Peter the Great St.Petersburg Polytechnic University

Department of Computer Systems & Software Engineering

Laboratory report №1

Discipline: «Information Security»

Theme: «Encryption and Signing with GPG, Gpg4win»

Made by student:

Boyarkin N.S.
Group: 13541/3

Lecturer:

Bogach N.V.

Saint-Petersburg
2017 y.

Contents

Laboratory work №1

1.1 Work purpose

Learn utilities, based on PGP technology, for encrypting and decrypting data.

1.2 Task

1. Study the description and launch graphic tool Kleopatra
2. Create a key pair with OpenPGP (File -> New Certificate)
3. Export Certificate (File -> Export Certificate)
4. Sign/Encrypt Files (File -> Sign/Encrypt Files)
5. Load other users certificates
6. Import a certificate, sign it
7. Verify the signature
8. Using your partner certificate encrypt, sign and send her a file
9. Accept, check and decrypt a file from your partner
10. Following the instructions in GNU Privacy handbook play with gpg by CLI,i.e. without graphic tool.

1.3 Work Progress

1.3.1 Introduction

Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

GnuPG is a hybrid-encryption software program because it uses a combination of conventional symmetric-key cryptography for speed, and public-key cryptography for ease of secure key exchange, typically by using the recipient's public key to encrypt a session key which is only used once. This mode of operation is part of the OpenPGP standard and has been part of PGP from its first version.

1.3.2 Kleopatra frontend

Creating a new certificate

Let's illustrate the stage of creating a new certificate (File -> New Certificate ...). The first stage is the choice standard for a key pair. In addition to OpenPGP, Kleopatra also supports X.509:

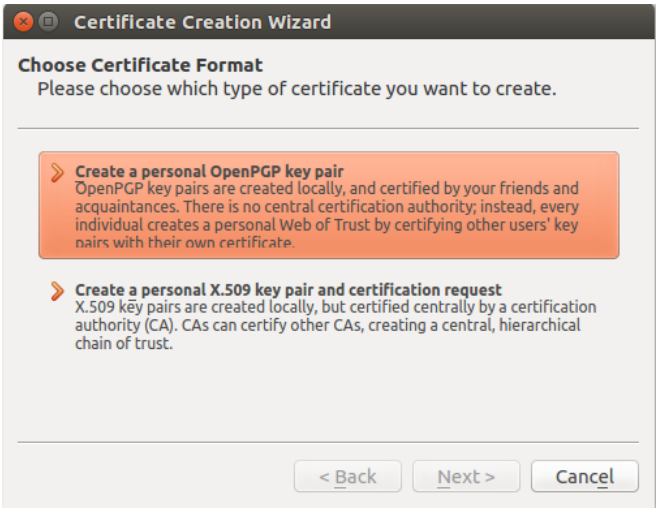

Рис. 1.1: Select a standard for the key pair

After that, the process of configuring the certificate (selection of the encryption algorithm, length key, certificate name, etc.):

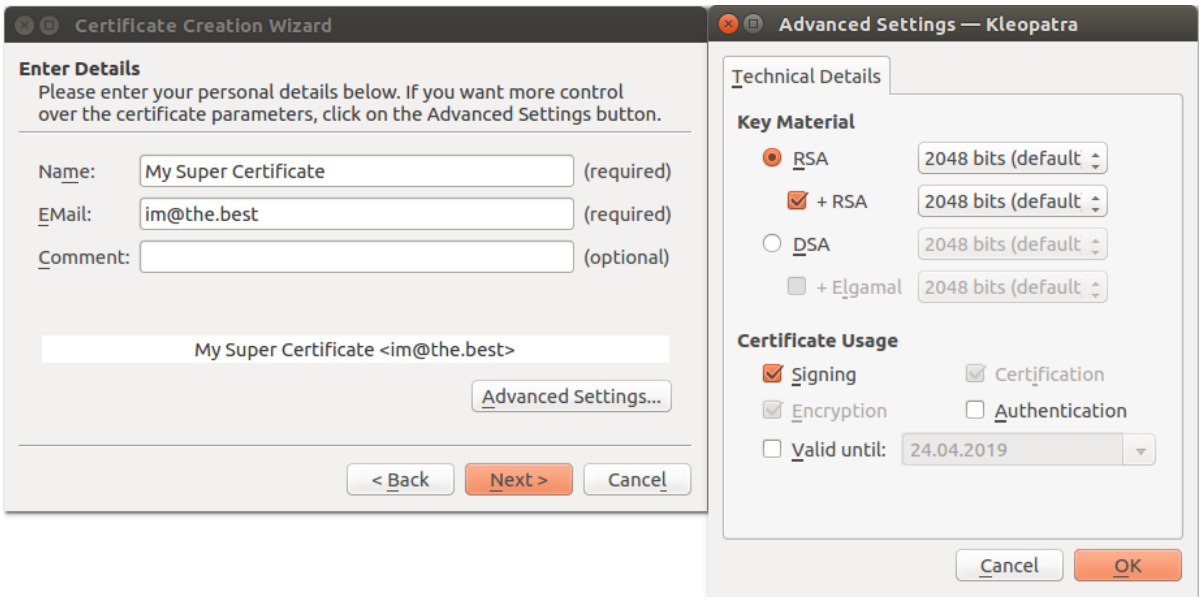

Рис. 1.2: Configure the certificate and select the encryption algorithm

Then, the process of generating a pair of keys (based on random characters and the movement of the window) occurs, and the password for accessing the private key is set:

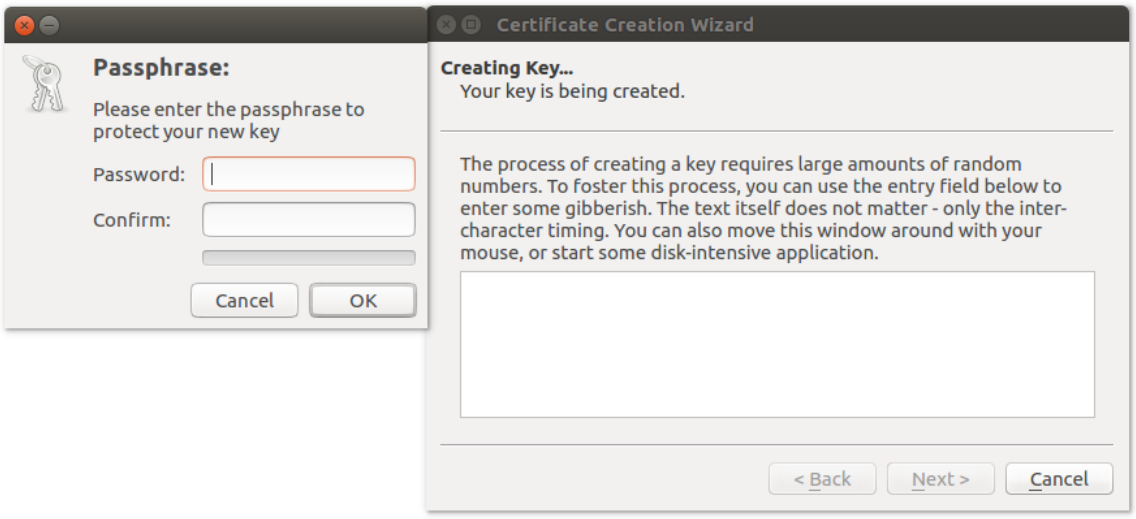

Рис. 1.3: The process of generating a key pair and setting a password for accessing a private key

The generated certificate appears in the list of certificates:

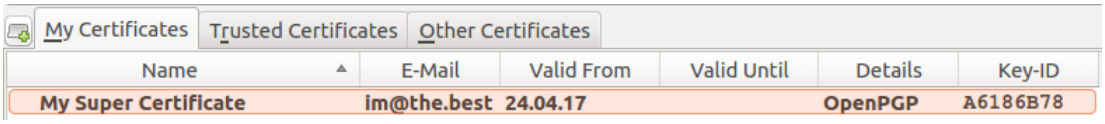

Рис. 1.4: The result of creating a certificate

To obtain a public key, use the command MRC -> Export Certificate... Open key is stored in a file with it's own extension:

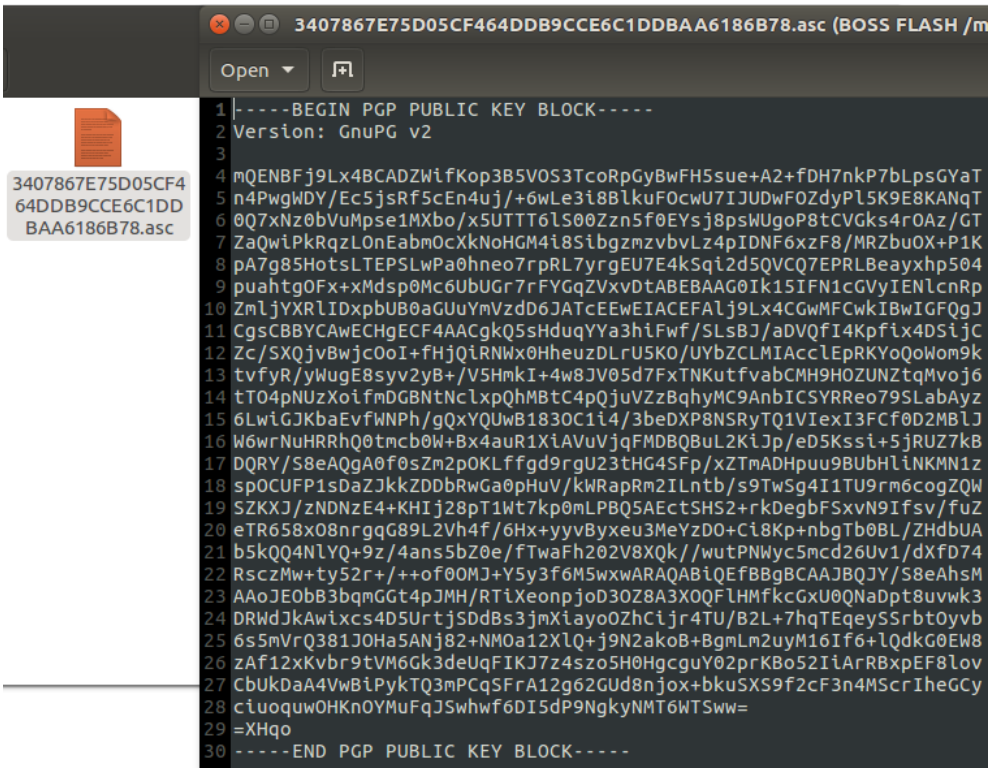

Рис. 1.5

Encrypting

On the **second** computer, we import a certificate (File -> Import Certificates ...), specifying as a parameter created public key:

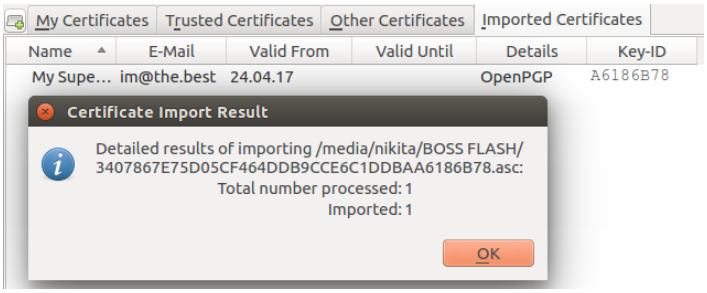

Рис. 1.6: The result of importing the certificate on the second computer

To encrypt files, the command File -> Sign / Encrypt files was used ... A window appears with the choice of encryption parameters:

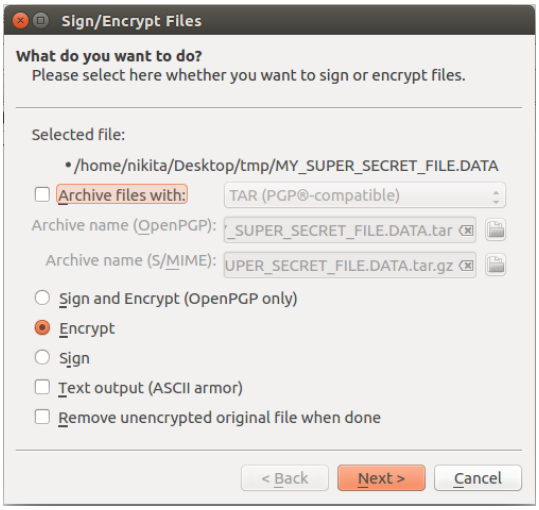

Рис. 1.7: Choosing encryption options

The following is the certificate for encrypting the file:

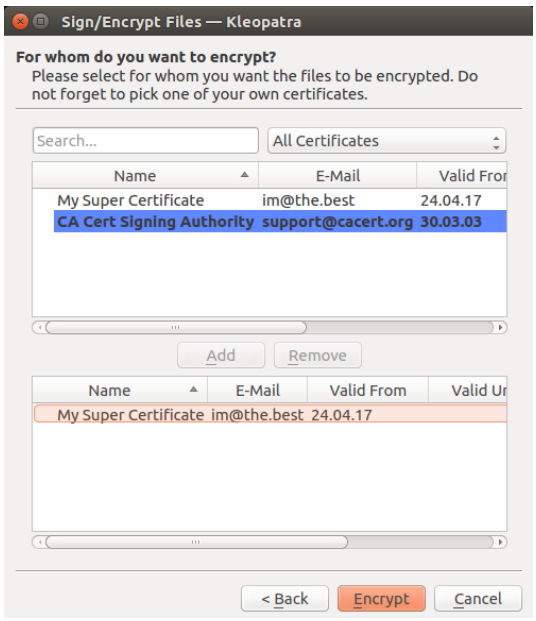

Рис. 1.8: Choosing a certificate for encryption

The result of file encryption:

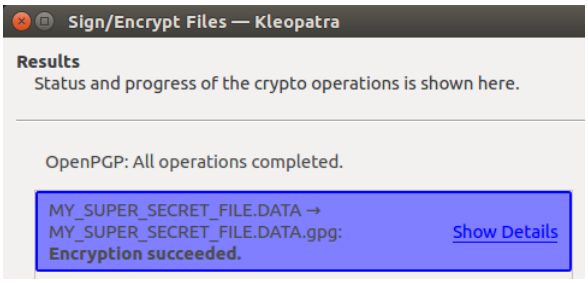

Рис. 1.9: The result of file encryption

The file was encrypted in .gpg format, the decryption of this file is possible only with a private key, so you can not decrypt it on this computer, even considering that we encrypted it.

Decrypting

Transfer the .gpg file created on the second computer to the **first** (on which the certificate was created). To decrypt the files, we use the command File -> Decrypt / Verify files ... A window appears with the decoding parameters:

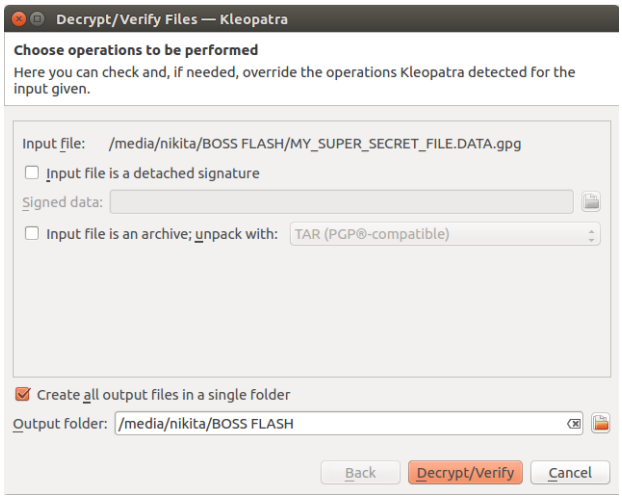

Рис. 1.10: Selecting decryption options

To access the decryption with a private key, you must enter the password that was created with the certificate:

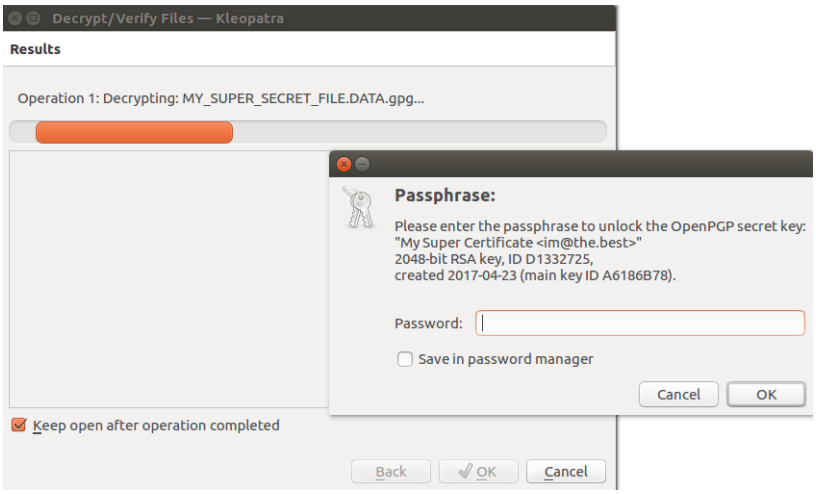

Рис. 1.11: Explanation by the private key

The result of decrypting the file:

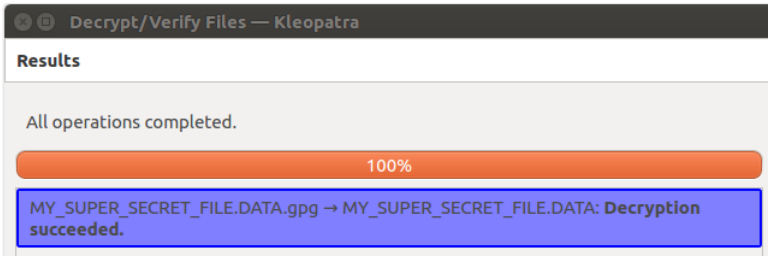

Рис. 1.12: The result of decrypting the file

The file was successfully decrypted: the name and contents of the file are the same as the original.

1.3.3 GPG command line

Symmetric-key encrypting

For symmetric encryption, the -c flag is used:

```
nikita@nikita-VirtualBox:~/temp$ ls
SECRET.DATA

nikita@nikita-VirtualBox:~/temp$ cat SECRET.DATA
! My secret data !

nikita@nikita-VirtualBox:~/temp$ gpg -c SECRET.DATA
gpg: keyring '/home/nikita/.gnupg/pubring.gpg' created

nikita@nikita-VirtualBox:~/temp$ ls
SECRET.DATA  SECRET.DATA.gpg

nikita@nikita-VirtualBox:~/temp$ cat SECRET.DATA.gpg
-> UNREADABLE SYMBOLS FOR LATEX <-
```

To decrypt a file, the combination of the -o and -d flags is used:

```
nikita@nikita-VirtualBox:~/temp$ ls
SECRET.DATA.gpg

nikita@nikita-VirtualBox:~/temp$ gpg -o SECRET.DATA -d SECRET.DATA.gpg
gpg: keyring '/home/nikita/.gnupg/secring.gpg' created
gpg: AES encrypted data
gpg: encrypted with 1 passphrase

nikita@nikita-VirtualBox:~/temp$ ls
SECRET.DATA  SECRET.DATA.gpg

nikita@nikita-VirtualBox:~/temp$ cat SECRET.DATA
! My secret data !
```

Public-key encrypting

At the first step we creating and export the certificate by the following commands:

```
nikita@nikita-VirtualBox:~/temp$ gpg --gen-key
gpg (GnuPG) 1.4.20; Copyright (C) 2015 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.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
```

```
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 2048
Requested keysize is 2048 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Donald
Email address: donald@trump.gov
Comment:
You selected this USER-ID:
    "Donald <donald@trump.gov>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
You need a Passphrase to protect your secret key.

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.

gpg: key 8A882796 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: public key of ultimately trusted key A6186B78 not found
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   2  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 2u
pub   2048R/8A882796 2017-11-05
      Key fingerprint = 0C4F 7BCD CA34 E401 77D8  07F4 EFB3 7A31 8A88 2796
uid                  Donald <donald@trump.gov>
sub   2048R/49ECD6F1 2017-11-05

nikita@nikita-VirtualBox:~/temp$ gpg --list-keys
/home/nikita/.gnupg/pubring.gpg
------------------------------
pub   2048R/8A882796 2017-11-05
uid                  Donald <donald@trump.gov>
sub   2048R/49ECD6F1 2017-11-05

nikita@nikita-VirtualBox:~/temp$ gpg --armor --export Donald
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQENBFn+gHEBCADR+ghOmcJeiDZk6TscxuurxEJBSFD7mPgaQHnPxxaj7iz9Z7am
HGxBe6pNDPbzhkRrZH7eSRC3bu94351X5kKwz39h94tCp9BbLA36VZ4j2y448Wfl
gWDrrT++cnE2xs/qcNOMB0wqd0iyPLyhcK7WP+0ZXmqoTFTZe3hY3xE6XhAYoAEB
d1j49j+K55PinZtOJa+hF8HQxig/CBRgDYeixG57fWdxU3XcNvm1OJwEpaUjHmcw
780pGTq2fAx9BEz5Dsmj0vPAWS5BfF5OMMA9CtTtHtK9ZNce5IIwdds6oahFgPWA
a0UpadDnOyLNHKRleEaTqQgFEGoWOggqL/tZABEBAAG0GURvbmFsZCA8ZG9uYWxk
QHRydW1wLmdvdj6JATgEEwECACIFAln+gHECGwMGCwkIBwMCBhUIAgkKCwQWAgMB
Ah4BAheAAAoJEO+zejGKiCeW2hUH/RNa19AKEJyHD7RQaK7B0OnzEFKUzRyje/Gi
FTn/4qhR0al0m3P8kz7m4GLVTnXhBLcxfjFa+N2LdijISe9WebeF6wG+WMGPoLL6
e98okr24aZ0i2YEgocoSHM/ySz7TBXx/yVZR8vIzjHKiqjnRn9dCrVIF/jW/rYnL
CinxUwAzb22Bz17Zt56VVJnEIGMKGcaHCMUsqxthC3Qe7h15Lt92ozIrhEQoyic5
LzzY9BYVKOyBPU4C02+wcUMsTZuaadQhcQYE3kkvhtWQBpCI8HExmIuYKokv1czX
```

```
CGMEM4PRGnmkdKEQFwb0ZAXo55PRhKEcoVLA7ccewEIBSGTRSAC5AQ0EWf6AcQEI
AKWbeRA3RN3LVkUtU79CxVtFIAMvrUJ9zZFHzQuEEefeswC4bXmWHmhlAlVTJEGS
NG1XDciIMN0qoIBvzZPMX5F4OAJg452u3T4zaaQ5R3OEm541e7b8/P/T1+iRmu3c
hCEomLqySGkzGJTcd6s6xgUFrb1XYv9xUgBZ7sKbQDRtwDCpclYhjhOmOWjLQmor
lnBP9O7btJOwcO/FaU7OXqmFYtyH4eF4vQph95gdw3YFHYTcf1iuZQVFu6trjDP+
4SuXmrhtkmftKfhLPFPy/TkHTJ1H5B6ZdPLTZkL4c8lIM7byKA86tjLlKixybEvH
fJUWPFfO/LWPxX4kV4YippkAEQEAAYkBHwQYAQIACQUCWf6AcQIbDAAKCRDvs3ox
iognlpsDB/9ooll0kv1Vu/SHk+kPZXsi452G4duGN3h1v3yndvxmhvv+lKObZm3B
uctxa7CoMXHZ14X1pd/yiurZfkxV3OSo6USzKXou8kuLGJ6O+qAPSkKCYgEWdUyM
Iwhh1gD0fJ4Dr2lZG/sJ5lvqyBKsm+0t3bdTuFJHiCGF7bYI6rfl1UYgumT9VIFX
S7ucTeUebk+P1KF5j5IRFbxZFAlrYQVrxMv5JKCuzqSM2NF+yIKrNs5e1Emd8G3Q
o5Phwy+RW6bg3rAuDViCqjYyhzjL4GqNBUfJS1r2D3YbrVLO3djB78ytWnj+v2d5
11u7VGYZbEafG58WsRrhWDoye7rTV/7d
=WxVr
-----END PGP PUBLIC KEY BLOCK-----
```

Encrypting file on the second machine by the public key:

```
nikita@nikita-pc:~/temp$ ls
key

nikita@nikita-pc:~/temp$ gpg --import key
gpg: key 8A882796: public key "Donald <donald@trump.gov>" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)

nikita@nikita-pc:~/temp$ gpg --list-keys
/home/nikita/.gnupg/pubring.gpg
--------------------------------
pub   2048R/A6186B78 2017-04-23
uid                  My Super Certificate <im@the.best>
sub   2048R/D1332725 2017-04-23

pub   2048R/8A882796 2017-11-05
uid                  Donald <donald@trump.gov>
sub   2048R/49ECD6F1 2017-11-05

nikita@nikita-pc:~/temp$ echo "! My secret file !" > SECRET.DATA

nikita@nikita-pc:~/temp$ gpg -o SECRET.DATA.gpg -e -r Donald SECRET.DATA
gpg: 49ECD6F1: There is no assurance this key belongs to the named user

pub  2048R/49ECD6F1 2017-11-05 Donald <donald@trump.gov>
 Primary key fingerprint: 0C4F 7BCD CA34 E401 77D8  07F4 EFB3 7A31 8A88 2796
      Subkey fingerprint: D128 458C A1B6 EBCF 340C  752F 98ED 17FB 49EC D6F1

It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y

nikita@nikita-pc:~/temp$ cat SECRET.DATA.gpg
-> UNREADABLE SYMBOLS FOR LATEX <-
```

The result of decrypting the file on the first machine:

```
nikita@nikita-VirtualBox:~/temp$ ls
SECRET.DATA.gpg

nikita@nikita-VirtualBox:~/temp$ gpg -o SECRET.DATA -d SECRET.DATA.gpg

You need a passphrase to unlock the secret key for
user: "Donald <donald@trump.gov>"
2048-bit RSA key, ID 49ECD6F1, created 2017-11-05 (main key ID 8A882796)

gpg: encrypted with 2048-bit RSA key, ID 49ECD6F1, created 2017-11-05
```

```
11          "Donald <donald@trump.gov>"
12
13 nikita@nikita-VirtualBox:~/temp$ ls
14 SECRET.DATA  SECRET.DATA.gpg
15
16 nikita@nikita-VirtualBox:~/temp$ cat SECRET.DATA
17 ! My secret file !
```

1.4 Conclusion

In this paper, we examined asymmetric encryption using the Kleopatra program of the OpenPGP family. Asymmetric encryption has the advantage over symmetric in the ease of exchange keys, but loses in encryption speed. The encryption considered in this work is one-way. In order to carry out two-way transmission, two channels are used. In modern cryptosystems, asymmetric encryption is used for key exchange, and at the same time symmetric encryption for data exchange.