Security on the Internet, summer 2006

MICHAEL NÜSKEN

5. Exercise sheet

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

Exercise 5.1 (Cryptanalysis). (10 points)

At `http://www.cryptool.de/` you can download the CrypTool. It incorporates a lot of cryptographic algorithms and analyses.

Download the file `text01.txt`. Agent Leach reports: It was encrypted using the Vigenère cipher.

(i) Look up the definition of this cipher and summarize it in your own words. [2]

(ii) Use CrypTool to decrypt the file. 'Who' is the key? What is a Ningi? [1]

(iii) How does the previous attack work and succeed? [2]

Download the file `text02.txt`. Agent Leach reports: Text 2 was encrypted using DES in CBC mode, the key written in hexadecimal gives a decimal date (so it starts with 8 zero hex-digits).

(iv) Look up the most important dates and facts in the DES history. [Why were so many people suspicious that there might be a backdoor in DES? And how has NIST (Who is this?) tried to prevent that in the selection of AES?] [2]

(v) Use CrypTool to decrypt the file. How much time does CrypTool need when it has to look for 20 key bits? Which date served as key? And what happened to the man who said 'how great it would be to be nice to people for a change' according to the text? [2]

(vi) How much time would you have needed to find a complete 56 bit key? [1]

Exercise 5.2 (RSA). (10 points)

3 (i) We want to build an RSA system using the prime numbers $p = 17$ and $q = 23$. (In practice these prime numbers are of course much to small!) Furthermore we choose $e = 15$ and $N = p \cdot q$ for our public key. Use the extended Euclidean Algorithm to compute a matching private key d so that holds: $e \cdot d = 1$ in $\mathbb{Z}_L$ with the repetition length $L = (p-1)(q-1)$.

Important: You must hand in the entire tableau of the extended Euclidean scheme!

2 (ii) Encrypt $x = 304$ to obtain the answer. (Describe intermediate steps!)

2 (iii) Decrypt $y = 66$ to obtain the answer. (Note that some answers do not change. ;-))

3 (iv) Compute $3^{1\,000\,000\,003} \bmod 101$ by hand. *Note*: Only a small calculation is needed! Argue. Brute force does not earn credits here.