Christian Ortolf

Freiburg, 2017-01-19
Aditya Oak

Exercise No. 12
Peer-To-Peer Networks
Winter 2016

Exercise 1 *Basic security terms*

Explain each of the three main goals of security:

1. Confidentiality
2. Integrity
3. Availability

Also, name and explain an attack for each of the three.

Exercise 2 *(Distributed) Denial of Service attacks*

Explain whether DoS- and DDoS-attacks are the same in regard to:

1. The result
2. How easy or difficult the attack can usually be blocked
3. The basic systematics behind the attack

Exercise 3 *AES / RSA*

Explain whether (and why) you would use RSA or AES in the following situations:

1. Encrypted transfer of a large file
2. Secured, but unencrypted transfer of a large file
3. Sending a large mail to a person which is not online at the moment you?re writing the mail

Exercise 4 *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*