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 example in the lecture
- the encryption scheme that takes a block cipher and the IV and uses the CBC mode of operation

Every instance of the encryption scheme should represent one session, i.e., multiple calls of encryption for the same block should return different results.

Write a unit test that checks the inversion condition: randomly generates some blocks, encrypt and decrypt them, 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 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

We define a block cipher that maps a 16-bit key k to a bijection $E_k : \mathbb{Z}_{16} \to \mathbb{Z}_{16}$ as follows:

- Let $S : \mathbb{Z}_4 \to \mathbb{Z}_4$ be the substitution $x \longmapsto ((x+1) \cdot 3) \bmod 5 - 1$ (which is a bijection).
- Let $P : \mathbb{Z}_{16} \to \mathbb{Z}_{16}$ be the permutation that does a cyclic 1-bit left-shift of the binary representation of its argument.
- Let $\text{addKey}_k : \mathbb{Z}_{16} \to \mathbb{Z}_{16}$ be the bijection $x \longmapsto x \oplus k$ (bit-wise xor).
- Finally let E_k by $\text{addKey}_k \circ P \circ S^4$ where S^4 means that S is applied separately to every 4-bit chunk of its argument.

No we define an encryption scheme using the trivial mode of operation that chooses a key k and then encrypts every 16-bit block b as $E_k(b)$.

Informally prove the following

1. E is comp-ind if k is chosen with a PRG. It might help to first show that addKey applied to each individual block is already comp-ind secure.
2. E is *not* CPA-ind secure. E can be broken deterministically using a chosen-plaintext attack. Since the security of E is mainly based on addKey, it might be useful to think about recovering the key using a chosen-plaintext attack.