Institut for Matematik og Datalogi
Syddansk Universitet

March 6, 2003
JFB

Cryptology – F03 – Note 5

Lecture, February 25

We finished chapter 3 in the textbook, skipping most of the first four sections. We also covered section 5.1 and the beginning of section 5.3.

Lecture, March 4

We will continue with chapter 5. Note that subsections 5.2.1 and 5.2.3 were covered in discussion sections earlier.

Lecture, March 11

We will continue with chapter 5.

Assignment due Thursday, March 20, 8:30 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. If it is late, it will not be accepted.

1. 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 $2^{341} \pmod{341}$.

2. Do problem 5.9 in the textbook.

3. 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?

4. Consider the following cryptosystem:

   - Choose an odd number E.
   - Choose two prime numbers, P and Q, where $(P-1)(Q-1)-1$ is evenly divisible by E.
   - Calculate $N = P \cdot Q$.
   - Calculate $D = \frac{(P-1)(Q-1)(E-1)+1}{E}$.

   Explain how this system is similar to RSA.

   Explain how this system is different from RSA.

Problems for Thursday, March 13

For problems using Maple, it is fine if you use Mathematica instead.

1. First, we will discuss the problems from the first assignment.
2. Look at problems 5.3, 5.6, and 5.7 in the textbook. If you are at all unsure of how to do them, please do them. Even if you are not unsure, you might consider this an opportunity to try using Maple. The following Maple functions should be useful: `igcdex` (extended Euclidean algorithm for integers), `mod` (where the operation `&^` should be used for more efficient modular exponentiation - try them both to compare), `msolve` (solve equations in $\mathbb{Z}_m$), and `chrem` (Chinese Remainder Algorithm).
3. Another easy problem. Let $n = 143$ be a modulus for use in RSA. Choose a public encryption exponent e and a private decryption exponent d which can be used with this modulus. Try encrypting and decrypting some value to see that the exponents you have chosen work.
4. Suppose you as a cryptanalyst intercept the ciphertext $C = 10$ which was encrypted using RSA with public key $(n = 35, e = 5)$. What is the plaintext M? How can you calculate it?
5. In an RSA system, the public key of a given user is $(n = 3599, e = 31)$. What is this user's private key?