Christian Ortolf

Freiburg, 2017-02-03
Aditya Oak

Exercise No. 14

Peer-To-Peer Networks

Winter 2016

Exercise 1 *Three Byzantine Generals* According to the lecture, the Problem of Byzantine Generals can only be solved for three generals if cryptography is used.

1. Find the original work in the literature where this has been shown.
2. Explain why and how it can be solved with cryptography.
3. Elaborate the requirements for the used cryptographic algorithm.
4. Can you use AES here?

Exercise 2 *Freenet*

Assume Edward Snowden puts some secret files from the NSA into Freenet. Is it safe from the NSA, who wants to take it down?

Exercise 3 *Onion Routing* Assume that while uploading the data from the previous exercises, Snowden additionally used Onion Routing to hide himself. Discuss what possibilities would the NSA could have to deanonymise him during the upload?