Secure E-mail

[Ugeopgave 3] *

Mirza Hasanbasic

ABSTRACT

In this assignment we are looking at how to create a secure way to send e-mails using PGP and thunderbird's plugin enigmail. Furthermore why the size of the key was chosen and why it could be a problem to upload the revocation to someone. Read till the end to see if it is safe to use this method as a way to safekeep it for passwords

1. APPROACH TO THE ASSIGNMENT

The way I approached the assignment was to carefully read what I have to do. Hereafter I downloaded and installed thunderbird. When I was done installing thunderbird I found the enigmail plugin. But I had a problem installing PGP so I manually found PGP4WIN and installed this too. After this I created my key and uploaded it to pgp.mit.edu by copy the key to clipboard and upload it.

I have sent mails to janro.datanet@gmail.com and got it signed. More info in the appendix

2. CHOICE OF KEY

I choose the key type RSA and the key size is 4096 because there were some weaknesses discovered in SHA-1, which is the hash used by DSA. The reason to go with the key size of 4096 is if by any chance someone managed to find a way to crack something of the size of 2048 in 100 hours, then this doesn't mean that it will take 200 hours to crack the 4096. The downside with using a key size of 4096 is that it uses more CPU and more storage space, but this should not be that big of a problem for the sake of security

Although both algorithms are based on mathematical problems which are not proven to be secure, then I cannot be more secure by using one over the other, but since DSA is using SHA-1 then I might have a bigger security problem than with RSA.

.

*

DIKU '16 El Diku, Copenhagen

DOI: 10.475/133_7

3. REVOCATION

If I upload the revocation certificate as part of the assignment, then anybody with access to it will be able to revoke my key and I will lose all of my reputation on the OpenPGP. This is the only consequence, they will not be able to gain access to my private key. Since I probably never will need it unless my password gets stolen at any time then it will be a good idea to have the revocation certificate at hand at all time. This can be solved by creating a QR-code and print it. Hereafter I can delete the digital file and the only one who can access the revocation would be me with the QR-code.

4. SAFEKEEPING PASSWORD

The biggest problem can be some sort of compromise of the system. If I choose to store my key encrypted under a strong passphrase, then this could be compared to have the same risk as with a password manager. But if someone roots my system and manage to unlock my key then they will have all of my passwords. But since Eric is using his G-mail account, then it all depends on the Google teams ability to maintain security. It would still be a good idea to have a strong passphrase. This way it works kinda like double security. Someone would need both the G-mail password and the passphrase for the gpg key

But in the end the most important thing to remember is to have a strong passphrase, that contains both capitalization, numbers and special characters and this passphrase should be unique.

APPENDIX

A. PRINTOUT FROM MIT KEY SERVER

Figure 1: Both my ku-mail and my personal mail

B. EMAIL TO TA

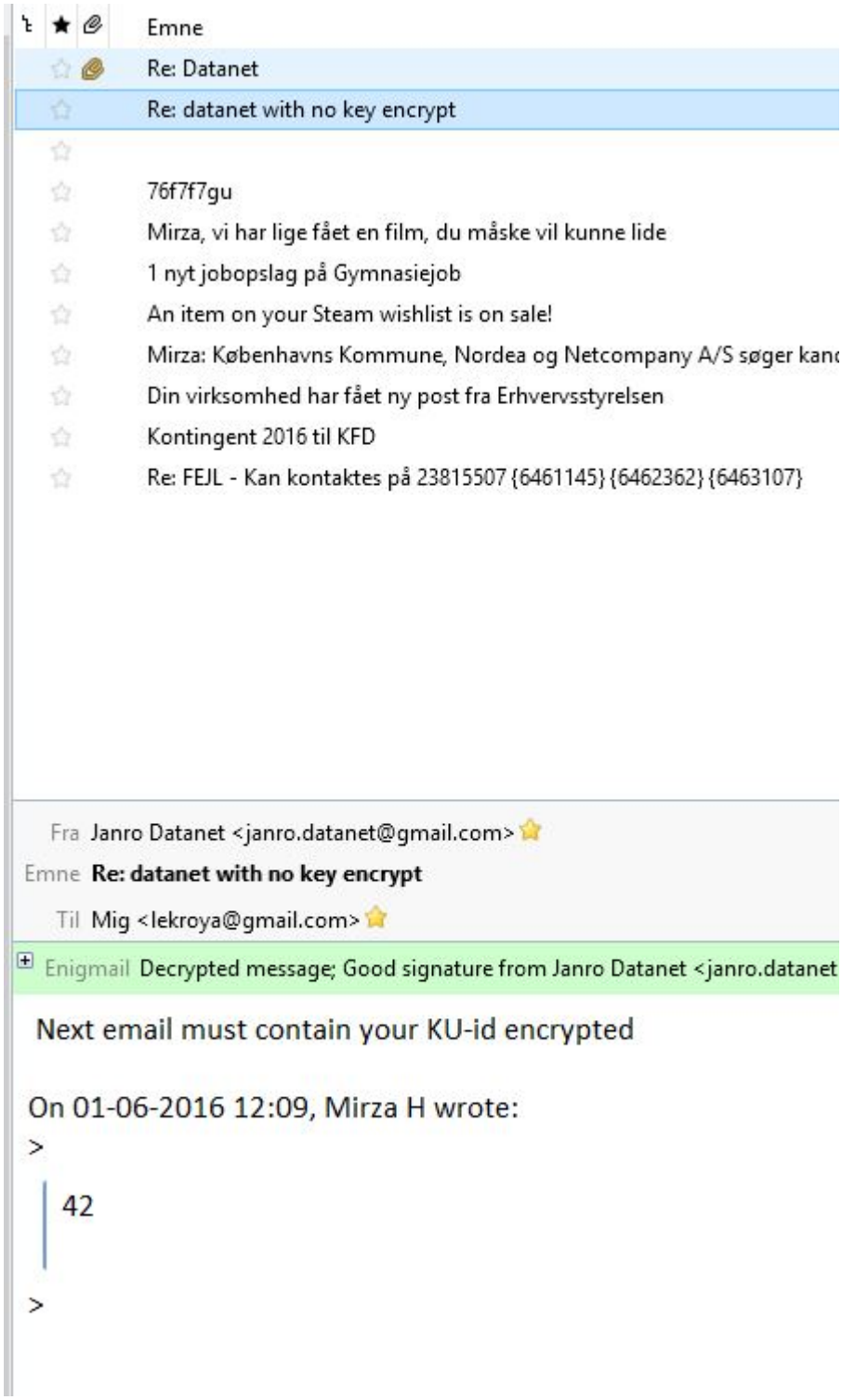

Figure 2: Showing that I sent an e-mail to a TA with the number 42

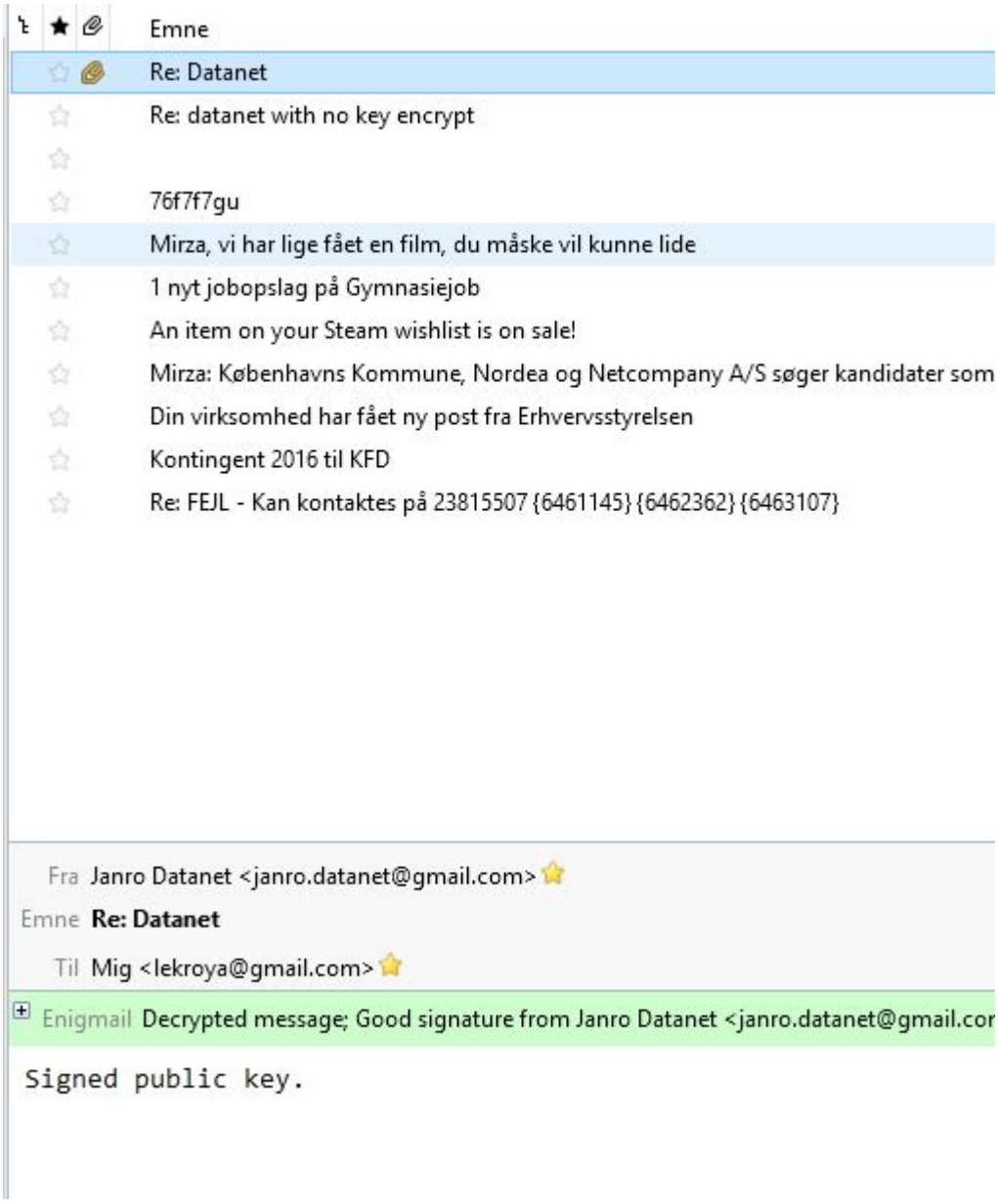

Figure 3: Showing that the TA signed the key

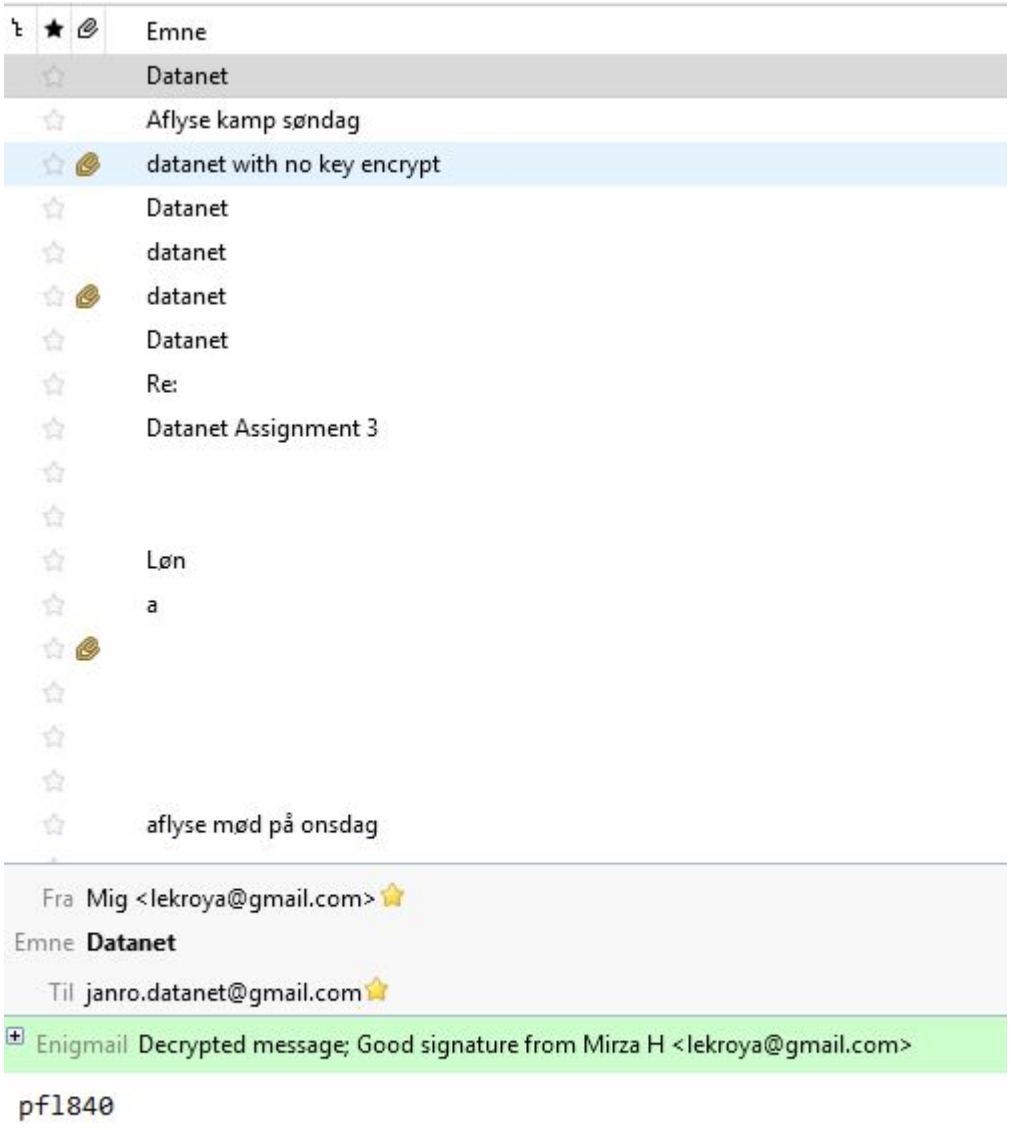

Figure 4: Showing that I sent an e-mail to a TA with my KU id

Search results for '0x7c6877233841bc4c'

```
Type bits/keyID     cr. time   exp time   key expir
------------------------------------------------------------------------------
pub  4096R/3841BC4C 2016-05-28

uid Mirza H <lekroya@gmail.com>
sig  sig3  3841BC4C 2016-05-28 __________ 2021-05-27 [selfsig]
sig  sig1  75F02C93 2016-06-01 __________ __________ Janro Datanet <janro.datanet@gmail.com>

uat [contents omitted]
sig  sig3  3841BC4C 2016-05-30 __________ 2021-05-27 [selfsig]
sig  sig1  75F02C93 2016-06-01 __________ __________ Janro Datanet <janro.datanet@gmail.com>

sub  4096R/2A1F555F 2016-05-28
sig sbind  3841BC4C 2016-05-28 __________ 2021-05-27 []
```

Figure 5: Showing that the key has been signed