Institut for Matematik og Datalogi
Syddansk Universitet

February 28, 2014
JFB

Introduction to Computer Science
F14 – Discussion sections – Week 11

1. Consider an RSA system with Alice's public key $N = 1517$ and $e = 227$. Note that $1517 = 37 \cdot 41$.

   (a) Find Alice's secret key d. Use the Extended Euclidean Algorithm from the slides used in lectures on February 12 and February 19.

   (b) Try encrypting 423. Use the algorithm for fast modular exponentiation (also from those slides).

   (c) Decrypt the number, using fast modular exponentiation. Is the result correct?

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

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

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

   YMNX HWDUYTLWFR NX JFXD YT IJHNUMJW.

   Discuss which techniques you used.

5. Work in groups for this one. 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.

6. 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! Why?

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

   Discuss which techniques you used.

7. Work in groups for this one. 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.

8. Find four different square roots of 1 modulo 143 (numbers which multiplied by themselves modulo 143 give 1). Note that all of these numbers should be at least 0 and less than 143.

9. Add two of these different square roots which are not negatives of each other modulo 143 (two where adding them together does not give 143). Find the greatest common divisor of this result and 143. Subtract these same two different square roots and find the greatest common divisor of this result and 143. (Think about why you get these results.)