
August 20, 2004

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. Your tutors are Pradeep Kumar Atrey and Hemal Namdev Rathod. During the tutorial sessions, your tutors will ask a randomly selected student to answer each question, so with 4 to 6 questions per tutorial, there is a fair chance that you will be asked to answer a question next week. The tutors will use your responses to grade your tutorial participation. If you are unable to answer a question, you can PASS, which is a no-fault way of avoiding answering. However, if you PASS, then you must answer a question the following week.

1. In class, we looked at a three-way system for transferring a message from A to B, which had the interesting property that neither A nor B had to reveal their keys. Given a message m, the first message (from A to B) would be $K_A(m)$, the second message (from B to A) would be $K_B(K_A(m))$, and the third message (from A to B) would be $K_A^{-1}(K_B(K_A(m))) = K_B(m)$. B could then calculate $K_B^{-1}(K_B(m)) = m$, and retrieve the message. If both A to B used a random byte sequence for their key, and then used the XOR function to both encrypt and decrypt the message, then surely this is a perfect technique for transferring data... right? (Its a one-time pad, and neither participant has to reveal a key, and a third party cannot decrypt/unlock the message). Well... actually... it is not a good scheme. Explain exactly why it is not a good scheme, using your knowledge of the properties of the XOR function.

2. Some of the wily hackers in our class used the program nmap, which is a port scanner (as briefly discussed in class), to examine the computer opo.comp.nus.edu.sg remotely, to try to discover what the machine was. This is the same program that Trinity used in the Matrix movie clip we saw. Is there any good/honest reason for regularly using nmap? (i.e. some reason that you would not be ashamed to tell your Mom and Dad about)... Well... actually... the answer to the previous question is YES, but I want you to tell me what that reason is and who would use it.

3. Given an ASCII string “Matrix”, and a key represented by the ASCII string “9MQ4Z+”, calculate or show the resultant encrypted string, using the XOR bit-string technique shown in class.

4. Fields and Groups:
   (a) Why are the Integers using addition and multiplication not a field?
   (b) Why are the Natural numbers using addition not a group?
   (c) Show the tables for addition and multiplication for the positive integers mod 5 ($\mathbb{Z}_5$) similar to the table on page 20 of the book. By the way - that table has an error...

5. Fields:
   (a) Show, without using the table, that in GF($2^3$):

   \[
   \begin{align*}
   6 + 4 &= 2 \\
   5 \times 3 &= 4
   \end{align*}
   \]

   (b) Using table 2.4, show that GF($2^3$) is a field.

---

1 pradeepk@comp.nus.edu.sg
2 hemalnam@comp.nus.edu.sg.