Name: _____

Student Number: _____

COMP SCI 3C03/SFWR ENG 4C03 (Networks & Security) Michael Soltys

DAY CLASS
DURATION OF EXAMINATION: 2 Hours
MCMASTER UNIVERSITY FINAL EXAMINATION April 2012

THIS EXAMINATION PAPER CONSISTS OF 2 PAGES AND 6 QUESTIONS.

YOU ARE RESPONSIBLE FOR ENSURING THAT YOUR COPY OF THE PAPER IS COMPLETE.
BRING ANY DISCREPANCY TO THE ATTENTION OF YOUR INVIGILATOR.

No aids allowed.

All questions worth 10 marks, for a total of 60.

Q1. **IPv4** addressing is the current IP addressing scheme, while **IPv6** is the IP addressing scheme of the future.

1. **IPv4** is 32-bits, while **IPv6** is 128-bits. The former is often described with decimal digits, and the latter with hexadecimal digits: give the details of both notations.
2. What is the main reason for replacing **IPv4** with **IPv6**; mention the concept of the "Internet of things."
3. In **IPv4** *classful addressing scheme* there are three kinds of addresses; the A,B,C classes (as well as D,E which you may ignore for this question). Explain what they are in terms of *netid* and *hostid*. Explain it also with the "/" (i.e., the 'slash') notation.
4. Suppose that your home LAN's addressing space is given by `192.168.0.0/24`, i.e., a reserved for "private use" address. Explain how your hosts can communicate with the rest of the Internet (mention NAT in your answer).

Q2. Explain the Address Resolution Protocol (ARP); in your answer mention the terms *broadcast* and *MAC addressing*. ARP is consigned to which conceptual layer?

Q3. The TCP sliding window mechanism operates at the octet level; it solves two important problems: efficient transmission and flow control.

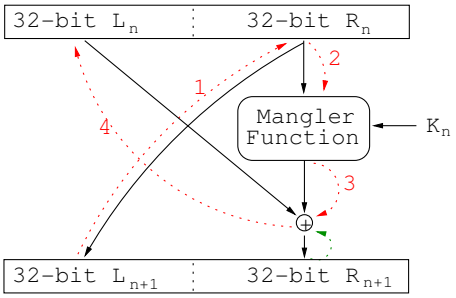
Consider the following window, where 1 through 11 are octets:

1 2 | 3 4 5 6 | 7 8 9 10 11 ...

Let "ack" abbreviate "acknowledged."

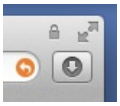
1. Explain what is the status (sent/ack) of the octets in this example.
2. How does the sliding window improve the efficiency of transmission?
3. How does it improve flow control?

Q4. When we were discussing DES in class, we spent some time explaining how DES is reversible—i.e., how we can decrypt with the same key. We pointed out that regardless of how complicated the "Mangler function" is, we can still invert each round. Recall that this is what we called a "Feistel cipher." Explain how this inversion works; a diagram is included for your convenience.



Q5. Explain how to mount a "man-in-the-middle attack" against Diffie-Hellman; explain how to avoid such an attack with an "authentication scheme" in place.

Q6. In Mac OS X, when connecting with `HTTPS` to a secure website, there is an icon of a lock in the upper-right corner of the browser.



When pressed, it displays the *certificate* of the web site, as well as a *chain* to a *trust anchor*. Explain these terms, as well as outline this authentication scheme; make sure that you mention *Certification Authority* and *Public Key Infrastructure* in your answer.

END OF EXAM