

**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 Trial Exam**  
 Cryptography and Security  
 Sample Paper (2004)

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

You must hand in this entire exam paper, the answer booklets, and your reference sheet. Failure to do so will result in zero marks for the subject and a possible 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, or devices capable of wireless communication may not be used. Use or possession of a non-allowed device will result in zero marks for the subject 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. Write *WORKING ONLY* on the front of one answer booklet. Flip the answer booklets over and turn them upside down - you must write your answer on the *last* two pages.

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

Examiner's Use Only											
	Inst	A	12	13	14	15	16	C	D	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.

Each question is worth 5 marks.

## Question 1

What is the difference between a MAC and a plain hash?

---

---

---

---

When would you use a MAC rather than a plain hash?

---

---

---

---

## Question 2

Here is a diagram of a network configuration:

Here are the rules for the network adaptor marked 'A' on the firewall:

Briefly explain what traffic is permitted on this network and what is not.

**Allowed:** \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

**Not allowed:** \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

### Question 3

How much work is needed to find a (any) collision in an ideal 128 bit hash function? Given a hash value how much work is needed to find a preimage for that value? Explain your answers.

Collision: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Preimage: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

## Question 4

Give an example of how an attacker could use social engineering to burgle your house without breaking in.

---

---

---

---

---

---

---

---

---

---

## Question 5

You are a security consultant. Which clients would you suggest install an IDS and what would you recommend? (ie what type(s) of IDS, not what brandnames). Briefly explain your recommendations.

---

---

---

---

---

---

---

---

---

---

## Question 6

Give arguments for and against the use of firewalls.

**For:** \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

**Against:** \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

## Question 7

Give snort rules to detect ...

---

---

---

---

---

---

---

---

---

---

## Question 8

What is ARP and what is it used for?

---

---

---

---

Explain the mechanics of poisoning an ARP cache.

---

---

---

---

## Question 9

Explain how a buffer overflow attack works.

---

---

---

---

How could a local user on a host use a buffer overflow attack to get root access on the host?

---

---

---

---

## Question 10

Here is an encrypted IP packet which an attacker has extracted from a WEP frame.

```
11110000111100001111000011110000
00001111000011110000111100001111
11110000111100001111000011110000
00001111000011110000111100001111
11110000111100001111000011110000
00001111000011110000111100001111
11110000111100001111000011110000
00001111000011110000111100001111
...
```

Clearly mark the bits they could to change before retransmitting the packet to have it decrypted by the Access point and transmitted to their own network in the clear.

State why you selected these bits.

---

---

How would the bits need to be changed? (you don't need to give the new bits, just say how they would have to be calculated)

---

---

---

---

## Question 11

In this simplistic example suppose an authority uses a public RSA key ( $e=11, n=85$ ) to sign documents. You wish them to sign your message (which is the number 42) but you don't want them to know what they are signing so you use a blinding factor "r" of 11.

In your calculations you may wish to use the following results:

$$11 * 35 = 1 \pmod{64}$$

$$11 * 31 = 1 \pmod{85}$$

Show brief working.

What number should you give the authority to sign?

---

What number will the authority give back to you?

---

Extract the signature for 42 from this number.

---

Verify this answer using the private key.

---

## Question 12

Give a zero knowledge protocol for proof of identity and explain why each step is needed.

---

---

---

---

---

---

---

---

---

---

## Part B: Long Answer Topics

Select and answer *TWO only* of the following 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). 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 of any answer (counting from the back of the book).

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

You are the IT manager for a large law firm "Wiley and Fox". Your firm is representing an Australian Telecommunications Company "Telstrus" in a trial against company "BadGuy" which provides internet pornography. BadGuy is a wealthy company registered in the Bahamas. They have significant telecommunications and technical expertise.

What, if anything, should you be doing as IT manager? Set out your plan in point form and give brief explanations as to your reasons.

#### **Background:**

*The trial is due to start in one month and will last for about one month. Preparation for the trial started over a year ago but a large amount of work remains to be done in the final weeks before trial, and once the trial has commenced. A number of witnesses will be called by both sides to testify about various documents and their recollection of past events. Wiley and Fox have engaged the barrister "H. Rumpole" to argue their case in court.*

*Over the next eight weeks before the trial finishes solicitors in your firm will be interviewing and preparing Telstrus' witnesses, planning the questions to ask BadGuy's witnesses, preparing documents to be presented to the court, and will be in constant communication with Rumpole and Telstrus about the facts of the case and planning the trial strategy.*

*If BadGuy wins all their claims they will win \$20 million from Telstrus plus get all their legal fees back, if they lose all their claims they could lose up to \$10 million in cross claims and legal expenses. So far BadGuy has spent over \$2 million in legal expenses. At any point in the proceedings if either party feels they are going to lose they can enter into negotiations with the other side to terminate the trial and settle for a sum of money agreeable to both parties.*

### Topic B

Your company is engaged in confidential negotiations with another company. In what ways could rivals use sniffing to get this commercially sensitive data? For each way say what you could do to minimise the risk.

*tip - devote more space in your answer to the biggest risks*

### Topic C

Outline proposed and attempted attacks on the AES/Rijndael algorithm. In your response

include an analysis of a range of types of attacks including Side Channel attacks as discussed in lectures. For each attack or type of attack explain whether or not it is feasible. Finally, contrast how susceptible to attack Rijndael is in comparison to the other 4 finalists of the AES competition.

## **Topic D**

*a question about Firewalls*

## **Topic E**

*a question about Number Theory*

## **Topic F**

*a question about Intrusion Detection Systems*

## **Topic G**

*a question about Honeypots*

## **Topic H**

*a question about Denial of Service*

## **Topic I**

*a question about Spam*

## **Topic J**

*a question about On-line elections*

## **Topic K**

*a question about Malware*