University of Toronto at Scarborough
Department of Computer & Mathematical Sciences

Term Test

MAT C16H

Examiner: P. Selick

Date: October 29, 2007
Duration: 110 minutes

FAMILY NAME: ____________________

GIVEN NAMES: ____________________

DO NOT OPEN THIS BOOKLET UNTIL INSTRUCTED TO DO SO.

Instructions:

- There are 8 numbered pages in this exam. It is your responsibility to ensure that, at the start of the exam, this booklet has all its pages.
- Answer all questions. Unless noted otherwise, explanation and justification of your answers is expected.
- Calculators are permitted.

STUDENT NUMBER: ______________________________

FOR MARKERS ONLY	
Question	Marks
1	/6
2	/12
3	/9
4	/12
5	/15
6	/12
7	/12
8	/12
9	/10
TOTAL	**/100**

1. [**6 points**] How many possible keys are there for the affine cipher?

2. [**12 points**]

   (a) What are "confusion" and "diffusion".

   (b) Which of the following encryption schemes possess confusion and diffusion? [Only a brief explanation of your choices is expected.]

      i. substitution cipher

      ii. Hill cipher

      iii. Enigma machine

      iv. DES

3. [**9 points**]

   (a) Is the composition of two affine ciphers another affine cipher?

   (b) Is the composition of two Vigenère ciphers with the same key length another Vigenère cipher?

   (c) Is the composition of two Vigenère ciphers with different key lengths another Vigenère cipher?

4. [**12 points**] Naive Nelson uses RSA to receive a single ciphertext c, corresponding to the message m. His public modulus is n and his public encryption exponent is e. Since he feels guilty that his system was used only once, he agrees to decrypt any ciphertext that someone sends him, as long as it is not c, and return the answer to that person. Evil Eve sends him the ciphertext $2^e c \pmod n$. Show how this allows Eve to find m.

5. **[15 points]** Let u and m be positive integers.

   (a) What condition on u and m determines whether or not there exists an integer v having the property that $uv \equiv 1(\text{mod } m)$?

   (b) Is there an efficient algorithm for determining whether or not the condition in part (a) is satisfied? Why or why not?

   (c) Assuming that there is an integer v such that $uv \cong 1(\text{mod } m)$ describe an efficient method for finding v?

Note: An "efficient" algorithm is one in which the number of steps required grows no faster than a polynomial in the number of digits in the inputs. If you wish to make use of algorithms which were shown in class to be efficient, you may do so without going into the details (beyond the name/statement) of those algorithms.

6. **[12 points]** Find an integer x such that $x \equiv 5 (\text{mod } 9)$, $x \equiv 6 (\text{mod } 25)$, and $x \equiv 1 (\text{mod } 7)$. (Simplification is not required. e.g. leave the answer as a sum or product if you wish.)

   Show your steps: little credit will be given for guessing an answer.

7. **[12 points]** Let K be the finite field given by $K = \mathbb{F}_2[\omega]/(w^4 + w + 1)$ where $\mathbb{F}_2 = \{0, 1\}$ is the field with two elements.

   (a) How many elements are there in K?

   (b) In K, evaluate $(\omega^3 + 1)(\omega^2 + 1)$?

   (c) In K, find ω^{-1}?

8. **[12 points]** Assuming that each A and B have public key encryptions, and that they are obligated to keep their decryption keys secret, describe a protocol by which A and B can exchange messages so as to achieve CONFIDENTIALITY, DATA INTEGRITY, AUTHENTICATION, and NON-REPUDIATION. (Include an explanation why your method achieves the desired goals.) What precaution should they take to ensure that Eve, who has been observing the encrypted messages, does not store old messages and then resend them to attempt to confuse their communications?

9. [**10 points**]

   (a) Define the Euler ϕ-function $\phi(n)$.

   (b) What is $\phi(720)$?

(This page is intentionally left blank.)