


# Übungsprotokoll

## ITSI – Informationstechnologie Sicherheit

	<b>Übungsdatum:</b> 14.04.2020	<b>Klasse:</b> 2AHIT	<b>Name:</b> Felix Schneider
	<b>Abgabedatum:</b> 14.04.2020	<b>Gruppe:</b> ITS12	<b>Note:</b>
<b>Leitung:</b> Jürgen HAUPTMANN	<b>Mitübende:</b> Clemens Schlipfinger (Datei erstellen + senden)		
<b>Übungsbezeichnung:</b>  GPG-Verschlüsselung			

## Inhaltsverzeichnis:

1	Aufgabenstellung.....	2
2	Abstract (English).....	2
3	Theoretische Grundlagen .....	2
4	Übungsdurchführung.....	2
5	Ergebnisse.....	4
6	Code.....	4
7	Kommentar.....	4

## 1 Aufgabenstellung

Datenverschlüsselung GnuPG

## 2 Abstract (English)

Data encryption GnuPG

## 3 Theoretische Grundlagen

Es gibt 2 Schlüssel (private + public).

## 4 Übungsdurchführung

```
root@debian:~# gpg --gen-key
gpg (GnuPG) 2.2.12; Copyright (C) 2018 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

Hinweis: "gpg --full-generate-key" ruft den erweiterten Dialog auf.

GnuPG erstellt eine User-ID, um Ihren Schlüssel identifizierbar zu machen.

```
Ihr Name ("Vorname Nachname"): Felix Schneider
Email-Adresse: f.schneider@htlkrems.at
Sie haben diese User-ID gewählt:
"Felix Schneider <f.schneider@htlkrems.at>"
```

Ändern: (N)ame, (E)-Mail oder (F)ertig/(A)bbrechen? f

Bitte geben Sie die Passphrase ein,  
um Ihren Schlüssel zu schützen.

Passphrase:

<OK>

<Abbrechen>

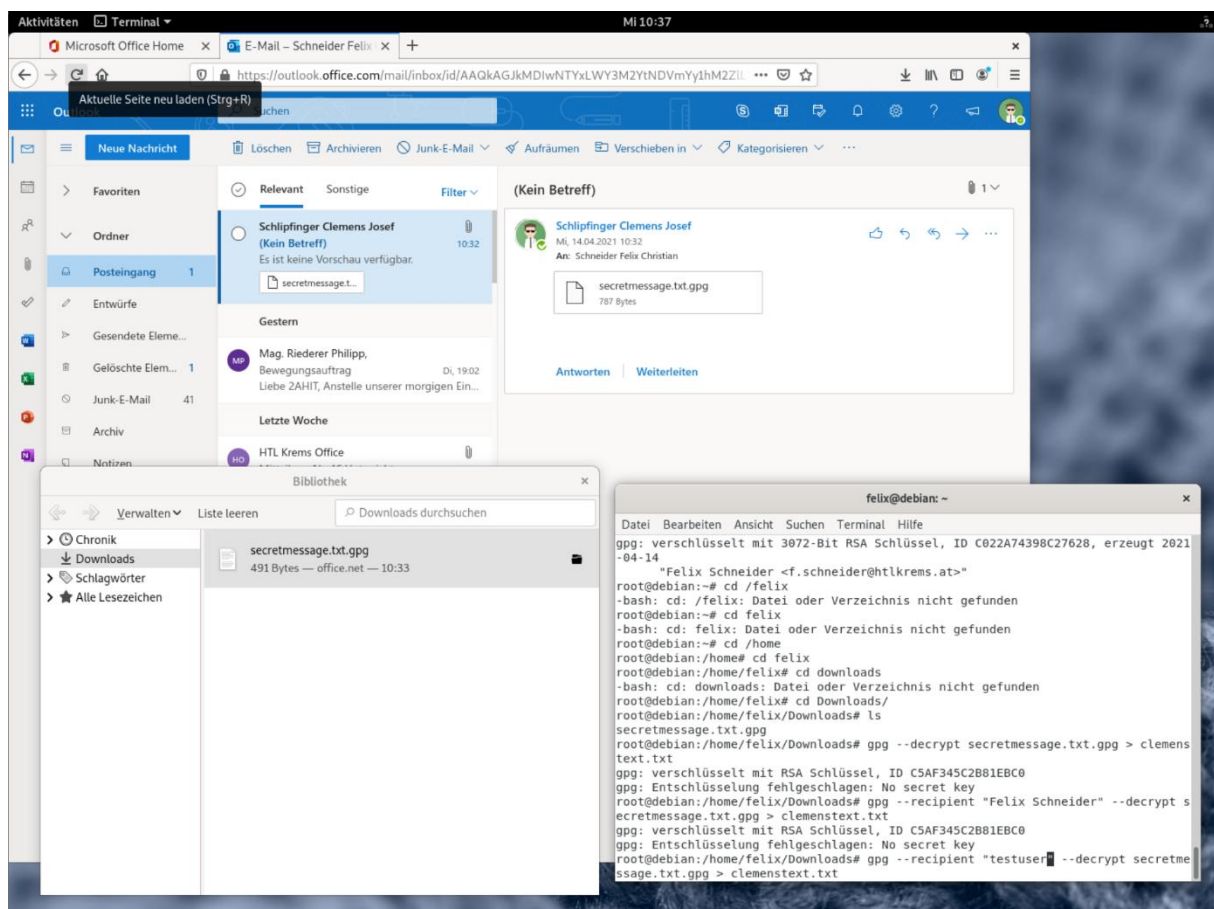
```

Ändern: (N)ame, (E)-Mail oder (F)ertig/(A)bbrechen? f
Wir müssen eine ganze Menge Zufallswerte erzeugen. Sie können dies
unterstützen, indem Sie z.B. in einem anderen Fenster/Konsole irgendetwas
tippen, die Maus verwenden oder irgendwelche anderen Programme benutzen.
Wir müssen eine ganze Menge Zufallswerte erzeugen. Sie können dies
unterstützen, indem Sie z.B. in einem anderen Fenster/Konsole irgendetwas
tippen, die Maus verwenden oder irgendwelche anderen Programme benutzen.
gpg: /root/.gnupg/trustdb.gpg: trust-db erzeugt
gpg: Schlüssel E022B975D0161CB4 ist als ultimativ vertrauenswürdig gekennzeichnet
gpg: Verzeichnis '/root/.gnupg/openpgp-revocs.d' erzeugt
gpg: Widerrufszertifikat wurde als '/root/.gnupg/openpgp-revocs.d/8AF0CCAA2E8F9FDDA9991918E022B975D0161CB4.rev' gespeichert.
Öffentlichen und geheimen Schlüssel erzeugt und signiert.

pub  rsa3072 2021-04-14 [SC] [verfällt: 2023-04-14]
     8AF0CCAA2E8F9FDDA9991918E022B975D0161CB4
uid                          Felix Schneider <f.schneider@htlkrems.at>
sub  rsa3072 2021-04-14 [E] [verfällt: 2023-04-14]

root@debian:~#

```



```
root@debian:/home/felix/Downloads# ls
private.key  secretmessage.txt.gpg
root@debian:/home/felix/Downloads# gpg --import private.key
gpg: Schlüssel 05171CCA339C085C: Öffentlicher Schlüssel "testuser" importiert
gpg: Schlüssel 05171CCA339C085C: geheimer Schlüssel importiert
gpg: Anzahl insgesamt bearbeiteter Schlüssel: 1
gpg:          importiert: 1
gpg:          gelesene geheime Schlüssel: 1
gpg:          geheime Schlüssel importiert: 1
root@debian:/home/felix/Downloads# gpg --list-secret-keys
/root/.gnupg/pubring.kbx
-----
sec   rsa3072 2021-04-14 [SC] [verfällt: 2023-04-14]
      8AF0CCAA2E8F9FDDA9991918E022B975D0161CB4
uid   [ ultimativ ] Felix Schneider <f.schneider@htlkrems.at>
ssb   rsa3072 2021-04-14 [E] [verfällt: 2023-04-14]

sec   rsa3072 2021-04-14 [SC] [verfällt: 2023-04-14]
      D9086AC894CB7AF8B0C8E19705171CCA339C085C
uid   [ unbekannt ] testuser
ssb   rsa3072 2021-04-14 [E] [verfällt: 2023-04-14]

root@debian:/home/felix/Downloads# gpg -r testuser --decrypt secretmessage.txt.gpg > clemenstext
gpg: verschlüsselt mit 3072-Bit RSA Schlüssel, ID 99F41C436C62C1C1, erzeugt 2021-04-14
      "testuser"
root@debian:/home/felix/Downloads# ls
clemenstext private.key secretmessage.txt.gpg
root@debian:/home/felix/Downloads# nano clemenstext
root@debian:/home/felix/Downloads# cat clemenstext
Moin meister!
root@debian:/home/felix/Downloads# █
```

Clemens Schlipfing hat die Datei erstellt, den Privat-Key erstellt und mir beides per E-Mail zukommen lassen.

Das habe ich dann heruntergeladen, importiert und encrypted.

Clemens geheime Botschaft lautet: Moin meister!

## 5 Ergebnisse

Verschlüsselung funktioniert.

## 6 Code

<http://www.online-tutorials.net/security/gnupg-gpg-tutorial/tutorials-t-69-124.html#einfhrung-in-a-href-wiki-gpgpg-a>

## 7 Kommentar

Die Anleitung war ausführlich.