Christian Schindelhauer

Freiburg, 2016-01-29
Joan Bordoy
Sebastian Sester

Exercise No. 13
Peer-To-Peer Networks
Winter 2015

Exercise 1 *Shamir's Secret Sharing*

Give an example (with formulars and values) for Shamir's secret sharing where four people share a secret and where two of them are required to reveal the same. You do not have to use Galois fields and you may use low numbers (numbers, which could be cracked within milliseconds in praxis). Can a single person decode the secret on their own, too?

Exercise 2 *Blakley's Secret Sharing*

Repeat the previous task for Blakley's Secret Sharing.

Exercise 3 *Cryptographic functions*

Explain what kind of cryptographic function each of the following names describes and whether its use is recommended or not.

1. DES
2. AES
3. SHA-1
4. SHA-2
5. MD5
6. RSA
7. Whirlpool

Exercise 4 *Basic cryptographic knowledge*

1. Explain the difference between a cryptographic hash- and a cryptographic encryption-function. Can you use a hash function as an encryption function? What about the other way around?
2. Explain the difference between a block and a stream cipher. Can you use a block cipher as a stream cipher, too?