Cryptography, winter 2015/16

MICHAEL NÜSKEN, SIMON SCHNEIDER

1. Exercise sheet
Hand in solutions until Friday, 6 November 2015, 23:59

For future exercises it might be important to use b-it computers. So please register an account for the b-it. (Ask at the infodesk for the procedure.)

A word on the exercises. They are important. Of course, you know that. You need 50% of the credits to be admitted 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.

Exercise 1.1 (Secure email). (4 points)

(i) Send a digitally signed email with the subject $\boxed{2}$

```
[15ws-crypto] hello
```

to us at

```
schneid@cs.uni-bonn.de,nuesken@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 I recommend using `enigmail` and `gpg`. In any case make sure to register your key at `http://pgp.mit.edu/`.

Choose yourself among this solution and possible others. 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 an email with it. Guess, why!) $\boxed{2}$

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 (Monoalphabetic cipher). (8 points)

The following text is encrypted by the monoalphabetic cipher:

> QDH FAX YN XKT ANRKDHXTJ PDROMDXTHG FQ XKT ANQDGKYFNDPET TNJ FQ XKT MTGXTHN GWYHDE DHU FQ XKT CDEDSI EYTG D GUDEE ANHTCDHJTJ ITEEFM GAN.
>
> FHPYXYNC XKYG DX D JYGXDNRT FQ HFACKEI NYNTXI-XMF UYEEYFN UYETG YG DN AXXTHEI YNGYCNYQYRDNX EYXXET PEAT CHTTN WEDNTX MKFGT DWT- JTGRTNJTJ EYQT QFHUG DHT GF DUDBYNCEI WHYUYXYVT XKDX XKTI GXYEE XKYNO JYCYXDE MDXRKTG DHT D WHTXXI NTDX YJTD.
>
> XKYG WEDNTX KDG - FH HDXKTH KDJ - D WHFPETU, MKYRK MDG XKYG: UFGX FQ XKT WTFWET FN YX MTHT ANKDWWI QFH WHTXXI UARK FQ XKT XYUT. UDNI GFEAXYFNG MTHT GACCTGXTJ QFH XKYG WHFPETU, PAX UFGX FQ XKTGT MTHT EDHCTEI RFNRTHNTJ MYXK XKT UFVTUTNXG FQ GUDEE CHTTN WYTRTG FQ WDWTH, MKYRK YG FJJ PTRDAGT FN XKT MKFET YX MDGN'X XKT GUDEE CHTTN WYTRTG FQ WDWTH XKDX MTHT ANKDWWI.
>
> DNJ GF XKT WHFPETU HTUDYNTJ; EFXG FQ XKT WTFWET MTHT UTDN, DNJ UFGX FQ XKTU MTHT UYGTHDPET, TVTN XKT FNTG MYXK JYCYXDE MDXRKTG.
>
> UDNI MTHT YNRHTDGYNCEI FQ XKT FWYNYFN XKDX XKTI'J DEE UDJT D PYC UYGXDOT YN RFUYNC JFMN QHFU XKT XHTTG YN XKT QYHGX WEDRT. DNJ GFUT GDYJ XKDX TVTN XKT XHTTG KDJ PTTN D PDJ UFVT, DNJ XKDX NF FNT GKFAEJ TVTH KDVT ETQX XKT FRTDNG.
>
> DNJ XKTN, FNT XKAHGJDI, NTDHEI XMF XKFAGDNJ ITDHG DQXTH FNT UDN KDJ PTTN NDYETJ XF D XHTT QFH GDIYNC KFM CHTDX YX MFAEJ PT XF PT NYRT XF WTFWET QFH D RKDNCT, FNT CYHE GYXXYNC FN KTH FMN YN D GUDEE RDQT YN HYROUDNGMFHXK GAJJTNEI HTDEYBTJ MKDX YX MDG XKDX KDJ PTTN CFYNC MHFNC DEE XKYG XYUT, DNJ GKT QYNDEEI ONTM KFM XKT MFHEJ RFAEJ PT UDJT D CFFJ DNJ KDWWI WEDRT. XKYG XYUT YX MDG HYCKX, YX MFAEJ MFHO, DNJ NF FNT MFAEJ KDVT XF CTX NDYETJ XF DNIXKYNC.
>
> GDJEI, KFMTVTH, PTQFHT GKT RFAEJ CTX XF D WKFNT XF XTEE DNIFNT-DPFAX YX, D XTHHYPEI GXAWYJ RDXDGXHFWKT FRRAHHTJ, DNJ XKT YJTD MDG EFGX QFHTVTH.

4 (i) Compute the frequency table. (Ie. for each ciphertext letter compute the frequency.)

4 (ii) Decrypt. (And find the key, as far as possible.)