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.

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 with some repetitive structure 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 secure 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: The adversary can perform a chosen-plaintext attack to recover the key by encrypting a self-chosen message.

Solution: For $x \in B^8$, we have $E_k(x) = C(x) \oplus k$ where $C : B^8 \to B^8$ is the bijection of the substitution and the permutation step. Note that C is fixed, non-random, and public. Thus, an adversary that knows $y = E_k(x)$ can recover the key via $k = y \oplus C(x)$ (*).

1. We proceed indirectly. Assume the scheme is not comp-ind secure, i.e., we have an adversary consisting of
   - a pick $n \mapsto (x_1 \in \Sigma^n, x_2 \in \Sigma^n)$ of messages,
   - a PPT $A(n \in \Sigma^*) \in \{1, 2\}$ that guesses whether its input is the encryption of x_1 or x_2,

such that the guess is correct with 1/2-plus-non-negligible probability.

The guess of A can be used together with (*) to guess the key. Because the key is the output of the PRG, if we can guess the key with non-negligible probability, we can guess whether something is the output of the PRG with non-negligible probability. Thus, we can use A to build an adversary A' that disproves the PRG property.

2. In a CPA-attack, the adversary can ask for the encryption $y = E_k(x_0)$ of some $x_0 \in B^8$ and then use (*) to recover the key.
