COMPSCI 314

THE UNIVERSITY OF AUCKLAND

FIRST SEMESTER, 2010
Campus: City

COMPUTER SCIENCE
Modern Data Communications
(Time allowed: TWO hours)

NOTE: Examination conditions: Closed book, no calculators permitted.

Attempt **ALL** questions. Total possible: **100 marks.**

This is an **ungraded sample** exam, which should take you about 15 minutes to complete.

Instead of using a script book, you should write your answers on a blank sheet of paper. Do **not** write your name on your answer sheet.

There will be a brief (approximately 5 or 10 minute) reading period at the beginning of the examination, during which you are **not** allowed to pick up a pen or pencil.

A. The following questions refer to the series of four messages (M1-M4) described below.

M1. Alice → Bob: E_b("I'm Alice", a , t_a)

M2. Bob → Alice: E_a("Hi Alice, how can I help you?", t_a , t_b)

M3. Alice → Bob: E_b("Hi Bob, Please open a free email account for me.", a , t_a)

M4. Bob → Alice: E_a("No worries. Your username is a. Your password is x7ty23#", t_a , t_b)

1. If Eve is able to intercept messages, will she learn Alice's username (a) and initial password (x7ty23#) on Bob's email server? Explain briefly.   **(3 marks)**

2. If Eve is able to fabricate messages, will she be able to open an account on Bob's email server with username a which Alice doesn't know about? Explain briefly.   **(4 marks)**

B. Consider the following code:

e	0
t	1
i	00
a	01
n	10
m	11

4. Give three different possible decodings of 001.   **(3 marks)**

5. If this code is extended by adding a parity bit to the end of each codeword, would the resulting code be prefix-free? Explain briefly.   **(4 marks)**

C.   (Other questions). **[84 marks]**

_____