Name:

ID:

THE UNIVERSITY OF AUCKLAND

FIRST SEMESTER, 2010
Campus: City

COMPUTER SCIENCE
Modern Data Communications
(Time allowed: 45 minutes)

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

Attempt **ALL** questions. Total possible: **50 marks.**

Please write your **name and UPI** on all pages of this answer book.

In the questions on security protocols,

- *a* and *b* are public keys for Alice and Bob,
- *a'* and *b'* are the corresponding private keys,
- t_a and t_b are timestamps,
- *E* is a public-key encryption function, and *D* is the corresponding decryption function.

Name:

ID:

A. The following questions refer to the series of three messages (M1-M3) described below.

M1. Alice → Bob: E_b("Hi Bob, I have a new public key. Please use my new key *c*.", a , t_a)

M2. Bob → Alice: E_c("Hi Alice, no worries, I have updated my records.", t_a , t_b)

M3. Alice → Bob: E_b("Thanks!", a, t_a , t_b)

1. If Eve is able to intercept messages, will she know the values of a, b, c, t_a , and t_b? Explain briefly. **(5 marks)**

2. If Eve is able to fabricate messages, will she be able to impersonate Alice? Explain briefly. **(5 marks)**

B. The following questions refer to a Hamming code with the following properties.

- Each codeword is 7 bits long, with four data bits (d1, d2, d3, d4) and three check bits (r1, r2, r4).
- Check bit r1 is even parity on d1 and d3.
- Check bit r2 is even parity on d2 and d3.
- Check bit r4 is even parity on d4.

3. If we are transmitting d1 = 1, d2 = 1, d3 = 1, d4 =1, what are the values of r1, r2, and r3? Show your work. **(5 marks)**

Name:

ID:

4. If we receive d1 = 0, d2 = 0, d3 = 0, d4 = 0, r1 = 0, r2 = 0, r3 = 1, what is the corrected data? Show your work. **(5 marks)**

5. Is there any chance of an undetected error in a codeword? Explain briefly.

(5 marks)

C. Consider the following code:

0	0000
1	0001
2	0010
3	0011

4	0100
5	0101
6	0110
7	0111

8	1000
9	1001
A	1010
B	1011

C	1100
D	1101
E	1110
F	1111

6. Is this code prefix-free? Explain briefly. **(5 marks)**

7. We can use this code to transmit a sequence of positive integers, in the following way. Each integer is represented as a series of symbols in the range 0-E. The symbol F indicates the end of the string that represents an integer. The value of each integer is the sum of the (hexadecimal) values of the symbols (in the range 0-9 and A-E) in the string for that integer. For example, the sequence (14, 9, 0, 15) can be represented as the 8-symbol string "EF9FFE1F", which is encoded as 1110 1111 1001 1111 1111 1110 0001 1111. Use this method to encode the sequence (14, 30). Show your work. **(5 marks)**

Name:

ID:

D. The following questions refer to a channel that can carry analog signals from 20 Hz to 10020 Hz with a SNR of 30 dB.

8. If we used amplitude shift keying (ASK) on this channel, with one bit per symbol at a frequency of 1 kHZ, what is its bit rate? Explain briefly. **(5 marks)**

9. Can we use amplitude shift keying with 1 bit per symbol, at a frequency of 10 kHz, on this channel? Hint: use the Nyquist theorem. To receive full credit, you must use the word "Baud" correctly in your answer. **(5 marks)**

10. What is the Shannon capacity (maximum bitrate) of this channel? Show your work. **(5 marks)**