CS3235 Tutorial for week 3 (Aug 28-Sep 1, 2006)

August 25, 2006

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 number. You must hand in your submission for question 1 at the beginning of the tutorial. Late submissions will not be accepted.

1. Assume that (after work hours) you wish to send information from your home to a client (also at home), using symmetrically encrypted messages over the Internet. You have exchanged a secret (one-time-pad) key $k_1$ with your client, and you take your (100 character) message $m$, and XOR it with the first 800 bits of your key, and send this encrypted message $k_1(m)$ to the client. The client XORs the encrypted message with her copy of the key $k_1$, and so retrieves the original message. Assuming that no-one except you and the client knows your key $k_1$ then this is a fairly safe activity.

However, your boss at work thinks it is not safe enough, and demands that you first send your encrypted message $k_1(m)$ to him, and then he re-encrypts the encrypted message using his own key $k_2$ giving $k_2(k_1(m))$, which he uses to send messages to his counterpart in the client’s company. His counterpart then decrypts this message using the key $k_2$ (which he shares with your boss), leaving $k_1(m)$ which he then sends on to your client. All the communications take place over the Internet.

(a) Is this system any safer than before? (In terms of a bad person reading the message $m$.) If so - why? If not - why not?

(b) Your boss has possibly added a new and different form of insecurity to his life. Explain what a bad person may be able to do to your boss (and how).

Your answer to question 1 is likely to include information about the properties of the XOR function.
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. 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) How long before an A is translated to a G again?

3. Given an ASCII string “MATRIX”, and a key represented by the ASCII string “ELVIS!”, calculate or show the resultant encrypted string, using the XOR bit-string technique shown in class.

4. Describe an operation \(\ast\) which forms a group with the Integers from 2 to 6. Define the operation, and give the identity, and the inverse mappings.

5. Show the tables for addition and multiplication for the positive integers mod 5 (\(\mathbb{Z}_5\)) similar to the table on page 23 of the book.

\(^1\)In actual fact, they do not.