TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI

VICTORIA
UNIVERSITY OF WELLINGTON

EXAMINATIONS — 2009
END-YEAR

COMP306

Computer Networks

Time allowed: THREE HOURS

Instructions: The examination contains 6 questions.

There are NO optional questions.

The exam consists of 180 marks in total.

Paper foreign to English language dictionaries are allowed.

Electronic dictionaries and programmable calculators are not allowed.

Question 1 Cryptography and Cryptanalysis **[30 marks]**

(a) [2 Marks] Both Steganography and Cryptography seek to prevent the content of a message from being revealed. However they both achieve this in very different ways. Explain the significant difference between Steganography and Cryptography, examples should be given to reinforce your explanation.

(b) [2 Marks] What is Kerckhoffs principle?

(c) [4 Marks] Show, with the use of an example, how a polyaphabetic cypher might encode the word "Adam". You may choose your own scheme and key – so you must explain your scheme, show all steps and information used in the process.

(d) [6 Marks] Is a polyalphabetic cypher susceptible to a frequency analysis attack? Be sure to state any conditions or assumptions your argument is relying on. Use an example to support your claims.

(e) Consider the efforts at Bletchley Park to crack the WWII German enigma code.

 i. [4 Marks] What type of Cypher was the Enigma Code?
 ii. [8 Marks] State and explain (with examples were needed) the four techniques used by the Cryptanalysts at Bletchley Park to crack the Enigma code.

(f) [4 Marks] Define what it means for a Cryptographic system to be secure.

Question 2 Cryptography and Authentication **[30 marks]**

(a) [4 Marks] What is Cypher block chaining, and why was it needed in the DES encryption standard?

(b) [8 Marks] The major problem in the 1970s was the exchange of keys. Outline the DHM (Diffie, Hellman and Merkle) algorithm for establishing a key, without a prior physical key exchange. Be sure to explain the importance of one-way functions in this protocol. You may explain the algorithm directly or by using an analogy.

(c) [8 Marks] Shamir's algorithm enables us to share a secret, specifically allowing any n of m members of a group to be able to decode the message. Explain, preferably using a diagram, how key fragments are created, and how we can reconstruct the key from any n of the m fragments.

(d) [5 Marks] Show, with the aid of a diagram, how RSA public-private keys can be used to authenticate two parties that can safely obtain, or already have, the other's public key.

(e) [5 Marks] Show how, with the aid of a diagram:

  i. a digital signature and a digest are used to 'sign' a documents, and

  ii. how the receiver can verify the digital signature.

Question 3 Application Layer **[30 marks]**

(a) [2 Marks] Define the term 'protocol' as used in computer networking.

(b) [3 Marks] Explain, with examples, why the transport layer is considered an Hourglass protocol.

(c) [3 Marks] Give three good reasons why layering is a good idea for networking.

(d) [4 Marks] Explain the difference between sockets and ports.

(e) [2 Marks] What is SOAP?

(f) [4 Marks] What is an RPC/RMI? Include a brief discussion of how an RPC/RMI is carried out.

(g) [4 Marks] Define the difference between a Web-based Service and a Web service.

(h) DNS

  i. [3 Marks] Explain zone delegation in the DNS.
  ii. [5 Marks] Show, with the aid of diagrams how an iterative DNS query is performed.

Question 4 Transport Layer **[30 marks]**

(a) [2 Marks] What does it mean for a protocol to be 'connection-less'?

(b) [4 Marks] Discuss why some applications may prefer connection-less protocols to connection oriented protocols. Use examples to reinforce your explanation.

(c) [8 Marks] Explain how TCP deals with duplicate connections requests.

(d) [8 Marks] Explain TCP's mechanism for flow control. Use diagrams to show how the receive window operates and be sure to detail how the receive window information is communicated back to the sender.

(e) [8 Marks] Explain TCP's mechanism for congestion control. Be sure to include a brief discussion on slow start, fast retransmit and fairness.

Question 4 Network Layer and IP Addressing **[35 marks]**

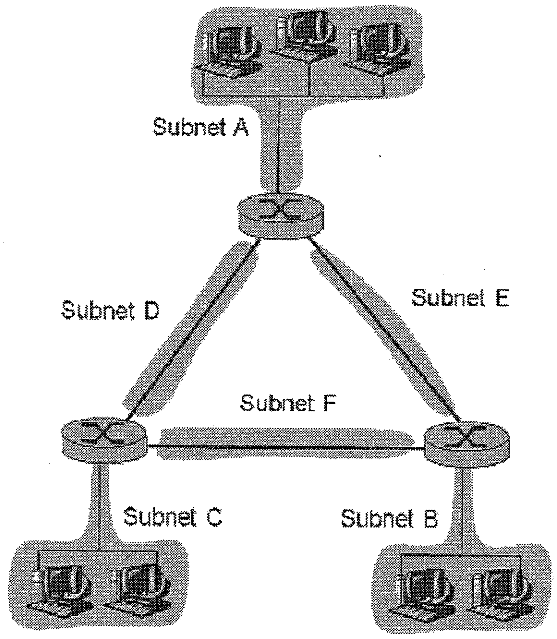
(a) [10 marks] Consider a datagram network using 8-bit host addresses. Suppose a router uses longest prefix matching and has the following forwarding table:

Prefix Match	Interface
00	0
010	1
011	2
10	2
11	3

For each of the four interfaces, give the associated range of destination host addresses and the number of addresses in the range (write your answer using the table format specified below).

Destination Address Range	Interface	No. of Addresses

(b) [14 marks] Consider the following topology, which has six subnets (A, B, C, D, E and F).



Suppose all addresses for the host and router interfaces MUST be allocated from 214.97.254/23. Assign network addresses to each of the six subnets with the following requirements:

1. Subnet A should have enough addresses to support 250 interfaces.
2. Subnet B should have enough addresses to support EXACTLY 120 interfaces.
3. Subnet C should have enough addresses to support 120 interfaces.
4. Subnets D, E and F should each be able to support two interfaces.

For each subnet, the assignment should take the form a.b.c.d/x or a.b.c.d/x – e.f.g.h/y (write your answer using the table format specified below).

Subnet	**Address**

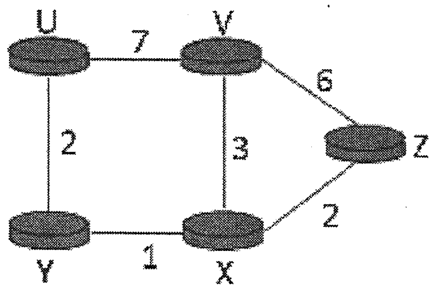
(c) [3 marks] What is the deference between CIDR (Classless Interdomain Routing) and Classful Addressing?

(d) [3 marks] What does DHCP do?

(e) [5 marks] What is NAT traversal problem and how do we address this problem using UPnP (Universal Plug and Play)?

Question 6 Routing and Mobile Networks **[25 marks]**

(a) [17 marks] Consider the network shown below.



Assume that each node initially knows the link costs to each of its neighbours. Compute **the distance table at Node Z** after the initialisation step and after each iteration of a synchronous version of the distance-vector algorithm - nodes exchange cost information in a synchronous manner (write your answer using the table format specified below).

		Cost to				
		U	V	X	Y	Z
From	V					
	X					
	Z					

(b) [3 marks] In Mobile IP, what is the difference between a permanent address and a care-of address? Who assigns a care-of address?

(c) [5 marks] What are the purposes of the HLR and VLR in GSM networks? What elements in Mobile IP are similar to the HLR and VLR?

* * * * * * * * * * * * * * * * * * *