Institut for Matematik og Datalogi
Syddansk Universitet

November 21, 2008
JFB

Introduction to Computer Science E08 – Week 11

Announcement

Imada holder pizzamøde for alle studerende mandag 1/12 kl. 16.15 i U49. Mødet vil indeholde generel information om kandidat- og bachelorstudiet, samt orientering om planlagte valgfri kurser i næste semester. Til slut vil der være gratis pizza, øl og sodavand til de fremmødte.

There will be a ”pizza-meeting” for all students of Imada on Monday, December 1 at 16.15 in room U49. At the meeting Imada will give general information on the bachelor and candidate studies, and specific information on the elective courses planned for the next semester. The meeting will end with a free pizza, beer, and soft drink session.

Lecture, November 17

Daniel Merkle lectured on bioinformatics.

Lecture, November 19

We finished with cryptography (from section 12.6 in the textbook and the notes and links mentioned above). covering RSA.

Lecture, November 24

We will cover chapter 7 in the textbook.

Lecture, November 26

We will cover on-line algorithms.

Lecture, December 1

We will begin on chapter 11 in the textbook.

Discussion section: first in week 49

Discuss the following problems (some are from the textbook) in groups of 3 to 4. (Think about these problems before coming to discussion section. Prepare your secret encryptions in advance.)

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. In such a cipher, the key is permutation of the alphabet, so that you decide according to this key what letter "A" maps to, what letter "B" maps to, etc.

   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 611. Try decrypting. What is the problem here?

6. Do problem 49 on page 611. (Note that 111 is an encryption of a message.)

Discussion section: second in week 49

Discuss the following problems from the textbook in groups of 3 to 4. (Think about these problems before coming to discussion section.)

1. Questions 1 and 2 on page 347.

2. Questions 1 and 2 on page 354.

3. Question 3 on page 362.

4. Questions 1, 2, 3, 4, and 6 on page 371.

5. Questions 4, 5 and 6 on page 375.

6. Questions 1 and 3 on page 376

7. Issues 1, 3, 5, and 6 on pages 386–387.

Assignment due 12:15, December 8

Late assignments will not be accepted. Working together is not allowed. (You may write this either in English or Danish, but write clearly if you do it by hand.) Show your work.

1. Suppose that the public exponent for user A using RSA is 103 and that the modulus is 143. What is the private exponent?

2. Use the algorithm given in class and on the weekly notes for exponentiation to encrypt 5 using the above system, where the public exponent is 103 and modulus is 143. Show the intermediate values computed.

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

   IXEVZUMXGVNE OY LAT.

   Explain which techniques you used.