Institut for Matematik og Datalogi
Syddansk Universitet

November 15, 2016
JFB

Cryptology – E16 – Lecture 14

Announcement

The next pizza meeting will be held starting at 16:00 in U163 on November 23.

Lecture, November 9

We finished with the Goldwasser-Micali encryption system, covered section 3.1, and finished section 16.1.

Lecture, November 15

We will continue with chapter 16 and cover sections 4.1, 4.2, 4.3, and 4.5, with emphasis on curves of characteristic $p > 3$.

Lecture, November 21

We will cover some digital signature schemes from chapter 16 and begin on chapter 19.

Problem session November 16

1. A plaintext x is said to be *fixed* if $e_K(x) = x$. Show that for RSA, the number of fixed plaintexts $x \in \mathbb{Z}_N^*$ is equal to

   $$\gcd(e-1, p-1) \cdot gcd(e-1, q-1),$$

   where the modulus $N = p \cdot q$, and e is the exponent in the public key. Hint: Use the Chinese Remainder Theorem. (Problem 5.18 in CTP.)

2. Using various choices for the bound B, attempt to factor 262063 and 9420457 using Pollard's $p-1$ method. How big does B have to be in each case to be successful? (Problem 5.25 in CTP.)

3. Suppose you, as a cryptanalyst were interested in an RSA modulus N, and you were given a t such that $a^t \equiv 1 \pmod{N}$ for all $a \in \mathbb{Z}_N^*$. (Note that t is not necessarily $\phi(N)$. In the case $N = 69841$, $\phi(69841) = 69300$, but t could have many other values including 2310 and 138600.)

   (a) Give an efficient algorithm for determining the message m which was encrypted using the public exponent e, producing the cryptotext c.

   (b) Give an efficient algorithm for factoring N. (Hint: some ideas from the Miller-Rabin primality testing algorithm may be helpful.)

4. 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?

5. I may lecture at the end.