

# COMP3441/9441 Assignment 1

Due 26 Sept. 2003, 5pm

## Submission instructions

- Each submission should include your name, student number, and submission date on top of the first page, or on a cover page. Please underline your surname/family name. Write clearly that the submission is Assignment 1, Session 2, 2003. Hand-written assignments are acceptable, but marks will be deducted for illegible work.
- Hand in your assignments at the CSE school office, ground level, K17.
- This assignment is worth 25% of your total mark for the subject. Late submissions will be penalized by deducting 5 marks from your score for each day late.
- **Plagiarism:** You are reminded of the school's policy on plagiarism (See <http://www.cse.unsw.edu.au/school/facilities/yellowform.html>) You may discuss the *general approach* to solving a problem with other students, but your specific solutions on this assignment must be your own work. You must cite the source of any other author's material that you include. Anyone found to have plagiarised on any part of this assignment will be awarded 0 marks for the whole assignment.

## Question 1 [5 marks]

This question requires you to perform cryptanalysis on a piece of text. It has been encrypted with a substitution cipher, and digits and punctuation characters have been removed prior to encryption. Also, the whole text has been converted to lowercase letters.

The piece of text you need to crack depends on your student number. We have made available 100 different pieces of ciphertext, which are available from the subject webpage. They have names in the range `00.txt`, `01.txt`, ..., `99.txt`. You must use the text file that corresponds to the last two digits of your student number. For instance, Alice with student number 1234567 would download and attempt to crack `67.txt`. Using appropriate tools, you need to find the substitution function and recover the plaintext. Unix commands that will be of value to you in your endeavors include:

- `tr`
- `wc`
- `charcnt`

Help on using `tr` and `wc` can be found by typing `man command`. `charcnt` is not installed on the lab computers. Instead, you need to download it from the subject webpage. No help is available for this command, but the C source code is available to you. You need to compile it yourself, using the command `gcc -o charcnt charcnt.c`.

In your assignment submission, you should explain the steps you took to crack the cipher. Also, you need to separately submit the substitution function and the recovered plaintext as files. Submission instructions for these files will be available soon on the webpage.

**Question 2 [6 marks]**

Carol has a single bit secret that she is about to reveal to the world. (Is she accepting Ted's marriage proposal or not?) Carol has already told the secret to her good friend Alice. Alice wants to convince Bob that she was told the secret by Carol, but she doesn't want to offend Carol by letting the secret out before Carol decides to reveal it.

Develop a protocol, using only random numbers and hash functions, that has the following properties:

1. The protocol consists of two parts: messages exchanged between Alice and Bob before Carol reveals her secret, and messages exchanged between Alice and Bob after Carol reveals her secret.
2. Bob cannot determine the secret from the messages sent before Carol reveals the secret.
3. The messages exchanged after Carol reveals the secret convince Bob that Alice already knew the secret before Carol revealed it.

Use the notation  $S$  for the secret,  $N_a, N_b, \dots$  for the random numbers (nonces), and  $h$  for the one-way collision-free hash function.

Explain why your solution works. Note that it is not enough for Alice to tell Bob the result after it is announced, for Bob can claim that Alice cheated by waiting for the result to come out.

**Question 3 [8 marks]**

A university wants to make information about grades and enrolments available to students and lecturers from their home machines and laptops. The ability to update the information is not a requirement, as this is handled using machines on the university's secure network.

Consideration is being given to the use of a public key infrastructure (PKI) in order to meet the requirements of this application. Your task is to design the way the PKI should be deployed. For each of the following issues, describe what design decision you would make and why:

1. Discuss the security policy for this application.
2. Describe the overall architecture of your solution. What role(s) do public keys play in your solution?
3. What information should be contained in the certificates?
4. Where should the keys be generated?
5. How are certificates distributed?
6. Should there be a single certificate authority, a hierarchical structure, or a "web of trust" similar to the PGP model?
7. Should delegation be possible, and if so, for what purposes? If so, are there any constraints on the delegated rights?
8. How would you manage certificate revocation?

(Limit your answer to at most 1,600 words.)

**Question 4 [6 marks]**

The following is a key distribution and authentication protocol that uses shared key cryptography and a trusted server.  $A$ ,  $B$ , and  $S$  are the principals ( $S$  is the server),  $N_a$  and  $N_b$  are nonces, and  $K_{ab}$ ,  $K_{bs}$ , and  $K_{as}$  are shared keys between  $A$  and  $B$ ,  $B$  and  $S$ , and  $A$  and  $S$ , respectively.

1.  $A \rightarrow S : A, B, N_a$
2.  $S \rightarrow B : \{A, B, N_a, K_{ab}\}_{K_{as}}, \{A, B, N_a, K_{ab}\}_{K_{bs}}$
3.  $B \rightarrow A : \{A, B, N_a, K_{ab}\}_{K_{as}}, \{N_a\}_{K_{ab}}, N_b$
4.  $A \rightarrow B : \{N_b\}_{K_{ab}}$

Answer the following questions relating to this protocol:

1. Explain what each step of the protocol does and the intention of each of the message components.
2. Show that the protocol has a weakness similar to that discussed in class for the Needham-Schroeder shared-key protocol. Hint: Consider a situation where an old session key  $K_{ab}$  has been compromised.
3. Propose a way to modify the protocol so as to fix the problem you identify.