Esecurity: secure internet & e-passports, summer 2011

Michael Nüsken, Raoul Blankertz

2. Exercise sheet
Hand in solutions until Sunday, 17 April 2011, 23:59

Exercise 2.1 (SMTP and mail format). (10 points)

(i) Look up the RFCs for SMTP and ESMTP, and describe briefly the major differences. $\boxed{4}$

(ii) Consider the virus warning "`[11ss-esec: <your name>] Virus warning`" that was sent to you on Wednesday, 13 April 2011, 18:26. (You might have to retrieve it from your spam folder...)

(a) Find out how to display the source code and copy the first ten lines or so. $\boxed{1}$

(b) Which parts are suspicious, which are not? $\boxed{2}$

(c) Which actions are appropriate in reaction to such a mail? $\boxed{1}$

(d) How do you know whether the warning is true? $\boxed{1}$

(e) What is the damage caused by it? $\boxed{1}$

Exercise 2.2 (LFSR over $\mathbb{F}_2$). (4 points)

Consider an LFSR given by $n \in \mathbb{N}_{\geq 1}$ and a linear function $f\colon \mathbb{F}^n \to \mathbb{F}$ with $f(x_0, \ldots, x_{n-1}) = \sum_{0 \leq i < n} f_i x_i$. For given $(a_0, \ldots, a_{n-1})$ let $A = (a_i)$ be the sequence defined by $a_{n+\ell} := f(a_\ell, \ldots, a_{n+\ell-1})$ for $\ell \in \mathbb{N}$. The output of the LFSR are the bits a_n, a_{n+1} and so forth. $\boxed{4}$

How many consecutive bits of the output sequence are needed to calculate f (ie. to calculate the coefficients $f_0, \ldots, f_{n-1}$)? Give a reason for your answer.

Exercise 2.3 (AES-CTR). (10+2 points)

The files mentioned in this exercise can be downloaded from the web page.

4 (i) The two files `text1.enc` and `text.enc` are both encrypted using AES-CTR with the same key and the same initialization vector. The plain text of `text1.enc` is zero (ie. 0x00 00 ... 00). What is the plain text of `text2.enc` (encoded with Unicode UTF-8)?

4 (ii) The file `stud.enc` is encrypted by using 128bit-AES in CTR-mode and the third 128-bit block of the plain text is zero (ie. 0x00 00 ... 00). Change this block such that when the file is decrypted your student ID is written at this place (encoded with Unicode UTF-8). Attach your changed file to the email with your solution to the other exercieses.

2+2 (iii) Interpret your observations: Does this mean that AES-CTR is a bad encryption scheme to use? Is it thus even broken?