Prof. Dr. Christian Schindelhauer
V. Goncharov, R. Borromeo, O. Jubran

Freiburg, 2010-01-13

Practical Exercises

Communication Systems (Rechnernetze II)

Topic No. 16 GnuPG

Exercise 1:
Gnu Privacy Guard (GnuPG or GPG) is a free encryption system, and used for data encrypting and signing. It uses a versatile key management system feature.
Note: Use the command *man gpg* to access GnuPG manual and get the commands.

1. Create with the *gpg* command a key pair (public and private key). It should be a DSA Key with a length of 1024 Bit for signing and crypting data. You can decide how long the key should be valid.

2. GNU Privacy Guard is widely used for signing emails. In this step, you should create a text file that you want to send to a friend of you, write some text in and sign the file with the private key you created before. Now suppose you are a recipient. Verify the signed file with your public key.

3. GPG might be also used for encrypting data. Export your public key to a file, exchange it with a neighbour. The neighbour should import the key. Now ask your neighbour for his/her public key and import it on your computer.

4. Encrypt the text file from the part 3 using your private key and the neighbour's public key, give it to the neighbour and ask him/her to decrypt the message.