

Bezpieczeństwo sieci komputerowych

Sprawozdanie z laboratorium

Data	Tytuł zajęć	Uczestnicy
26.10.2018 09:15	Kryptografia	Igor Bejnarowicz (218573) Bartosz Rodzewicz (226105)

Przebieg laboratorium

2. Generacja 3 par kluczy

Oboje wygenerowaliśmy trzy pary kluczy:

Command Prompt

```
GnuPG needs to construct a user ID to identify your key.

Real name: bartek3
Email address: bartek.modrzejewski95@wp.pl
Comment:
You selected this USER-ID:
"bartek3 <bartek.modrzejewski95@wp.pl>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
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
harddisks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
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 AEB4393FC093C6C3 marked as ultimately trusted
gpg: revocation certificate stored as 'C:/Users/barto/AppData/Roaming/gnupg/openpgp-revocs.d/4393FC093C6C3.rev'
public and secret key created and signed.

pub  rsa2048 2018-11-09 [SC] [expires: 2031-08-15]
      B8C7F2942C12D11BE0473FFD0A84393FC093C6C3
uid          bartek3 <bartek.modrzejewski95@wp.pl>
sub  rsa2048 2018-11-09 [E] [expires: 2031-08-15]
```

Key Pair Creation Wizard

Key Pair Successfully Created

Your new key pair was created successfully. Please find details on the result and some suggested next steps below.

Result

Key pair created successfully.
Fingerprint: 9E4DB8A1772803EA45A6F77719FF00DCEB26E88

Next Steps

Make a Backup Of Your Key Pair...

Send Public Key By Email...

Upload Public Key To Directory Service...

Finish

Cancel

Kleopatra

File View Certificates Tools Settings Window Help

Sign/Encrypt... Decrypt/Verify... Import... Export... Certify... Lookup on Server... Notepad

Search... <Alt+Q>

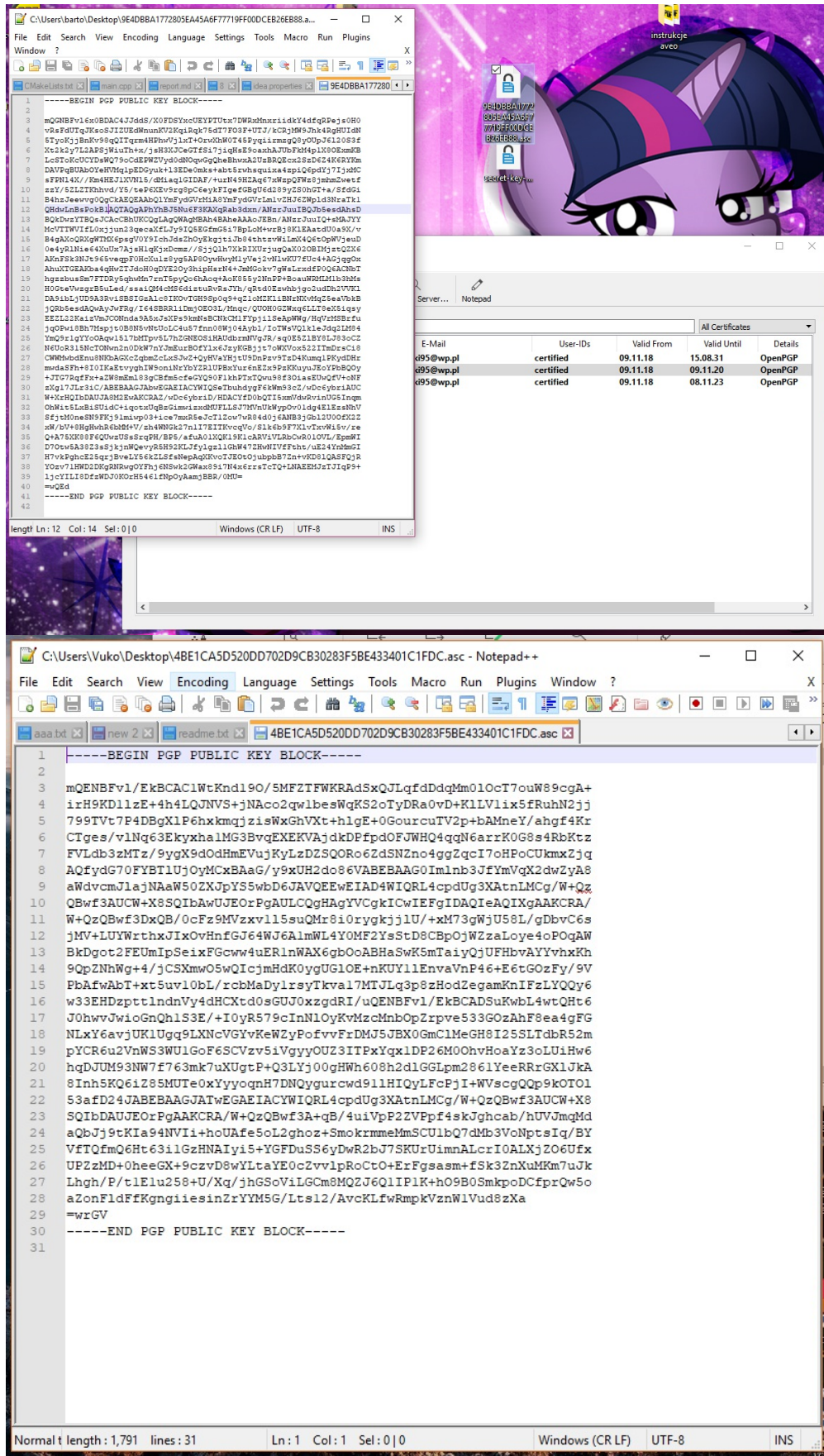
All Certificates

Name	E-Mail	User-IDs	Valid From	Valid Until	Details
igor_bej_kleo	igorbej3@interia.pl	certified	09/11/2018	09/11/2021	OpenPGP
igor_bej_gpg	igorbej3@interia.pl	certified	09/11/2018	07/11/2027	OpenPGP
igor_bej	igorbej3@interia.pl	certified	09/11/2018	07/11/2024	OpenPGP

3. Klucze publiczne

Wyeksportowaliśmy klucze do plików tekstowych. Odciski kluczy są następujące:

Osoba	Odcisk
Igor	4BE1CA5D520DD702D9CB30283F5BE433401C1FDC
Bartosz	9E4DBBA1772805EA45A6F77719FF00DCEB26EB88



```
-----BEGIN PGP PUBLIC KEY BLOCK-----

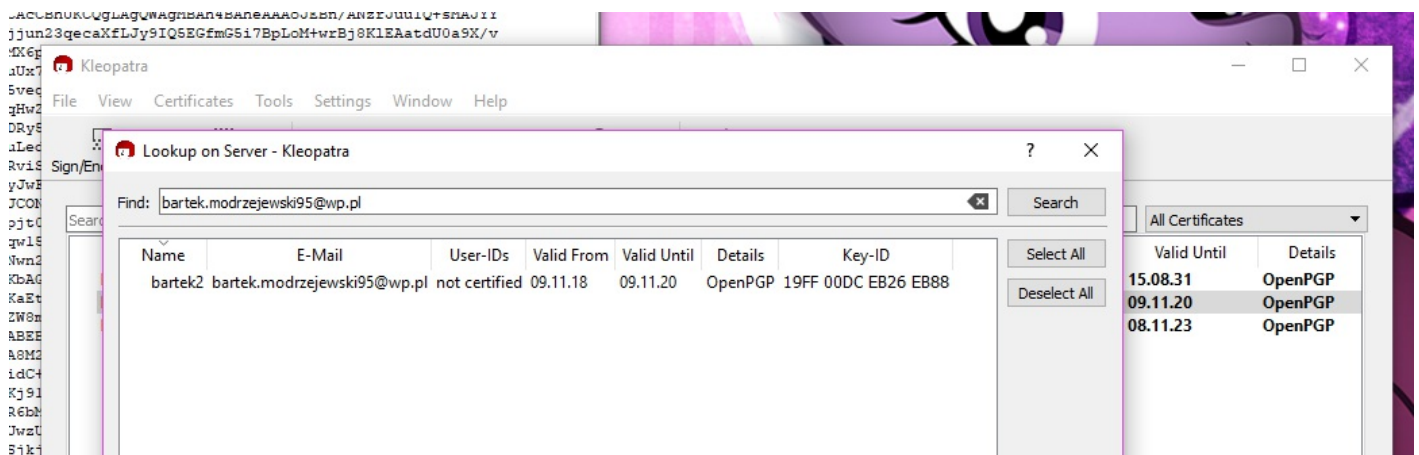
mQENBFv1eKBCAC1wtKnd190/5MFZTFWKRAdSxQJLqfDdggMm01OcT7ouW89cgA+
iZrKXD11ze+4h4LQJNV5+jNAco2qwlbesWqKS2oTyDRA0vD+K1L1vix5fRuhN2jj
799TVt7P4DBgK1P6hXkmqjz1sWxGhVXt+h1gE+0GourcuTV2p+bAMneY/ahgf4Kr
CTges/v1Nq63EkYxha1MG3BvqEXEKVAjkdDPdpOFJWHQ4qqN6arrK0G8s4RbKtz
FVLdb3zMTz/9ygyX9dOdHmEvujKyLzDZ5QORo6ZdSNZno4ggZqcI7oHPoCukmxZjQ
AQfydG7OYFBT1UjOyMxcBAAG/y9xUH2do86VABEBAAQImlnb3JfYmVqX2dwZyA8
aWdvcmlja1JNAaW50ZXJpYS5wbD6JAVQEeEiAD4WIQRL4cpdUg3XatnLMCg/W+Qz
QBwf3AUCW+X8SQIbAwUJEORpGAULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRAl
W+QzQBwf3DxBQ/0cFz9MVzxv115suQMr8i0rygkjj1U/+xm73gWjU58L/gDbvC6s
jMV+LUYWrthxJIxOvHnfGJ64WJ6A1mWL4YOMF2YsStD8CBpOjWZaLoye4oPOqAW
BkdGoc2FEUmiPSeixFGcw4uERlnWAXE6gb0oABHaSwK5mTaiyQjUfHbvAYYvXhKh
9QpZNhWg+4/jCSXmW05QIcjmHdK0yguUG10E+nKUY11EnvaVnP46+E6tGozF/9V
PbAfwAbT+xt5uv10bL/rcbMaDylrsyTkval7MTJLq3p8zHodZegamKnIFzLYQYy6
w33EHDzptclndnVy4dHCXtd0sGUJ0xgzdRI/uENBFv1/EkBCADSuKwbL4wtQht6
J0hwjWjwoGnQh1S3E/+IOYr579cInN1OyKvMzcMnbOpZrpve533GozAhF8ea4gFG
NLXy6avjUK1Ugg9LXNcVGyVkeWZyPofvFvFDMJ5JBX0GmC1MeGH8I25SLTdbR52m
pYCR6u2VnWS3WU1GoF6SCVzv5iVggyOUZ3ITPxyqX1DP26M0OhvHoaYz3oLUIHw6
hgDJUM93NW7f763mkUxUgtP+Q3LYj00gHw608h2d1GGLpm2861YeeRRrGX1JkA
8Inh5KQ6i285MUTE0xYyyoqnH7DNQygurcwD911HIQyLfcPjI+WVscgQQp9koTO1
23aFD24ABEBAAQJATvEAGeIACYWIQRL4cpdUg3XatnLMCg/W+QzQBwf3AUCW+X8
SQIbDAUJEOzPgAAKCRAlW+QzQBwf3A+qB/4uiVpP2ZVPpf4skJghcab/hUVJmgMd
aQbJ9j9Kia94NVIi+hoUafe5oL2ghoz+SmokrmmeMmSCULbQ7dMb3VoNptsIq/BY
VTQfEmQ6Ht6311GzHNAIyi5+YGFduSSyGdwR2bJ7SKURUimnALcrIOALXjZ06Ufx
UP2ZMD+0heeGX+9czvD8wYltaYE0cZvvpLroCto+ErFgsasm+f5k3ZnXmKfm7uJk
Lhgh/P/t1Elu258+U/Xq/jhGSoViLGCm8MQZJ6Q1IP1K+h09B05mkp0DCfprQw5o
aZonFldFfKnggiesinZrYMY5G/Lts12/AvcKLfwRmpkVznW1Vud8zXa
=wrGV
-----END PGP PUBLIC KEY BLOCK-----
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBFv1/EkBCAC1wtKnd190/5MFZTFWKRAdSxQJLqfDdggMm01OcT7ouW89cgA+
iZrKXD11ze+4h4LQJNV5+jNAco2qwlbesWqKS2oTyDRA0vD+K1L1vix5fRuhN2jj
799TVt7P4DBgK1P6hXkmqjz1sWxGhVXt+h1gE+0GourcuTV2p+bAMneY/ahgf4Kr
CTges/v1Nq63EkYxha1MG3BvqEXEKVAjkdDPdpOFJWHQ4qqN6arrK0G8s4RbKtz
FVLdb3zMTz/9ygyX9dOdHmEvujKyLzDZ5QORo6ZdSNZno4ggZqcI7oHPoCukmxZjQ
AQfydG7OYFBT1UjOyMxcBAAG/y9xUH2do86VABEBAAQImlnb3JfYmVqX2dwZyA8
aWdvcmlja1JNAaW50ZXJpYS5wbD6JAVQEeEiAD4WIQRL4cpdUg3XatnLMCg/W+Qz
QBwf3AUCW+X8SQIbAwUJEORpGAULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRAl
W+QzQBwf3DxBQ/0cFz9MVzxv115suQMr8i0rygkjj1U/+xm73gWjU58L/gDbvC6s
jMV+LUYWrthxJIxOvHnfGJ64WJ6A1mWL4YOMF2YsStD8CBpOjWZaLoye4oPOqAW
BkdGoc2FEUmiPSeixFGcw4uERlnWAXE6gb0oABHaSwK5mTaiyQjUfHbvAYYvXhKh
9QpZNhWg+4/jCSXmW05QIcjmHdK0yguUG10E+nKUY11EnvaVnP46+E6tGozF/9V
PbAfwAbT+xt5uv10bL/rcbMaDylrsyTkval7MTJLq3p8zHodZegamKnIFzLYQYy6
w33EHDzptclndnVy4dHCXtd0sGUJ0xgzdRI/uENBFv1/EkBCADSuKwbL4wtQht6
J0hwjWjwoGnQh1S3E/+IOYr579cInN1OyKvMzcMnbOpZrpve533GozAhF8ea4gFG
NLXy6avjUK1Ugg9LXNcVGyVkeWZyPofvFvFDMJ5JBX0GmC1MeGH8I25SLTdbR52m
pYCR6u2VnWS3WU1GoF6SCVzv5iVggyOUZ3ITPxyqX1DP26M0OhvHoaYz3oLUIHw6
hgDJUM93NW7f763mkUxUgtP+Q3LYj00gHw608h2d1GGLpm2861YeeRRrGX1JkA
8Inh5KQ6i285MUTE0xYyyoqnH7DNQygurcwD911HIQyLfcPjI+WVscgQQp9koTO1
23aFD24ABEBAAQJATvEAGeIACYWIQRL4cpdUg3XatnLMCg/W+QzQBwf3AUCW+X8
SQIbDAUJEOzPgAAKCRAlW+QzQBwf3A+qB/4uiVpP2ZVPpf4skJghcab/hUVJmgMd
aQbJ9j9Kia94NVIi+hoUafe5oL2ghoz+SmokrmmeMmSCULbQ7dMb3VoNptsIq/BY
VTQfEmQ6Ht6311GzHNAIyi5+YGFduSSyGdwR2bJ7SKURUimnALcrIOALXjZ06Ufx
UP2ZMD+0heeGX+9czvD8wYltaYE0cZvvpLroCto+ErFgsasm+f5k3ZnXmKfm7uJk
Lhgh/P/t1Elu258+U/Xq/jhGSoViLGCm8MQZJ6Q1IP1K+h09B05mkp0DCfprQw5o
aZonFldFfKnggiesinZrYMY5G/Lts12/AvcKLfwRmpkVznW1Vud8zXa
=wrGV
-----END PGP PUBLIC KEY BLOCK-----
```

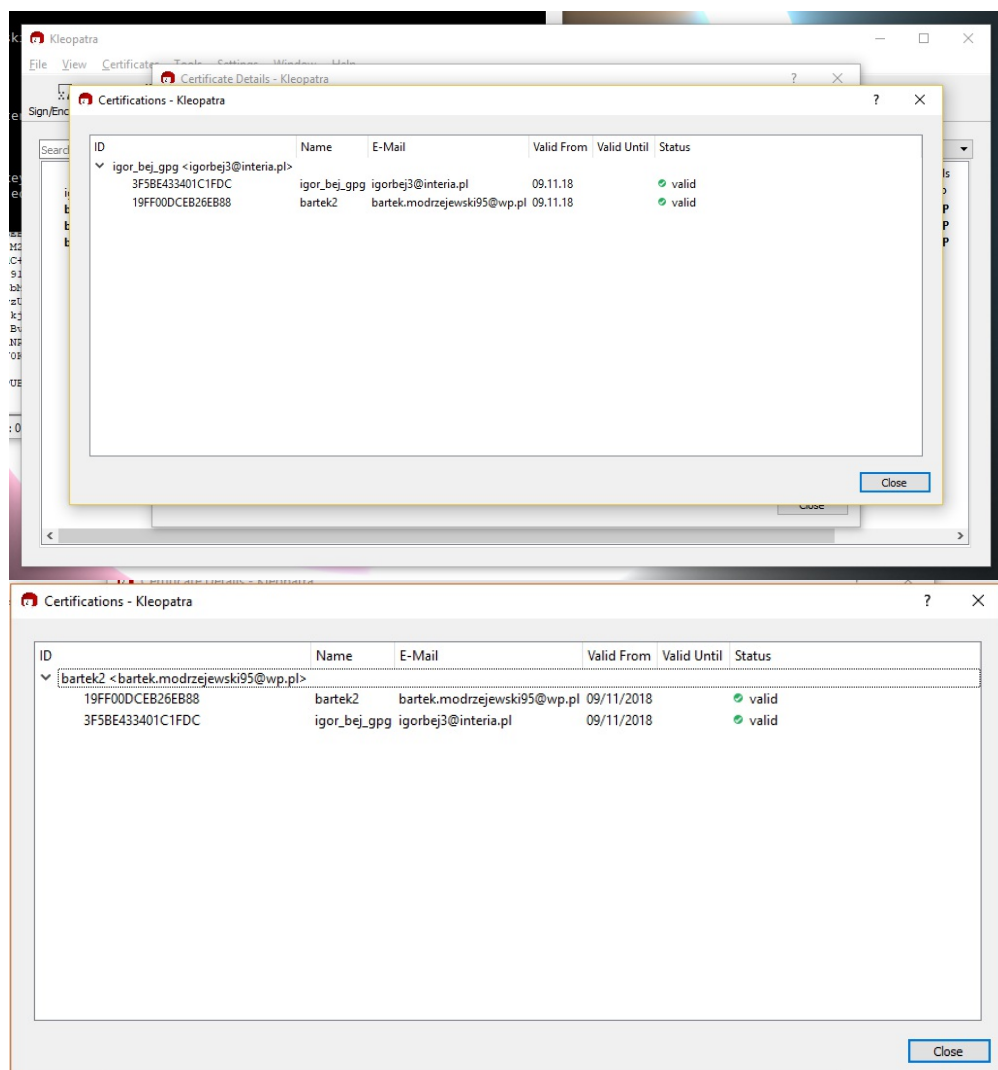
4. Serwer kluczy

Oboje wysłaliśmy nasze klucze na serwer kluczy `pgp.mit.edu`.



5. Wzajemne podpisanie kluczy

Poprzez serwer kluczy wymieniliśmy się naszymi kluczami i wzajemnie je sobie podpisaliśmy.

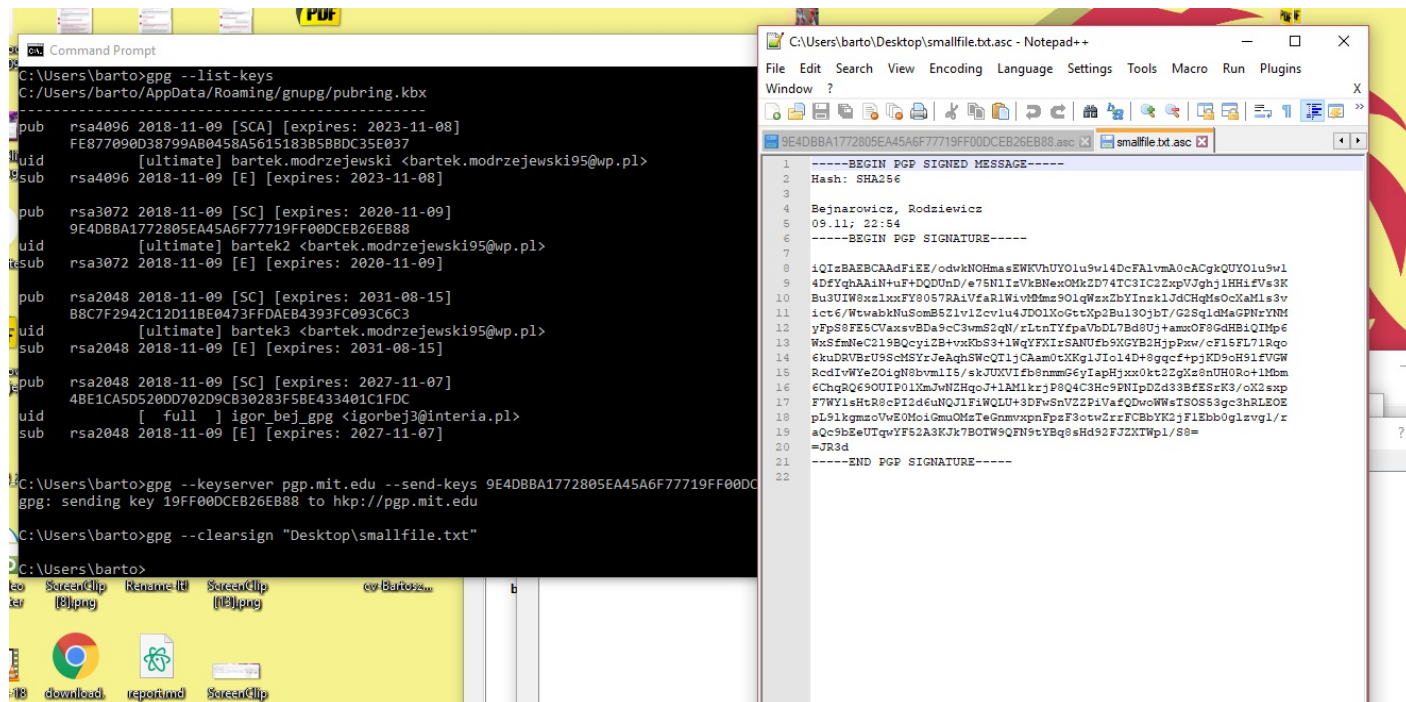


6. Podpisanie małego pliku

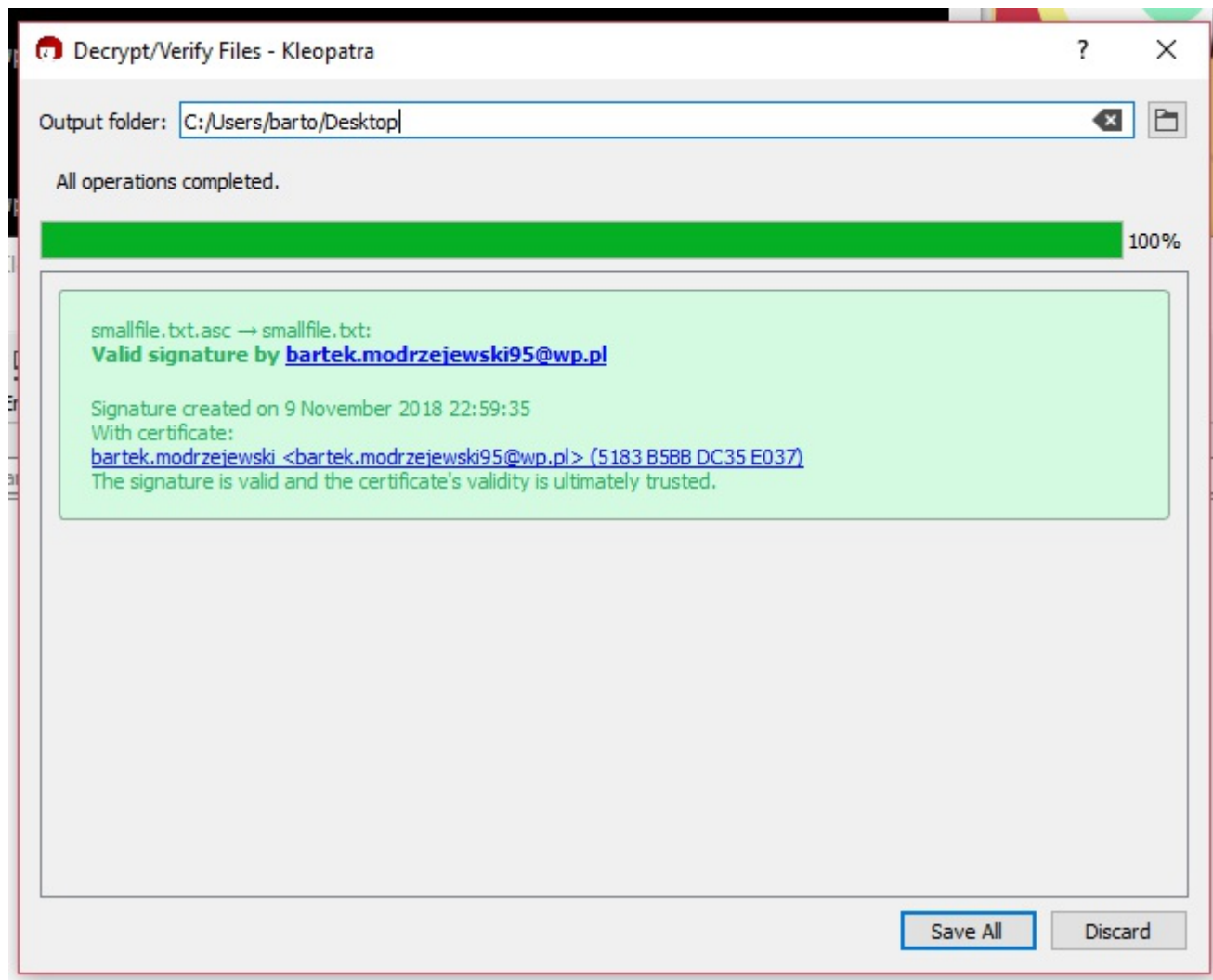
Utworzyliśmy plik o nazwie `smallfile.txt` o treści:

```
Bejnarowicz, Rodziewicz  
09.11; 22:54
```

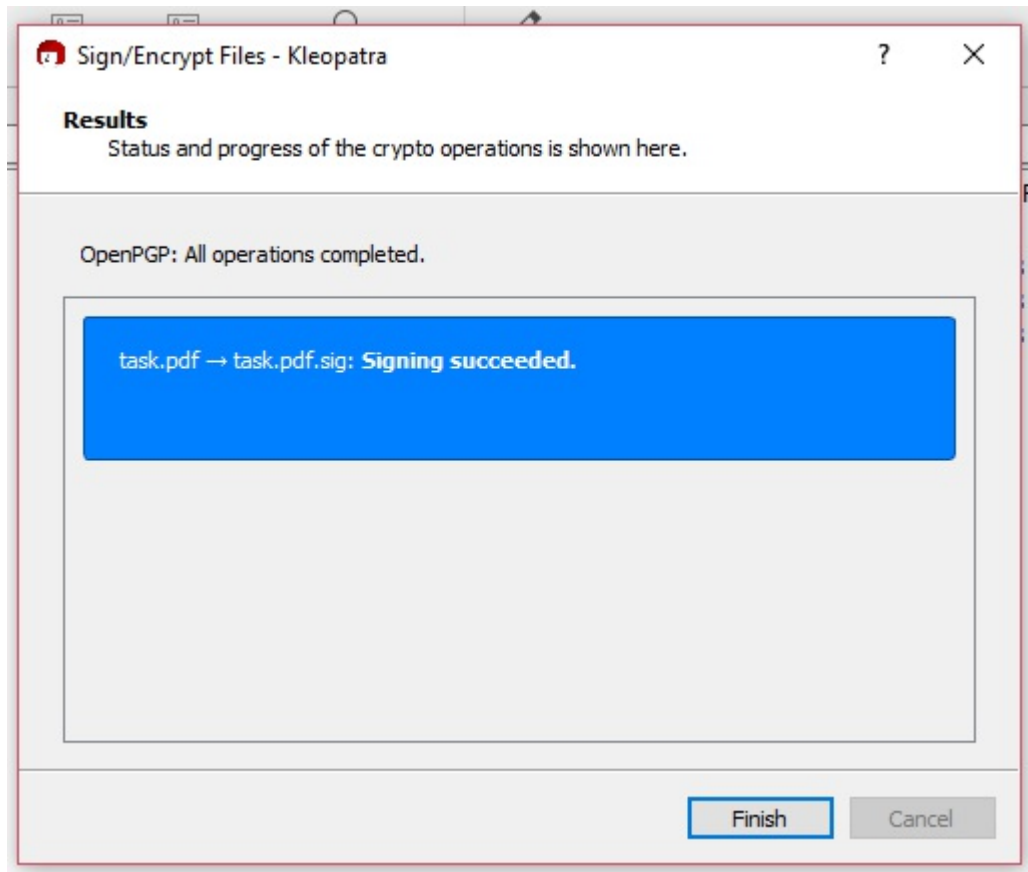

Został on podpisany z poziomu konsoli:



i sprawdzona jego poprawność z poziomu Kleopatry:



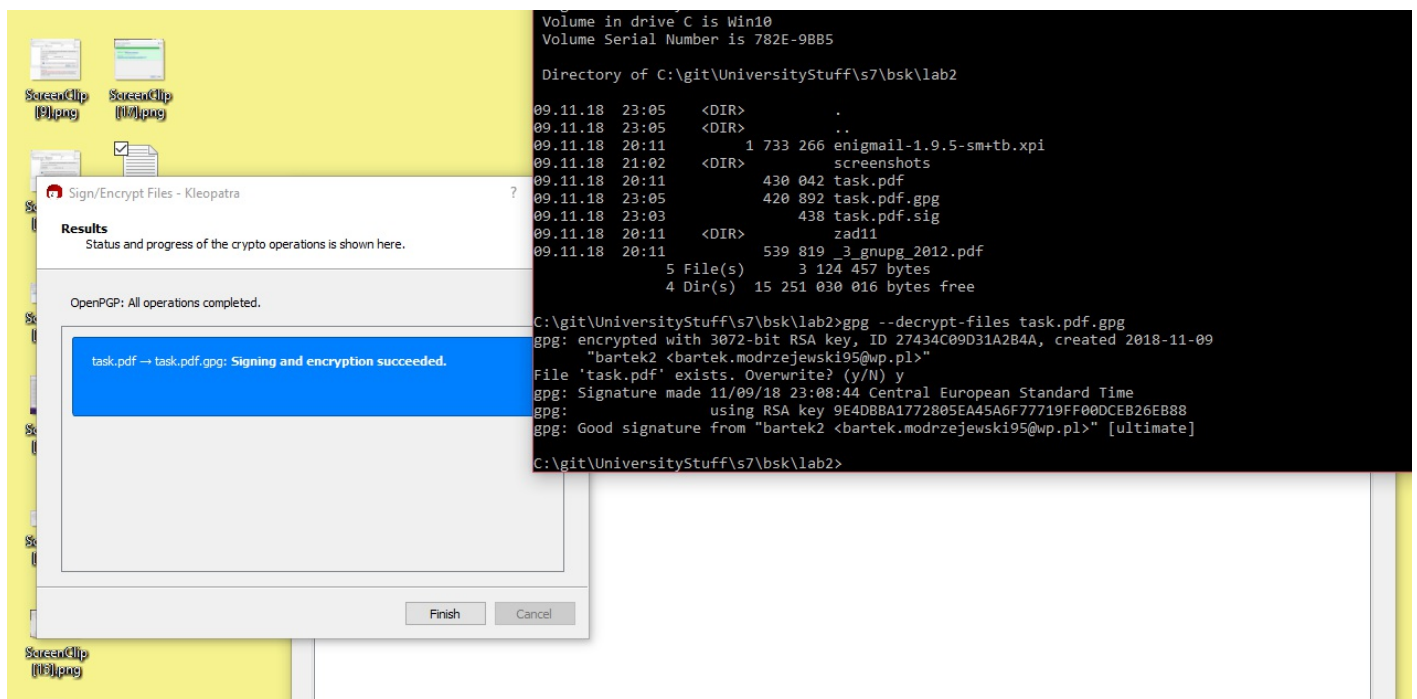
7. Podpisanie pliku binarnego



8. Zasyfrowanie pliku z Kleopatry, odszyfrowanie z konsoli

Użyta komenda:

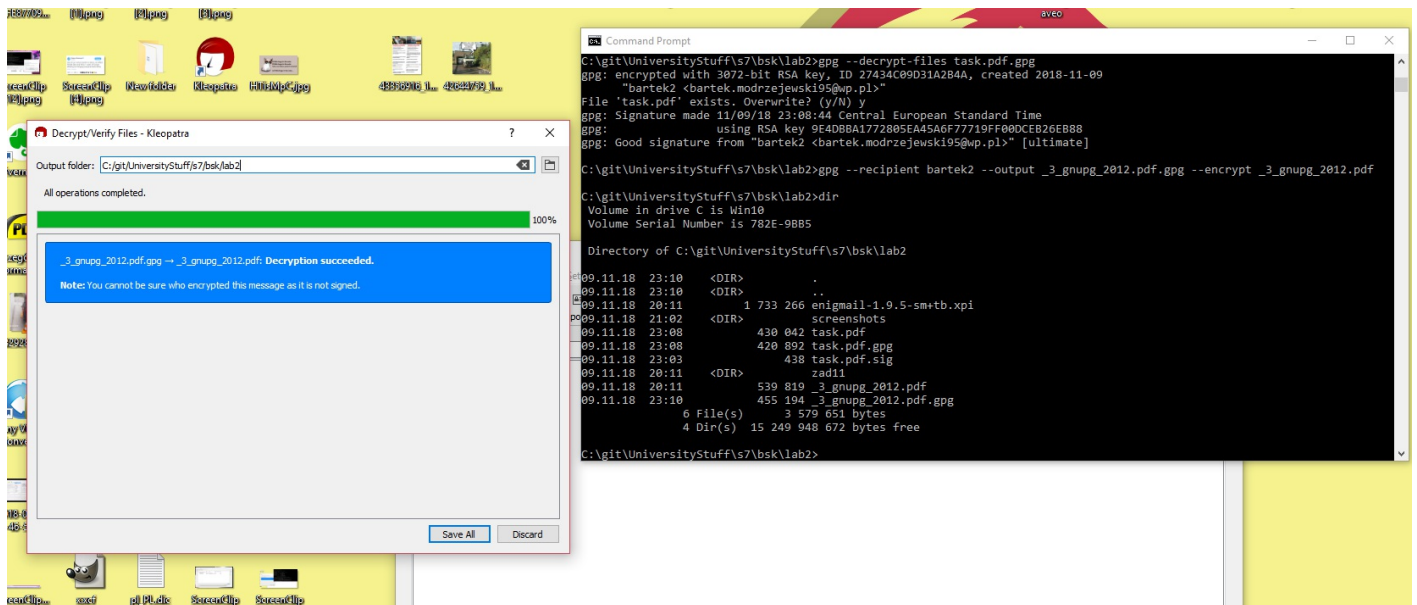
```
gpg --decrypt-files task.pdf.gpg
```



9. Zaszzyfrowanie pliku z konsoli, odszyfrowanie z Kleopatry

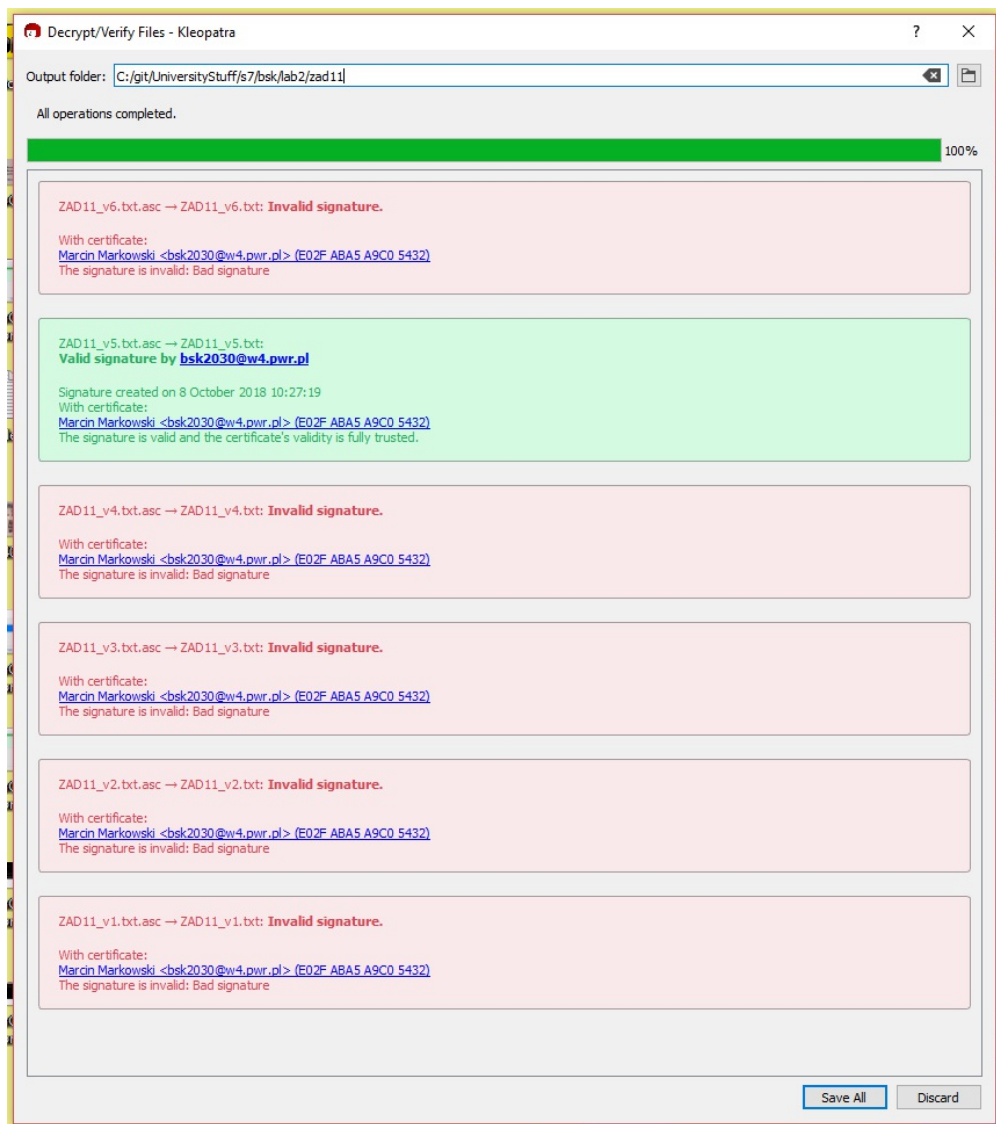
Użyta komenda:

```
gpg --recipient bartek2 --output _3_gnupg_2012.pdf.gpg --encrypt _3_gnupg_2012.pdf
```



11. Ukryte zadanie

Poprawnym zadaniem było zadanie nr 5.



Jego treść to:

Zapisać do pliku tekstowego imiona członków grupy.
Plik zaszyfrować za pomocą gpg algorytmem AES192 (tylko symetrycznym) z kluczem 'LABORKA'.
Obliczyć sumę kontrolną SHA-1 pliku (Kleopatra).
Komendy gpg, treść pliku przed i po zaszyfrowaniu oraz sumę kontrolną umieścić w sprawozdaniu.

Stworzony został plik o nazwie `imiona.txt`, z treścią `Igor Bartosz`.

Plik został zaszyfrowany komendą:

```
gpg --recipient "Marcin Markowski" --cipher-algo aes192 --encrypt imiona.txt
```

Nie zrozumieliśmy co znaczy, że mamy użyć klucza `LABORKA`.

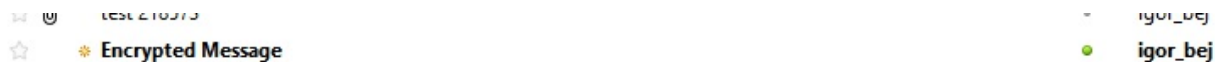
Po zaszyfrowaniu treść pliku to:

```
...|~ô|«-μ)HQ&e/sp
'ä@*ÜÊÜDBE>öp5'x1»cëoëu\F?H."RpZ
üñux@së%`ø¥éjT-.cAð0p`ÖöÖâ!is"ûφÜ    Î]G.."GäæVÄ~ñžàEööàib`)èö5% è""%¶}b·<Í{`Žox|ÎdμDbYÓiûφ)+²Ãð~"Q
`ð3    Öâ&...£ 1μAb"B]    @¶S¶{"`$ÈR£)+Ê; ,Î9iG"JVürμ#`ð...3, `óÚ!"W^«²EBeði«^IZöâ|¿Ê1â@â>ÖQÀ^Üðw=|!ÿ~e\Ä¼Kh,âea/šp6®+«:U,ÊjT\(\,0E"S
óó{HA-DU²}Ä¼6d`p\o,,U>G<0ä
```

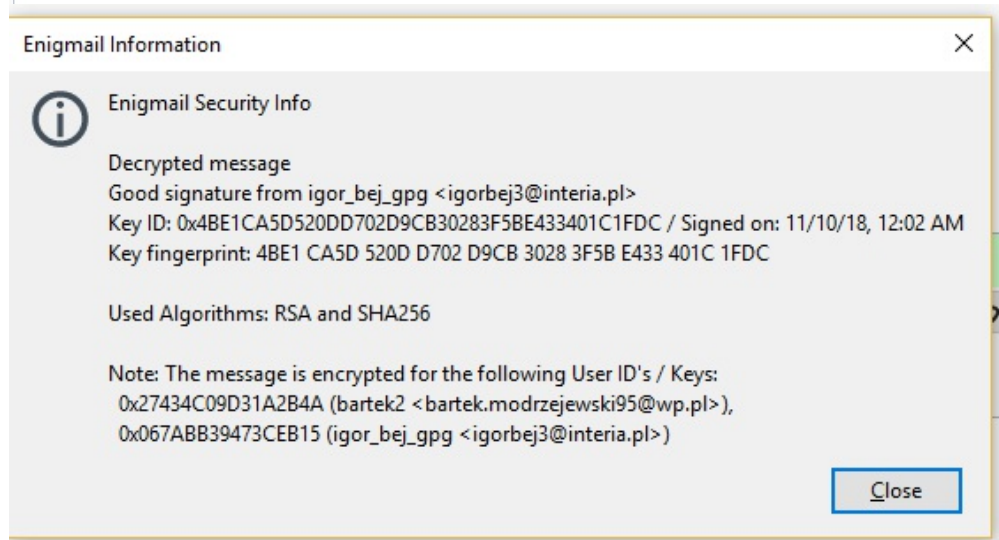
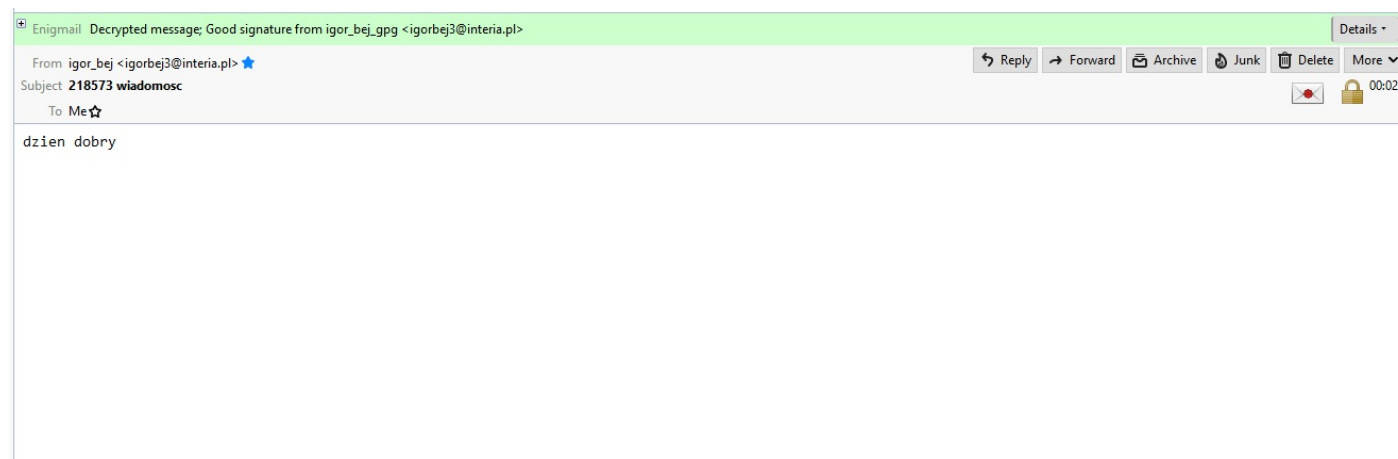
Suma kontrolna SHA-1: `55f24a0a2ae41f1d68085396f3eb3070`.

12. Zaszyfrowane maile

Przesłaliśmy sobie wzajemnie maile. Aby zachowana była zgodność kluczy potrzebna była zmiana domyślnego klucza w Thunderbirdzie. Przed odszyfrowaniem mail wygląda następująco:



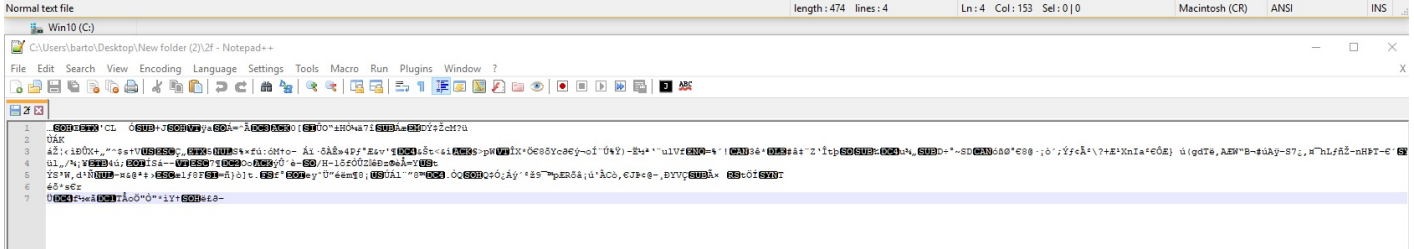
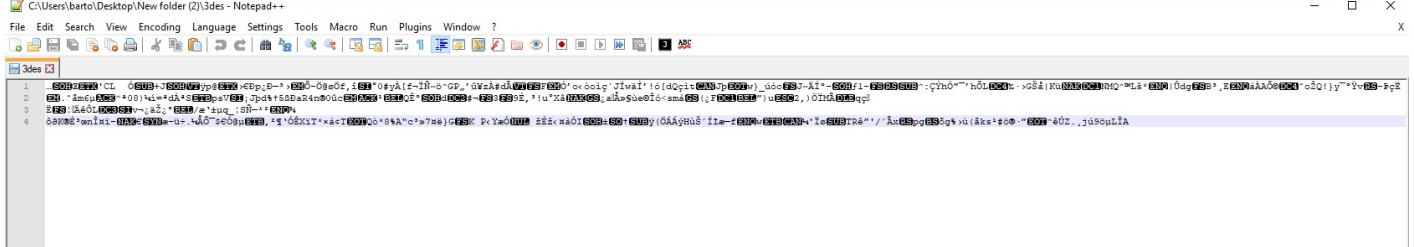
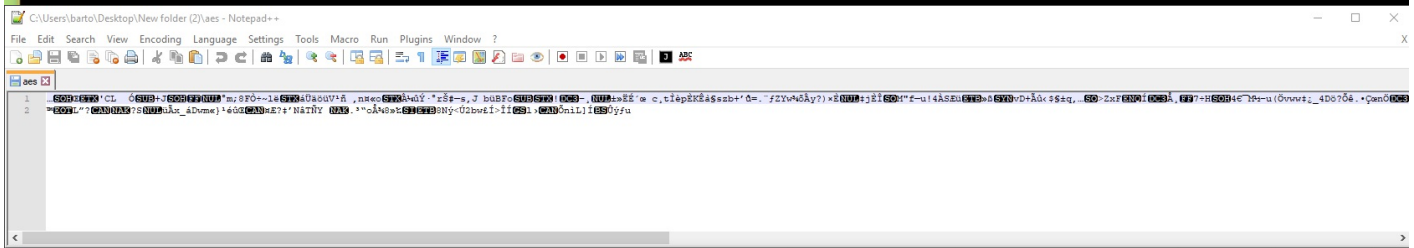
Po odszyfrowaniu wyświetla się wiadomość, że mail jest zaufany:



13. Porównanie szyfrowania

Domyślnym algorytmem szyfrowania jest **AES-128** (w **pgp** od wersji 2.1). Poniżej znajduje się porównanie plików zaszyfrowanych **AES-192**, **3DES** i **TWOFISH**.

```
c:\Users\barto\Desktop>pgpg --recipient "Marcin Markowski" --cipher-algo aes192 --encrypt imiona.txt
c:\Users\barto\Desktop>pgpg --recipient bartek2 --cipher-algo aes192 --encrypt imiona.txt
File 'imiona.txt.gpg' exists. Overwrite? (y/N) y
c:\Users\barto\Desktop>pgpg --recipient "Marcin Markowski" --cipher-algo aes192 --encrypt imiona.txt
File 'imiona.txt.gpg' exists. Overwrite? (y/N) y
c:\Users\barto\Desktop>pgpg --recipient bartek22 --cipher-algo aes192 --output aes --encrypt imiona.txt
pgpg: bartek22: skipped: No public key
pgpg: imiona.txt: encryption failed: No public key
c:\Users\barto\Desktop>pgpg --recipient bartek2 --cipher-algo aes192 --output aes --encrypt imiona.txt
c:\Users\barto\Desktop>pgpg --recipient bartek2 --cipher-algo 3des --output 3des --encrypt imiona.txt
c:\Users\barto\Desktop>pgpg --recipient bartek2 --cipher-algo twofish --output 2f --encrypt imiona.txt
pgpg: WARNING: forcing symmetric cipher TWOFISH (10) violates recipient preferences
c:\Users\barto\Desktop>
```



Name	Ext	Size	Date	Attr
2f		482	10.11.2018 00:05	-a--
3des		474	10.11.2018 00:05	-a--
aes		482	10.11.2018 00:05	-a--