Technische Universität München
Lehrstuhl Informatik VIII
Prof. Dr.-Ing. Georg Carle
Dr. Heiko Niedermayer
Cornelius Diekmann, M.Sc.
Dr. Ralph Holz

Network Security Winter Term 2014/2015
Short Exercise 4

Repetition 1 Modes of Encryption

a) Why are modes of encryption necessary?

b) What is required if the length of the message to encrypt is not a multiple of the cipher's block size?

c) Are modes of encryption necessary for stream ciphers?

Repetition 2 This task is about the IV in CBC

a) What is the main purpose of the IV?

b) Is it required that the IV is transmitted encrypted?

c) Is it required that the IV is fresh?

d) Is it required that the IV is transmitted with integrity protection?

Repetition 3 Disc Encryption

In this task, assume you want to encrypt your hard drive. We have a very simple attacker model: At exactly one point in time, the attacker will steal your hard drive. The attacker does not have access to the disc before she steals it. The attacker can not return the disc to you and steal it again.[1]

a) Is it a good idea to use ECB?

b) Is it a good idea to use CBC?

c) Is it a good idea to use OFB?

d) Is it a good idea to use CTR?

[1] Stronger attacker models lead to different conclusions than we will draw in this task. If you are interested, you can start reading at http://en.wikipedia.org/wiki/Disk_encryption_theory