Secure and Dependable Systems
Jacobs University Bremen
Dr. Florian Rabe

Homework 6
given: 2017-04-27

Homework 6

You have to submit your solutions as announced in the lecture.
Unless mentioned otherwise, all problems are due 2017-05-04, before the lecture.
There will be no deadline extensions unless mentioned otherwise in the lecture.

This homework is not published yet. I may still change it before publishing it.

Problem 6.1 *Practice: Building an Encryption Scheme*

Points: 5

Implement abstract classes for

- symmetric encryption schemes
- block ciphers

Implement concrete classes for

- the block cipher from the exercise in Sect. 15.3.3 in the lecture notes
- the encryption scheme that takes a block cipher and the IV and uses the CBC mode of operation

Combine the two concrete classes into an encryption scheme and write a unit test that checks the inversion condition: randomly generate a sequence of blocks, encrypt it, decrypt the ciphertext, and check for equality.

Problem 6.2 *Practice: Relevance of Modes of Operation*

Points: 2

Use your implementation from the previous problem to encrypt a file.

This should be a real file in an uncompressed format, e.g., a bitmap image. It should be big enough to consist of many blocks.

Modify your implementation to use the trivial mode of operation (where no IV is used and each block is simply passed to the block cipher). Encrypt the same file with this mode as well and compare both results with the original.

Note: This homeworks aims at reproducing the effect from the penguin image example at https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Electronic_Codebook_.28ECB.29.

Problem 6.3 *Theory: Security Analysis*

Points: 3

Consider the block cipher from the exercise in Sect. 15.3.3 but using only 1 round.

We define an encryption scheme using the trivial mode of operation that chooses an 8-bit key k and then encrypts every 8-bit block by applying the block cipher.

Informally prove the following

1. E is comp-ind if k is chosen with a PRG.
   Hint: This is already true for networks that use no substitution or permutation steps and only one key step.

2. E is *not* CPA-ind secure.
   Hint: To break E with a chosen-plaintext attack, the adversary can try to recover the key by encrypting a self-chosen message.