Cryptography, winter 2014/2015

PRIV.-DOZ. DR. ADRIAN SPALKA, DR. DANIEL LOEBENBERGER

8. Exercise sheet
Hand in solutions until
Wednesday, 07 January 2015, 23:59:59

Exercise 8.1 (DAC and MAC). (5 points)

In the lecture we discussed two fundamentally different access control mechanisms: discretionary access control and mandatory access control. Prove that they are actually equivalent. [5]

Exercise 8.2 (The Advanced Encryption Standard running). (11 points)

In this exercise we put hands on AES. There are three versions standardized, each with 128, 192 and 256 bit keys, respectively. We will play with AES-128, the version employing a 128 bit key.

(i) Find a library implementing the AES-128 in a programming language of your choice. Name the library and explain why you selected it. [2]

(ii) Now, using a randomly selected key (you might use the all zeroes key as well), run AES-128 for $i = 0 \ldots 27$ on 2^i blocks encoding the block number j in some suitable fashion. For example, the 128-bit block corresponding to $j = 1$ would be [7]

$$\underbrace{00\ldots00}_{\text{127 zeroes}}1.$$

Compute average runtime and deviation on each of the 2^i encryptions. Hand in your code.

(iii) Interpret the results. [2]

Exercise 8.3 (Modes of operation). (8 points)

(i) Discuss advantages and disadvantages of each of the modes of operation presented in class: ECB (Electronic Codebook), CBC (Cipher Block Chaining), and CTR (Counter mode). [2]

(ii) Answer the following questions concerning error propagation for each of the aforementioned modes. [6]

(a) Is encryption parallelizable? What about decryption?

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

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

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

Try to draw conclusions from your observations.

The following two exercises are thought to be solved on cold, boring holiday evenings. For getting the 20 bonus points for the exercises, respectively, you need to be very thorough in your argumentation. The solution will require several facts, which we did not discuss in the lecture or the tutorial, so there is some own research to be done.

Exercise 8.4 (A cryptanalytic challenge). (0+20 points)

+20 Cryptanalyse the following text found on the course webpage. Explain how you proceeded and find the corresponding plaintext.

```
Lizg lghlhh zbm esue br Exnpxv.  "Cbiw my cb?" dwqyl
Dvzbcu.  "Xny Plxibplokl'a Jyoxm ws zbm Jerufb.  Mz'm i
vsxn wi irykwvuhqf fuis.  Lx zytow eic hzklgwloho bsa
hmhh zi sqsc ujryz uvbxncvj.  Xnub'v mzm rrf." Glbkyx
ncurkx qw sbyz qixpwxwrs qq lom pdrjm.  "Q omqy bki
iidhv," ny admj.  "Xwq'x Vuvlg.  On'a wlk zquwz bmotlot
rv ohbhprcolfry bkmta iqchilb'w yuqg xu gm dpr xib."
"M'rf aksc swx luq qw aulsv," wgcl Isxx.  Ph wtubflkx qw
jxiu Dvzbcu ani edw ynqop nitgmta qw ey cn lx cua d
xci-ehiq-xmdh ruzn etx xxpryl lx uob rj ona fsbyz.  "Bsa
jzhwy nplw hobwst bmui eic vik uvg xny afvkyv ommbbv yv
aqymta gry zbm lrjyf." D wilmhr, gvwxx zbzhi ohkkiy vg
isal, tlx aj iqh ibiueinmuw hyodr zi nomiemu eilwvw zbm
vyxzifi.  "Eic zetn br otie dfuob Ysmivv, wu C mqxkl bkez
hipi yi." Plw lcvjixm bdtvyl vssy urvk embw.  "Ghl wlklm
zi glm." Wlk qwuhy Pwjst Wwqwzlcfxul Noikna ipglmg mt
azhit ukusym bki ywzhit.  Zwuh vlmvwkx i oexam uij vcwxuh
iw xny jrxziu rj zbm vgxymq etx ervjm jhkgh br ytxcoezy
ifvuma lx.  Gn bki yuuh xogm, wlk vwro hyodr zi asige bki
khbuc gm ehpr cv d wzcto uacmw qkuaxvkx drmiy.  Bkmy ca
zlgn bki hiwn wgcl.
```

Exercise 8.5 (A mathematical challenge). (0+20 points)

You and your bank want to agree on a common key via the `Diffie-Hellman protocol` in a multiplicative group $\mathbb{Z}_p^\times$. You know that in order to do so, a *large* prime number p has to be chosen and a generator for the multiplicative group $\mathbb{Z}_p^\times$ has to be determined. These may be tedious tasks. +20

As part of their Christmas campaign, the hardware company PIERPONTPRIMES-UNLIMITED advertises their exceptionally fast and cheap hardware for computations in specific multiplicative groups $\mathbb{Z}_p^\times$. Your bank has received a tempting offer, where p is the following 1024-bit prime number:

```
1073137282146338814025297276012340514033392142286643182 28\
5946106897867885100815144444489959819534285998417753833 51\
9511397207193450879131705172428770801749585396377454681 07\
8165004036511715043877217438068707562700109319150934601 13\
1782394001492737704925458198054954529649684761174385968 82\
0366678237029638036520 97
```

Of course, a long list of generators is included, so they would also spare themselves the work of searching for one of those.

Now, your bank turns to you: Since those two pieces of information (the chosen group and the chosen generator) are public anyways, there seems to be no reason to reject this offer.

Reply to this and justify your answer. (You may assume that the hardware really does the computations as claimed and nothing else.)

To spare you the nuisance of copying 309 decimal digits, there is a text-file containing p on the course-webpage.