Institut for Matematik og Datalogi
Syddansk Universitet

November 14, 2016
JFB

Introduction to Computer Science
E16 – Discussion Sections – Week 50

1. Why is a cryptographically secure hash function used in connection with RSA digital signatures? Give two reasons.

2. With RSA, why would you never use the value 2 as one of of the two primes for the modulus?

3. In RSA, why must the message being encrypted be a non-negative integer strictly less than the modulus?

4. Consider an RSA system with Alice's public key $N = 1517$ and $e = 17$. Note that $1517 = 37 \cdot 41$.

   (a) Find Alice's secret key d. Use the Extended Euclidean Algorithm from slide 51 of the RSA slides used in lectures. What multiplicative inverse did you find?

   (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? (To save time, do not do this in class.)

5. Why in RSA is it necessary that $gcd(e_A, (p_A - 1)(q_A - 1)) = 1$? Find an example (values e_A, p_A and q_A) where this greatest common divisor is not equal to 1.

6. 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)? Which calculations showed that the composite numbers were not prime?

7. 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.

8. 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.)

9. If you have time, try breaking these two:

   - This was entitled "Cold Country". It was encrypted using a monoalphabetic substitution 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.

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

     YMNX HWDUYTLWFR NX JFXD YT IJHNUMJW.

     Discuss which techniques you used.