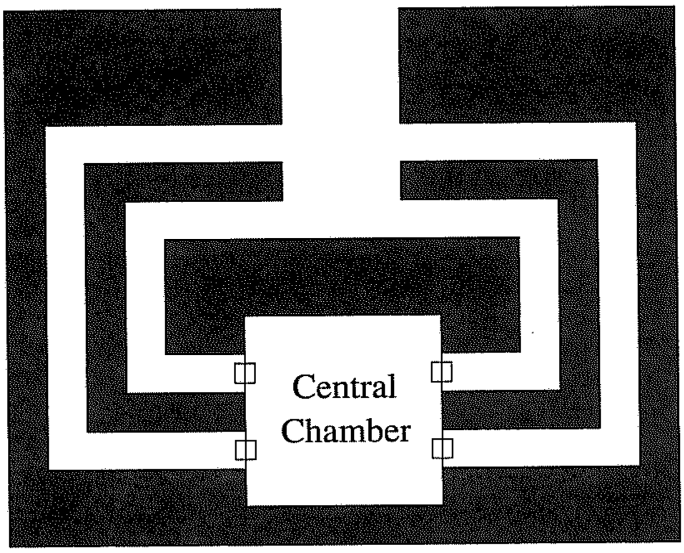
5) [6 marks]
Generate two valid shares for a secret K=30 in a (3, 4)-threshold secret sharing scheme (Blakely's method). Computations are done in GF(37). Explain the individual steps involved.

6) [6 marks]

Consider the diagram of tunnels in the figure below. Suppose each of the four doors to the central chamber is locked so that a key is needed to enter, but no key is needed to exit. Peggy claims she has the key to one of the doors.

Devise a zero-knowledge protocol in which Peggy proves to Victor that she can enter the central chamber. Victor should obtain no knowledge of which door Peggy can unlock.

How many rounds of the interactive proof are necessary until Victor has at least 99.95% certainty that Peggy has the key?



Part B – Text Questions

5+1 QUESTIONS (40 MARKS)

10 MARKS PER QUESTION

IN THIS PART, THERE ARE **5 STANDARD QUESTIONS** AND **1 EXTRA QUESTION**.

SELECT 4 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, BUT YOU CAN ALSO INCLUDE THE EXTRA QUESTION (12) IN YOUR POOL OF QUESTIONS FROM WHICH YOU CAN CHOOSE 4 QUESTIONS FROM.

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

7) Paper #14: A convenient method for securely managing passwords

- What is the problem the proposed mechanism is trying to address?
- What is the basic idea of the proposed password management scheme?
- Explain the basic steps of how passwords are generated?
- Explain the role of the two parameters *k1* and *k2*.

8) Paper #16: The TESLA Broadcast Authentication Protocol

- What is the TESLA protocol trying to achieve, and what are possible application scenarios?
- List the key benefits of TESLA compared to alternative approaches.
- Explain the basic concept of how TESLA works.
- Explain why loose time synchronisation is required, and discuss what can happen if this time synchronisation is lost.

9) Paper #2: Vanish: Increasing Data Privacy with Self-Destructing Data

- Describe the problem that Vanish is trying to solve.
- Describe how data is encapsulated in a VDO, and describe the relevant parameters.
- Describe how secret sharing is used in the context of Vanish, and discuss the relevant parameters.
- Describe how a DHT is used in Vanish.

10) Paper #10: 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.

11) Paper #12: 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.
- Discuss possible approaches for mitigation of the problem.

Extra Question

12) Paper #5: Bitcoin: A Peer-to-Peer Electronic Cash System

- What is the goal of Bitcoin, and what are its key differences to other electronic cash systems?
- Explain the different methods of acquiring bit coins.
- Explain the basic steps in a Bitcoin transaction.
- How does Bitcoin prevent double spending of coins?

END OF EXAMINATION