Institut for Matematik og Datalogi
Syddansk Universitet

October 29, 2019
JFB

Cryptology – 2019 – Lecture 13

Announcements

1. All lectures on Thursdays will start at 16:10, instead of 16:15.
2. Lectures on Thursday, October 31, and Thursday, November 21, are cancelled.

Lecture, October 28 and 29

We covered section 2.1. The slides are used are on the course homepage, those related to RSA. Note that by finishing primality testing, we have now seen that RSA can be implemented efficiently. On these dates, we also finished the problems from lecture note 9 and started on the Solovay-Strassen problem from lecture note 10.

Lecture, November 5

We will cover factoring from sections 2.3 and 2.4, and finish chapter 15. The problems from lecture notes 10 and 11 will be covered (though maybe not finished) on November 4.

Lecture, November 11

We will start on chapter 16, and cover section 3.1.

Problem session November 7

We will finish any problems not finished on November 4.

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?