Institut for Matematik og Datalogi
Syddansk Universitet

December 5, 2019
JFB

Cryptology – 2019 – Lecture 19

Announcement

1. Information about the exam and the required task for being allowed to take the exam are now available on the course homepage.

2. I have moved the remaining lectures on Thursdays to Mondays and Tuesdays in December.

Lecture, December 2

We finished protocols from the slides, covering up through the zero-knowledge proof for quadratic nonresiduosity (finished on December 3).

Lecture, December 9

We will look at zero-knowledge proofs for graph isomorphism and graph nonisomorphism. The graph isomorphism result is in section 21.1. The graph nonisomorphism result is just another example similar to the quadratic nonresiduosity. (Special soundness is defined in section 21.3.) We will also go over some problems from the second assignment and get volunteers to do more on December 10.

Problem session December 10

We will go over some problems from the second assignment and some problems not finished on December 3. We may talk about the exam or do that on December 16.