Institut for Matematik og Datalogi
Syddansk Universitet

November 17, 2015
JFB

Introduction to Computer Science
E15 – Discussion Sections – Week 48

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 slide 48 of the RSA used in lectures.

   (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 573. Try decrypting. What is the problem here if 1111 is interpreted in decimal instead of binary? What is the problem if each 1 is interpreted as a separate number to encrypt?

3. Do problem 50 on page 573.

4. Why is it necessary that $gcd(e_A, (p_A-1)(q_A-1)) = 1$? Find an example where the result is not equal to 1. You can use $e_A = 2$. Consider the last problem from last week with square roots in this context.

5. Try executing the Miller-Rabin primality test on 11, 15, and 561. With 561, try 2 or something else relatively prime to 561 as the random a. What happens differently if you try 3? Why? What is the difference between these three numbers (11, 15 and 561)?