

Name: \_\_\_\_\_

Student Number: \_\_\_\_\_

COMP SCI 2ME3 (Software Design I)

Michael Soltys

DAY CLASS

DURATION OF EXAMINATION: 2 Hours

MCMASTER UNIVERSITY FINAL EXAMINATION

April 2009

THIS EXAMINATION PAPER CONSISTS OF 2 PAGES AND 4 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 25 marks, for a total of 100.

1. Show that MTF, *Move To Front*, is a 2-competitive algorithm, and also that its competitive ratio is  $\leq 2 - \frac{1}{l}$ , where  $l$  is the length of the list. Do this question by following the outline below:

- (a) Let OPT be the optimal offline algorithm for the static list accessing problem. Let  $\sigma$  be any sequence of requests; show that

$$\text{MTF}(\sigma) \leq 2 \cdot \text{OPT}_C(\sigma) + \text{OPT}_P(\sigma) - \text{OPT}_F(\sigma) - n.$$

- (b) Show that  $\text{OPT}(\sigma) \leq n \cdot l$ .
- (c) Show that  $\mathcal{R}(\text{MTF}) \leq 2 - \frac{1}{l}$ .

2. Show that any page replacement algorithm can be modified to be demand paging without increasing the overall cost on any request sequence.

3. We say that we can *break* ElGamal, if we have an efficient way for computing  $m$  from  $\langle p, g, A, c_1, c_2 \rangle$ .
  - (a) Explain how ElGamal works; in particular, what are  $\langle p, g, A, c_1, c_2 \rangle$ .
  - (b) Explain what is the Diffie-Hellman Problem (DHP).
  - (c) Show that we can break ElGamal iff we can solve the DHP efficiently.
  
4. Explain the RSA Cryptosystem; show that if the two primes  $p, q$  are chosen close together, then one can break RSA.