Institut for Matematik og Datalogi
Syddansk Universitet
JFB

March 11, 2005

Cryptology – F05 – Lecture 6

Lecture, March 4

We finished section 3.6 and began on chapter 5 in the textbook. We covered the Chinese Remainder Theorem and section 5.3.

Lecture, March 11

We will continue with chapter 5.

Lecture, March 18

We will continue with chapter 5.

Problem session March 16

1. Do problems 5.9 and 5.17 in the textbook.
2. Do problem 5.13. Note that the decryption exponent should be d, not a, so there is a typo. Use $d = 477,319$.
3. Suppose $n = 11,820,859$ is an RSA modulus. Suppose you know $\phi(n) = 11,813,904$. Find the factors of n. Show your work. (You may use Maple to solve the quadratic equation, but explain how you used it.)
4. Find all square roots of 64 modulo 105.
5. Find a primitive element (generator) in the multiplicative group modulo 107 ($\mathbb{Z}_{107}^*$) and show that it is a primitive element.

6. Consider the following proposal for a primality test for an integer n: Check if $2^n - 2$ is divisible by n. Answer "prime" if it is and "composite" if it is not.

   a. Give an odd prime for which this test works correctly and an odd composite for which it also works correctly.

   b. Prove that the test answers "prime" for all primes.

   c. Show that it answers "prime" incorrectly for $n = 341$. Use Fermat's Little Theorem to compute $2^{341} \pmod{p}$ for each prime factor of 341. Then use the Chinese Remainder Theorem, to compute $2^{341} \pmod{341}$.

Assignment due Friday, April 1, 10:15 AM

Note that this is part of your exam project, so it must be approved in order for you to take the exam in June, and you may not work with others not in your group. If it is late, it will not be accepted (though it could become the assignment you redo). You may work in groups of two or three.

1. With RSA, there are often recommendations to use a public exponent $e = 3$.

   a. What would the advantage to this be?

   b. If $e = 3$, the two prime factors dividing the modulus, p and q, must be such that $p \equiv q \equiv 2 \pmod{3}$. Why is it impossible to have one or both of p and q congruent to 0 or 1 modulo 3?

   c. Suppose that $e = 3$, $p = 3r + 2$ and $q = 3s + 2$. What would the decryption exponent d be?

2. Suppose that user A wants to send a message $s \in \{s_1, s_2, ..., s_k\}$ to user B, where $s_i < 1024$ for $1 \leq i \leq k$. Assume that RSA is secure (when the modulus is large enough and is the product of two equal length prime factors).

   a Why would you still advise user A not to use RSA directly?

   b What would you recommend instead, if you still wanted to use RSA?

3. Find a primitive element (generator) in the multiplicative group modulo 103 ($\mathbb{Z}^*_{103}$) and show that it is a primitive element.

4. Suppose we have a set of blocks encoded with the RSA algorithm and we do not have the private key. Assume $(n = pq, e)$ is the public key. Suppose also that someone tells us they know one of the plaintext blocks has a common factor with n. Does this help us find the plaintext used to produce these blocks? If so, how? If not, why not?

5. Do problem 5.16 in the textbook.