Institut for Matematik og Datalogi
Syddansk Universitet

November 8, 2016
JFB

Cryptology – E16 – Lecture 13

Announcement

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

Lecture, November 7

We covered section 2.2–2.4 in chapter 2 and quickly covered the remainder of 15. We introduced the Goldwasser-Micali encryption system in chapter 16.

Lecture, November 9

We will finish with the Goldwasser-Micali encryption system, cover section 3.1, finish section 16.1, and possibly cover section 16.2.

Lecture, November 15

We will continue with chapter 16.

Problem session November 14

1. How slow is the Goldwasser-Micali encryption scheme compared to RSA?

2. Consider the following algorithm:

   procedure DiscreteLog(p, g, h):
   { Input: An odd prime p, $g, h \in \mathbb{Z}_p^*$, $h = g^x \pmod p$ }
   { Output: x }

{ Initialize }
$\ell \leftarrow h$
$index \leftarrow \Lambda$
while $(\ell \neq 1)$ **do**
    if $\left(\frac{\ell}{p}\right) = 1$ **then** $index \leftarrow 0||index$
        else
            { change QNR to QR, only changing low order bit of index}
            $index \leftarrow 1||index$
            $\ell \leftarrow g^{-1} \cdot \ell \pmod{p}$
    { ℓ is a QR }
    $\ell \leftarrow \sqrt{\ell} \pmod{p}$
return$(index)$

- Why, at first glance, does this algorithm appear to solve the discrete logarithm problem modulo a prime efficiently?
- What is wrong with the algorithm?
- What does this say about some other problem being hard?