CS3235 Tutorial for week 3 (Aug 27-31, 2007)

August 23, 2007

Your tutorial sessions are to be graded, and are worth 5% of your final assessment, so it is in your interest to *prepare* for them. In addition to the written answer to question 1 that you will submit to the tutor, during the tutorial sessions, your tutors will ask randomly selected students to answer each of the other questions. The tutors will use your responses to grade your tutorial participation.

Present your answer (on paper) to the following tutorial question at the *beginning* of the tutorial session. The tutors will assess your presentation for this question *after* the tutorial, according to the scale: A: *Brilliant*, B: *Correct but ordinary*, C: *Tried*, F: *Nothing worthwhile submitted*. Ensure that your submission is clearly marked with your name (as in the register), your matriculation number, and your tutorial class. You must hand in your submission at the beginning of the tutorial. Late submissions will not be accepted.

---

1 (To be handed in). In the Enigma movie clip we watched, the actors used an Enigma machine with three rotors. Each rotor had a fixed internal wiring which translates one of 26 letters to another different letter. The rotors are connected, so if rotor 1 translates an A to a P, and rotor 2 translates a P to a G, then the combined effect of the two rotors is to translate an A to a G.
In addition, the rotors rotate (step/cycle) in relation to each other, as each new letter is encoded, and so after translating an A to a G, the next time you press A it might be translated to a Z (or something else).

(a) Assuming that the rotors cycle through all possible combinations[1], how many characters must be encoded before the rotors are back where they started?

(b) Approximately how long before an A is translated to a G again?

After you have presented the tutor your written submission, some of you may be asked at random to answer questions on the whiteboard. If you give a reasonable answer then you get grades for these as well. During the semester, you can expect to be asked to present answers to questions at any time (the *lucky* students will be picked at random). Please come to the tutorial ready to present any one of your answers to the class.

---

2 (Do not hand in). The program **`nmap`**, is a port scanner (as briefly discussed in class), the same program that Trinity used in the Matrix movie clip we saw. Give a good/honest reason for regularly using **`nmap`**? (i.e. some reason that you would not be ashamed to tell your Mom and Dad about).

3 (Do not hand in). Differentiate between Cæsar, rotation and Vigenère ciphers.

4 (Do not hand in). Classify each of the following sentences as a violation of confidentiality, of integrity, of availability, or of some combination thereof. Justify your answer.

(a) Robert copies Maya's tutorial answer.

(b) Peter crashes Tan's computer.

(c) Dhaval registers the domain name "www.amazon.com" and refuses to let Amazon use the domain name.

[1] In actual fact, they do not.