Institut for Matematik og Datalogi
Syddansk Universitet

November 9, 2015
JFB

Introduction to Computer Science
E15 – Discussion Sections – Week 47

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

   YMNX HWDUYTLWFR NX JFXD YT IJHNUMJW.

   Discuss which techniques you used.

2. 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 key is a permutation of the alphabet, so that you decide according to this key what letter "A" maps to, what letter "B" maps to, etc. If the alphabet has 29 letters, the number of keys is now 29! Why? The original message here was in English, so there are only 26 letters. How many possible keys are there?

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

   Discuss which techniques you used.

3. 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.

4. 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.

5. 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.)