

**Family Name:**

**Other Names:**

**Signature:**

**Student Number:**

**This PAPER is NOT to be retained by the STUDENT**

The University Of New South Wales  
**COMP3441/9441 Skeleton Final Exam**  
Cryptography and Security  
November 2006

Time allowed: **3 hrs**  
Number of questions to answer: **14**  
Total number of marks: **101**

You must hand in this entire exam paper, the answer booklets, your reference sheet, and any reference material. Failure to do so will result in zero marks for the course and a charge of academic misconduct.

Do not use red pen or pencil in this exam. You may bring and refer to one reference sheet of A4 paper containing your name, student number, and any notes you wish. Scientific calculators may be used. Computers, programmable calculators, calculators capable of storing text, mobile phones, or other devices capable of wireless communication are not permitted. Use or possession of a non-permitted device will result in zero marks for the course and a possible charge of academic misconduct.

**Before you start:** Fill in all of the details on the front of *each* answer booklet, and SIGN each booklet. Do the same for this pink question paper. Check your name and student number are written clearly on your reference sheet. Flip the answer booklets over and turn them upside down - you must write your answer on the *last* pages of the booklet.

**There is one mark for following the examination instructions.**

<b>Examiner's Use Only</b>												
	Inst	p2	p4	p6	p8	p10	p12	p13	T1	T2	Total	

## Part A: Short Answer Questions

Answer these questions in the spaces provided below on **this pink question paper**. DO NOT answer these questions in one of the answer booklets!

Write your answers clearly. Keep your answers neat and very brief. Messy or long answers will not be marked.

In this part if you do not wish your answer for a question to be marked clearly write “*1 sympathy mark please*” in the space for the answer. If you do this as well as writing an answer, the answer will **not** be marked. If a question has consists of multiple subquestions writing this for any subquestion will result in one mark being awarded for the entire question.

Where a question is divided into sub-questions the sub-questions may not be worth equal marks.

Each question in this part is worth 6 marks.

**Question 1**

Compare and contrast the following concepts:

1. *blah and blah* and *encryption* \_\_\_\_\_

---

---

2. *bling* and *blong* \_\_\_\_\_

---

---

3. *mean-it* and *penut* \_\_\_\_\_

---

---

**Question 2**

You are a blah...

**I think the pootle is:** \_\_\_\_\_

**Because** \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Question 3**

Suppose you have invented a ...

**Is this blahblahblah than simply blahblahblah? (give brief reasons)**

---

---

---

**To what extent does blahblahblah?**

---

---

---

---

---

## Question 4

## Question 5

Distributed with your exam paper is a special reference sheet/thingo showing...  
question? \_\_\_\_\_

Reason 1:

Reason 2:

Reason 3:

**Question 6**

## Question 7

background to the question...

Your response:

## Question 8

**Question 9**

**Question 10**

## Part B: Long Answer Topics

Select and answer *TWO only* of the following *FOUR* topics.

Answer each topic in a separate booklet. Clearly write the topic letter on the back of each booklet in big digits AND fill in the two boxes below

Write your answers in the *back* of the answer booklet. (You will need to flip the booklet over and turn it upside down). Write your answer on a pair of facing pages inside the booklet. This lets us mark the booklet without seeing your name first.

Your answer must take no more than two pages. We will only mark the first two uncrossed-out pages inside the booklet (counting from the back of the booklet).

Make your answers as clear and easy to understand as possible. Provide diagrams and brief comments where necessary. Confusing, difficult to understand or illegible answers will lose marks.

I have chosen to answer topic  and topic   
Each topic is worth 20 marks.

### Topic A

### Topic B

(i) question?

(ii) Describe the most significant ...

(iii) Briefly describe one alternative....

*Divide your answer into 3 parts labeled (i) (ii) and (iii) corresponding to the questions above. Devote roughly half of your time and space to (ii), and a quarter to each of (i) and (iii).*

## Topic C

(i) State ...

(ii) Blah. Draft your response to him. You may use point form if you wish.

*Put the most important points first in your response. You should plan your answer carefully before starting writing.*

*Divide your answer into 2 parts labeled (i) and (ii) corresponding to the questions above. Devote roughly half of your time and space to each.*

## Topic D

Blah blah blah. Construct a two page threat tree against harm to one of these assets (state the asset at the top of the tree). There is no need to attach likelihood estimates to threats.

*Expand at least one part of the tree to produce leaf nodes to show us you know how to do this. Other than that your answer should aim for comprehensive coverage taken to a few levels of expansion, rather than a partial coverage of threats expanded all the way to leaf nodes.*