Institut for Matematik og Datalogi
Syddansk Universitet

November 18, 2014
JFB

Introduction to Computer Science
E14 – Study Group – Week 48

1. Discuss the results of your Maple exercises concerning finding large primes and factoring. Were there any surprises? What did the & do in the exponentiation modulo 1083?

2. Discuss your experiences with gpg. Did it take long to generate keys? How would you use fingerprints? What did `gpg -sea filename` do? Why might you want to encrypt a file that you were not sending to anyone? How convenient was gpg to use? Will you use it again?

3. 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.

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.