Security on the Internet, summer 2006

MICHAEL NÜSKEN

4. Exercise sheet

Hand in solutions on Tuesday, 16th of Mai, at the b-it info desk. Deadline for any completely signed(!) electronic solution is the same Tuesday, 23:59.

Exercise 4.1 (Modes of operation). (5 points)

(i) Discuss advantages and disadvantages of each of the modes of operation presented in class: ECB (Electronic Codebook) and CBC (Cipher Block Chaining). [1]

(ii) Answer the following questions concerning error propagation for each of the aforementioned modes. [2]

(a) How many text blocks are false if one of the transmitted blocks is corrupted?

(b) How many text blocks are false if one of the transmitted blocks is dropped unnoticed?

(c) How many text blocks are false if one of the block cipher boxes outputs a wrong result?

Try to draw conclusions from your observations.

(iii) Look up the definitions for the modes CFB (Cipher Feedback), OFB (Output Feedback) and discuss one of them. [2]

Exercise 4.2 (Repeated multiplication in a finite group). (6 points)

Consider the group $\mathbb{Z}_{101}^{\times}$.

(i) How many elements does it have? [2]

(ii) Choose an element $x \in \mathbb{Z}_{101}^{\times}$ at random. Start at $z = 1$ and multiply z by x again and again, so you compute 1, x, x^2, x^3, ... [3]

What do you observe? Does the sequence repeat? Do we ever get back to 1? (Try to answer these questions before executing the experiment.)

Let the order $\mathrm{ord}(x)$ of x denote the number of different z's that are generated, mathematically speaking, $\mathrm{ord}(x) = \#\left\{x^i \,\middle|\, i \in \mathbb{N}\right\}$.

Repeat the experiment until you have observed at least four different values for $\mathrm{ord}(x)$.

(iii) Which orders $\mathrm{ord}(x)$ have you observed? How do they relate to the number of available elements? Which is the maximum possible value? [1]

Exercise 4.3. (6 points)

Visit the following websites:

2 (i) `http://www.meganet.com/`, in particular `http://www.meganet.com/Technology/intro.asp` and `http://www.meganet.com/News/press/pressrelease04-01-01.asp`,

2 (ii) `http://www.usdsi.com/`, and

2 (iii) `http://www.privacy.li/` (Look at the company profile!), in particular `http://www.privacy.li/drivecrypt.htm`.

Describe (in a few words) what they claim about the security of their systems and where the security is based upon.

Would you use advice their cryptography for government security applications?