Advanced Cryptography: Lightweight Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

1. Exercise sheet
Hand in solutions until Monday, 07 November 2011, 23:59:59h.

A word on the exercises. They are important. Of course, you know that. You need 50% of the credits to be admited to the final exam. As an additional motivation, you will get a bonus for the final exam if you earn more than 70% or even more than 90% of the credits. The bonus does not help passing the exam, but if you pass the bonus will increase your mark by up to two thirds.

If you find any errors in the sheets, do not hesitate to write an email to the mailing list `11ws-ac@lists.bit.uni-bonn.de`.

Exercise 1.1 (Secure email). (6 points)

(i) Send a digitally signed email with the subject [4]

`[11ws-ac] hello`

to us at

`nuesken@bit.uni-bonn.de` and `daniel@bit.uni-bonn.de`

from your personal account. The body of your email must be nonempty and the signature must be verifiable and correct. [It is a good idea to verify this by sending a blind carbon copy (Bcc) to oneself.]

With Thunderbird we recommend using `enigmail` and `gpg`. In any case make sure to register your key eg. at `http://gpg-keyserver.de/`.

Choose yourself among this and possible other solutions. In any case use a pgp key pair.

(ii) Find the fingerprint of your own PGP key. Bring two printouts of it and an identification document to the next tutorial. (Do not send us an email with it. Guess, why!) [2]

Note: Future exercise hand-ins will only be accepted via signed email. Then a bonus point will be awarded for a correct signature and a malus for a missing or invalid signature.

Exercise 1.2 (AES amputated). (11 points)

The Advanced Ecnryption Standard (AES) is an extremely simple cipher and its description is very short. But still, can we make it even simpler, by hacking out superfluous bits without impacting on its strength?

2 (i) Give a high-level description of AES and explain shortly the different steps during one round.

Considering the four steps (`SubBytes`, `ShiftRows`, `MixColumns` and `AddRoundKey`) performed in each round, we want to see whether those steps are essential or not to the security of the cipher.

2 (ii) For instance, what would happen to AES should one remove the `SubBytes` step in each round?

2 (iii) What if one were to remove the `ShiftRows` step?

2 (iv) What about the `MixColumns` step?

2 (v) And the `AddRoundKey` step?

1 (vi) Conclude.

Exercise 1.3 (RFID design). (10 points)

10 In the lecture we encountered many security threats that RFIDs may have to face. We saw that when you realize a tag as an identifier carrying unit only (that can be read out via some command) many of the security features are not fulfilled. Design another *simple* RFID system that fills one of the security gaps left open in the lecture. Analyze your solution with respect to the security threats presented in the lecture.