

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 Final Exam
Cryptography and Security
November 2005

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, and your reference sheet. Failure to do so will result in zero marks for the course 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, 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.

Examiner's Use Only												
	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.

Each question is worth 5 marks.

Question 1

To what extent would not running the BSD "r" services prevent attacks based on the method allegedly used by Kevin Mitnick against Tsutomu Shimomura's computers on Christmas 1994? Justify your answer.

To what extent: _____

Justify: _____

Question 2

Suppose images from speed cameras are processed by the Digital Image Department (DID) of the Roads and Traffic Authority who compute the MD5 hash of each image and record the hash in a secure RTA database.

You've been called as an expert witness by a motorist challenging a photo which appears to show them speeding. The photo was processed by the DID in 2003.

You have been asked to comment, in light of MD5 being broken (by Xiaoyun Wang, Dengguo Feng, Xuejia Lai, and Hongbo Yu) in 2004, whether or not the photo could have been maliciously altered after being processed by the DID - without changing the hash value.

Answer, giving brief reasons:

Would your answer be different if the image had been processed by the DID in 2005 instead of 2003? Briefly explain why not or why:

Question 3

Renowned stage magician Harry Houdini (1874-1926) was outraged by psychics and mediums after some attempted to con him during his despair at his mother's death. He became a passionate debunker of mediums, delighting in publically exposing fakes.

He publically announced that he would try to contact his wife Bess via mediums after his own death and privately worked out a protocol with her to prevent the mediums cheating. He (correctly) anticipated that after his death mediums would try to pretend his spirit was in touch with them and would claim that he was saying they were not fakes after all.

Suppose you are Houdini and you need to devise the protocol to share with your trusted partner.

State and briefly justify the most important properties the protocol should have:

Give your protocol:

(Sadly the actual protocol which the real Houdini devised was flawed).

Question 4

How is an HMAC computed?

Briefly explain why HMACs are not vulnerable to length extension attacks or prefix attacks.

Question 5

An accountant has just resigned from his old partnership and is setting out on his own so he can spend more time with his family. He has set up a small home office and wants to connect it to his existing home broadband connection. He has a powerful desktop machine he will use for his work and is intending to buy a laptop and would like to have wireless access throughout the house. He has asked you to evaluate his security. Outline the *threat model* you will use.

Question 6

After the accountant from the previous question received your report he was so impressed he asked you to design design a network suitable for his present and likely future needs and implement firewall protection.

Explain your design and firewall setup with your reasons. Draw and label a diagram of the network and give the firewall rules in iptables format.

Question 7

Bruce Schneier writes:

... under some digital signature laws (e.g., Utah and Washington) ... you are not allowed to repudiate [your] signature. In other words, ... if your signing key has been certified by an approved CA, then you are responsible for whatever that private key does.

Decide: should Australia have such a law? Justify your decision by briefly describing the major advantages and disadvantages. *Note there are no marks for your decision, only for your arguments.*

In your answer say which parties would most benefit from such a law and which parties might be most disadvantaged.

Should Australia have such a law? _____

Advantages and Disadvantages:

Parties who benefit:

Parties disadvantaged:

Question 8

Your (slightly out of date) boss bursts into your office holding Microsoft Security Bulletin MS05-038. He shows you the following:

JPEG Image Rendering Memory Corruption Vulnerability - CAN-2005-1988

A remote code execution vulnerability exists in Internet Explorer because of the way that it handles JPEG images. An attacker could exploit the vulnerability by constructing a malicious JPEG image that could potentially allow remote code execution if a user visited a malicious Web site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

“How could this be possible??!!” He asks, looking bewildered. Explain to him the nature of the vulnerability and how an exploit could take advantage of it. There are a number of things Microsoft could have done to try to prevent the vulnerability from arising in the first place. State an important one.

Answer him assuming he has studied computing but has not taken a security course.

Vulnerability _____

Exploit _____

Microsoft could have...

Question 9

Suppose Google are setting up a new office in Sydney, for a team developing some exciting new secret google project. You have been asked to design the physical site security by the Chief Security Officer. In point form give the main parts of the threat model for the new office and, using that, write a brief policy for physical site security.

Use whatever format you like for the policy, including bullet points, but make it clear.

Threat model: _____

Physical site security policy:

Question 10

You are the security engineer at Nimbin University. Local police have shown you an intercepted ciphertext message. How might you be able to determine whether a polyalphabetic substitution cypher (such as Vignere) was used as opposed to a modern symmetric cypher (such as AES) without decrypting the message?

Question 11

The following article about DNSSEC is from Wikipedia, the free encyclopedia.

DNSSEC (short for DNS Security Extensions) adds security to the Domain Name System (DNS) used on Internet Protocol networks. It is a set of extensions to DNS, which provide:

- * origin authentication of DNS data
- * data integrity, and
- * authenticated denial of existence

DNSSEC was designed to protect the Internet from certain attacks such as DNS cache poisoning. All answers in DNSSEC are digitally signed. By checking the signature, a DNS resolver is able to check if the information is identical (correct and complete) to the info on the authoritative DNS server.

DNSSEC does not provide confidentiality of data.

Reducing the risk of one type of threat often increases the risk of another. State and explain how this might happen if DNSSEC starts to replace DNS in general use on the internet.

Threat that is reduced: _____

Threat that is increased: _____

Question 12

```
#include <stdlib.h>

int main(int argc, char *argv[])
{
    char text[1001];
    // a buffer to store the input argument so it is stored
    // in a local variable and hence saved on the stack

    strncpy(text, argv[1],1000); // no stack overflow with strncpy
    text[1000] = 0;             // ensure it is null terminated

    // store the "hidden" value
    char hidden;
    hidden = *argv[2];

    static int secret;
    secret = 0x42424242; // set this to your own secret before compiling

    printf (text);

    return 0;
}
```

Briefly explain state the vulnerability in the above code.

What input could you enter to exploit the above vulnerability to discover the value of `hidden`?

Suppose you knew the address of `secret` but not its value. Briefly explain, with an example, how would you determine an input to exploit the above vulnerability and discover the value of `secret`?

Part B: Long Answer Topics

Select and answer *TWO only* of the following *THREE* 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 Chief Information Officer of the School of Engineering and Computer Science at the University of South Wales (USW). You are head of the Computer Services Section (CSS). The CSS purchase, install, and maintain all the school's extensive hardware and software, and administer the school's servers and lab machines.

The CSS currently consists of 50 staff but it has just been announced that due to the school's tight financial situation 15 of the staff will be retrenched next year. At this stage it is not clear who will stay and who will go and you are aware that there is a fair degree of concern and anger in the CSS about the planned retrenchments.

What are the security concerns of the situation? Write a brief (2 page) plan setting out the concerns and how you will address them.

Topic B

You are an inventor who has discovered a way of constructing a new molecular lattice. You would like to sell your idea to a large company but do not wish to show them how to construct the lattice until they have paid you. They do not wish to pay you unless you can demonstrate that you do know how to construct the lattice.

In industrial metallurgy constructing molecular lattices is equivalent to solving jigsaw puzzles as follows:

The puzzle has 10,000 identically sized square pieces to be arranged in a 100×100 grid. Each side of a piece has been assigned a number between 0 and 25. The four sides on a piece are always assigned distinct numbers, but the same number can appear on more than one piece.

The pieces of the puzzle are not a secret - the secret is how to arrange them to form a legal 100×100 grid. A grid is legal if touching sides of adjacent pieces have the same number. A piece may be placed in any unoccupied position on the grid and it may be rotated to any of the 4 possible orientations, but it may not be flipped over.

Give a zero knowledge computer protocol you could use to convince the company that you know how to solve the jigsaw puzzle without revealing any information about your solution except that it is a legal solution. Justify the steps in your protocol and explain why it is zero knowledge.

Topic C

The following is an extract from The Age, Wednesday September 21, 2005.

Cited at <http://theage.com.au/articles/2005/09/19/1126981991083.html>

Double jeopardy

September 20, 2005

As personal online banking takes off, so the risk of fraud grows, reports Nick Galvin.

When nearly \$5000 suddenly disappeared from their bank account with no explanation, Janet France and her partner Robert felt like they had been mugged.

"It felt like we had walked out and somebody had said 'stick your hands up', taken our wallet and walked off," France says. "We felt completely vulnerable because we are not really high-tech people."

High-tech or not, the couple had fallen victim to identity theft.

Robert first noticed the \$4754 was missing when he checked the account on France's computer. The Northbridge pair immediately reported the loss to the police and their bank, completing a statutory declaration to say the transaction was unauthorised.

But the bank was far from sympathetic.

"Immediately, they went into this impersonal, defensive mode. (They) said you have to prove what has happened," France says. "They started to harass us, in a sense ... they started saying, 'Well, you've got to prove that you have all the security on your PC.' "

Luckily, France is assiduous in keeping her virus-checking software up to date and regularly runs anti-spyware programs, so she was able to provide the records demanded.

"Basically we heard nothing. Then, probably two months later, the money just mysteriously reappeared in our account," she says.

In March 2005 the Guardian newspaper reported that attacks on online bank accounts had more than trebled over the previous six months.

- (i) Explain the types of attacks used on online bank accounts
- (ii) How would two factor identification help, and how could it be implemented?
- (iii) What other defenses could banks or their customers use to help solve this problem?

Tip: Devote roughly equal time and space to each of the three questions above.