Institut for Matematik og Datalogi
Syddansk Universitet

November 8, 2019
JFB

Cryptology – 2019 – Lecture 14

Announcements

1. All lectures on Thursdays will start at 16:10, instead of 16:15.
2. Lecture on Thursday, November 21, is cancelled.
3. The next pizza meeting will be held starting at 16:00 on November 18.

Lecture, November 5

We covered factoring from sections 2.3 and 2.4, and finished chapter 15 (still need to mention fault analysis, though). The problems "parity" and "half" I talked about in connection the security of RSA are the functions B_1 and B_h from section 11.8.2 in the textbook. The problems from lecture notes 10 and 11 (problems 1a, 1b) were covered on November 4.

Lecture, November 11

We will start on chapter 16, and cover section 3.1 and 3.2, subsections 18.4.3 and 18.4.3, and subsection 11.7.2.

Lecture, November 14

We will continue with chapter 16, covering up through section 16.5, and cover sections 4.1, 4.2, 4.3, and 4.5, with emphasis on curves of characteristic $p > 3$.

Problem session November 12

We will finish any problems not finished on November 7.

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.