Institut for Matematik og Datalogi
Syddansk Universitet

December 5, 2011
JFB

Introduction to Computer Science
E11 – Lecture 17

Lecture, November 24, 12:15–14, U26

We covered sections 6.6 and 6.7 of chapter 6.

Lecture, November 29, 8:15–10, U26

Daniel Merkle will talk about CS + life sciences and sorting pancakes.

Lecture, December 6, 8:15–10, U26

We will cover the first five sections of chapter 7 in the textbook.

Discussion section (and study groups): December 7

In your study groups, if you didn't have time for the Maple exercises in the last lab, try the Maple exercises near the end of the Exercise 1 described here: http://www.imada.sdu.dk/ joan/projects/exercises.pdf Discuss what you learned from them.

1. This English message was encrypted using a Caesar cipher. Decrypt it.

   YMNX HWDUYTLWFR NX JFXD YT IJHNUMJW.

   Discuss which techniques you used.

2. Each person in the group should choose a secret key for performing encryption with the Caesar cipher (the alphabet is shifted by the amount specified by the key) and choose a secret message (not more than 15 letters). Encrypt your message with the secret key. Give everyone in your group a copy of the encrypted message and let them try to break it. Let them know if the message (and alphabet) is English or Danish.

3. This was entitled "Cold Country". It was encrypted using a monoalphabetic substiution cipher. A monoalphabetic substitution cipher works similarly to a Caesar cipher. However, instead of just shifting the alphabet a fixed amount to get the mapping defined for each letter, the alphabet is permuted randomly (reordered). The key says which letter maps to which. If the alphabet has 29 letters, the number of keys is now 29!.

   TOWWJPHJC ZY RXW PHOTWYR ZYPHJC ZJ RXW SFOPC.
   UFYR FB ZR ZY QFIWOWC SZRX ZQW RXFMYHJCY FB
   BWWR CWWD.

   Discuss which techniques you used.

4. Each person in the group should choose a secret key for performing encryption with a monoalphabetic substitution cipher and choose a secret message (with between 60 and 80 letters). Encrypt your message with the secret key. Give everyone in your group a copy of the encrypted message and let them try to break it. Let them know if the message (and alphabet) is English or Danish.

5. Do problem 48 on page 557. Try decrypting. What is the problem here if 110 is interpreted in decimal instead of binary?

6. Do problem 50 on page 557. (Try encrypting and decrypting some message.)

7. Discuss problems 2, 6, and 7 on pages 557–558.

8. Discuss the results of your Maple exercises concerning finding large primes.

Assignment due 12:15, December 16

Late assignments will not be accepted. Working together is not allowed. (You may write this either in English or Danish.) Turn in a copy of your Maple worksheet (don't change it to a PDF file this one time) via Blackboard and turn in an identical paper copy. Create a Maple worksheet with the following:

1. Include text saying your name, section number and the course number, DM526, at the top.

2. Try differentiating and integrating polynomials of at least 3 different (maximum) degrees.

3. Plot two of the functions.

4. Consider an RSA system with Alice's public key $N = 16,016,003$ and $e = 97$.

   (a) Find Alice's secret key d. Use the `igcdex` command first to find d. Check the result. Then write a `while` loop to find d (you can either do the brute force, inefficient way, or you can write a procedure for the Extended Euclidean Algorithm (which includes a while loop).

   (b) Try encrypting at least three numbers which are relative prime to N and one which is not. Then try decrypting them. In each case, try taking the gcd of your encrypted value with N. (Try to explain why you get these results when you take the gcd.)

   (c) With one of the encryptions, show all the steps from the algorithm for fast modular exponentiation (do not raise to any power greater than 2 in this process).

   Use text comments to explain what you are doing.