Institut for Matematik og Datalogi
Syddansk Universitet

November 25, 2015
JFB

Introduction to Computer Science
E15 – Study Group – Week 50

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. Note that simple hash functions, such as "modulo m" where m is not prime can cause some uneven distribution into bins, for example if many of the actual values being hashed have a factor in common with that m. For cryptographic purposes, even more is required of a hash function. For example, when a message is signed, the message is hashed, using a (hopefully) cryptographically secure hash function to a length that the digital signature system can handle. In order to prevent forgery, it must be infeasible for a forger to find a second message which hashes to the same value as a message already signed. Otherwise, the same digital signature will work on both messages.

   - Read about definitions of cryptographically secure hash functions on the Web. Find out what properties are generally required. There are three listed in Wikipedia, under "cryptographic hash function".
   - Figure out for which applications which property is sufficient.
   - Which is strongest (meaning requiring most of the hash function)?
   - What is the birthday attack?
   - Read about some modern cryptographic hash functions, such as SHA-1 and SHA-3.

4. Read the article http://www.wired.com/2015/07/google-says-ai-catches-99-9-percent-gmail-spam/ about how Google uses neural networks in its spam filter for gmail.

5. Discuss issues 1, 2, 3, and 14 on pages 536–538 of the textbook.