# Email Security with GPG

Fabrizio Demaria
900402-T417
demaria@kth.se

November 20, 2014

## 1 Getting started

- What is the fingerprint of the Course Key?

  8797 01BB 2B8B 2F7B 19E3 4F5B 1404 71E6 0745 00FE

- How long time did it take generate the keys?

  It took less than two seconds.

- Which cipher did you choose?

  The *RSA and RSA* option was selected.

- How do you motivate the choice?

  Since the requirements for this Lab include encryption operations, the choice was limited to *RSA and RSA* or *DSA and Elgamal*. Both would have been correct, so the first option was chosen since marked as *default*. [2]

- Which key-length did you choose?

  2048 bits

- How do you motivate the choice?

  For long-term security level, 2048 bits is recommended by the organizations cited on *http://www.keylength.com*

- The identity you created for the key

  ```
  uid       [ultimate] Fabrizio Demaria (IK2206) <demaria@kth.se>
  ```

- The fingerprint of the key

  A09C 2A3A 019E 062E 76E1 DCAF 6C31 9AFF 120D 23DE

## 2 Signed data

| Message | Analysis |
|---|---|
| 1 | It is a PGP PUBLIC KEY BLOCK without any message |
| 2 | The message does not include any signature |
| 3 | Signature for the message **is verified** using the public key of the course |
| 4 | Signature for the message **is verified** using the public key of the course |
| 5 | Bad signature detected. Message may have been signed with an incorrect private key or it may have been modified |
| 6 | Bad signature detected. Message may have been signed with an incorrect private key or it may have been modified |
| 7 | Signature for the message **is verified** using the public key of the course |
| 8 | The message does not include any signature |

Table 1: Signed messages mail (*Step 8*).

- Which key do you use to sign the reply?

  My reply was signed adopting my private key

- Output from GnuPG illustrating each type of incorrect message (for the possible causes please refer to the table above):

  Output for message 1:

  ```
  gpg: verify signatures failed: Unexpected error
  ```

  Output for messages 2 and 8 (output in Italian language, translation below):

  ```
  gpg: Non sono stati trovati dati OpenPGP validi.
  gpg: non è stato possibile verificare la firma.
  ```

  *gpg: No valid OpenPGP data found.*
  *gpg: the signature could be verified [1]*

  Output for messages 5 and 6:

  ```
  gpg: Signature made Gio 13 Nov 19:02:07 2014 CET using RSA key
       ID 074500FE
  gpg: BAD signature from "Internet Security and Privacy (IK2206)
       <gpg@netsec.xen.ssvl.kth.se>" [ultimate]
  ```

# 3 Encrypted data

| Message | Analysis |
|---|---|
| 1 | It is a PGP PUBLIC KEY BLOCK without any message |
| 2 | The message can't be decrypted because the receiving system is missing the private key |
| 3 | The message can't be decrypted because the receiving system is missing the private key of the course |
| 4 | The message has a good signature but it is not encrypted |
| 5 | The message can be **correctly decrypted** since it was previously encrypted using the public key of the receiving system |
| 6 | The message can't be decrypted because the receiving system is missing the private key of the course |
| 7 | The message is neither encrypted nor signed |
| 8 | The message has a bad signature and it is not encrypted. The signature has been probably generated from a private key that is not the private key of the course |
| 9 | The message has a good signature but it is not encrypted |
| 10 | The message can be **correctly decrypted** since it was previously encrypted using my public key (in this case it was also encrypted with the course public key) |
| 11 | The message can't be decrypted because the receiving system is missing the private key |

Table 2: Encrypted messages mail (*Step 9*).

- Which key do you use to secure the reply?

  My reply was secured adopting my public key and the public key of the course

- Output from GnuPG illustrating each type of incorrect message (for the possible causes please refer to the table above):

  Output for message 1:

  ```
  gpg: decrypt_message failed: Unexpected error
  ```

  Output for messages 2 and 11:

  ```
  gpg: encrypted with RSA key, ID 130E924D
  gpg: decrypt_message failed: No secret key
  ```

  Output for messages 3 and 6:

  ```
  gpg: encrypted with 2048-bit RSA key, ID 7C13DE15, created
       2014-11-11
        "Internet Security and Privacy (IK2206) <gpg@netsec.
        xen.ssvl.kth.se>"
  gpg: decrypt_message failed: No secret key
  ```

Output for messages 4 and 9:

```
gpg: Signature made Gio 13 Nov 19:02:07 2014 CET using RSA
     key ID 074500FE
gpg: Good signature from "Internet Security and Privacy (I
     K2206) <gpg@netsec.xen.ssvl.kth.se>" [ultimate]
```

Output for message 8:

```
gpg: Signature made Gio 13 Nov 19:02:07 2014 CET using RSA
     key ID 074500FE
gpg: BAD signature from "Internet Security and Privacy (IK
     2206) <gpg@netsec.xen.ssvl.kth.se>" [ultimate]
```

Output for message 7 (first line of the output in Italian language, translation below):

```
gpg: Non sono stati trovati dati OpenPGP validi.
gpg: decrypt_message failed: Unknown system error
```

*gpg: No valid OpenPGP data found. [1]*

# 4 Signed and encrypted data

| Message | Analysis |
|---|---|
| 1 | It is a PGP PUBLIC KEY BLOCK without any message |
| 2 | The message is **correctly** encrypted with the receiving system's public key and signed with the private key of the course |
| 3 | The message is **correctly** encrypted with the receiving system's public key and signed with the private key of the course |
| 4 | The message is encrypted with the public key of the course and the receiving system cannot decrypt it |
| 5 | The message has been **correctly** encrypted with both the public key of the course and the public key of the receiver. Moreover, it is correctly signed by the course. |
| 6 | The message is not encrypted and the attached signature from the course is BAD indicating that an incorrect private key has been used for generating the signature (or the message has been modified before reaching destination) |
| 7 | The signature is verified but the message is not encrypted |
| 8 | Encryption is possible with the key of the receiving system but it is not possible to verify the sender (message not signed) |
| 9 | The message is neither encrypted nor signed |
| 10 | The message is encrypted with the public key of the course and the receiving system cannot decrypt it |
| 11 | The message is encrypted with the receiving system's public key and with an unknown key. It is also signed with the private key of the course |
| 12 | The message is encrypted with the public key of the course and the receiving system cannot decrypt it |
| 13 | The message is encrypted with the receiving system's public key and with an unknown key. It is also signed with the private key of the course |
| 14 | The message is **correctly** encrypted with the receiving system's public key and signed with the private key of the course |
| 15 | The signature is verified but the message is not encrypted |

Table 3: Signed and encrypted messages mail (*Step 10*).

- Which key do you use to secure the reply?

  My reply was signed adopting my private key and encrypted using both my public key and the public key of the course

- Output from GnuPG illustrating each type of incorrect message (for the possible causes please refer to the table above):

  Output for message 1:

  ```
  gpg: verify signatures failed: Unexpected error
  ```

  Output for messages 4, 10 and 12:

```
gpg: encrypted with 2048-bit RSA key, ID 7C13DE15, created
     2014-11-11
      "Internet Security and Privacy (IK2206) <gpg@netsec.
       xen.ssvl.kth.se>"
gpg: decrypt_message failed: No secret key
```

Output for message 6:

```
gpg: Signature made Gio 13 Nov 19:02:08 2014 CET using RSA
     key ID 074500FE
gpg: BAD signature from "Internet Security and Privacy (IK
     2206) <gpg@netsec.xen.ssvl.kth.se>" [ultimate]
```

Output for messages 7 and 15 (this is not an error message but the encryption is missing):

```
gpg: Signature made Gio 13 Nov 19:02:08 2014 CET using RSA
     key ID 074500FE
gpg: Good signature from "Internet Security and Privacy (IK
     2206) <gpg@netsec.xen.ssvl.kth.se>" [ultimate]
```

Output for message 8 (this is not an error message but the signature is missing):

```
gpg: encrypted with 2048-bit RSA key, ID F56B5554, created
     2014-11-13
      "Fabrizio Demaria (IK2206) <fabriziodenny@gmail.com>"
```

Output for message 9 (first line of the output in Italian language, translation below):

```
gpg: Non sono stati trovati dati OpenPGP validi.
gpg: decrypt_message failed: Unknown system error
```

*gpg: No valid OpenPGP data found. [1]*

Output for message 11 (this is not an error message but the message has been also signed with an unknown key):

```
gpg: encrypted with RSA key, ID 130E924D
gpg: encrypted with 2048-bit RSA key, ID F56B5554, created
     2014-11-13
      "Fabrizio Demaria (IK2206) <fabriziodenny@gmail.com>"
```

# 5 Feedback

- References

  [1] Despite the fact that I set my OpenGPG in English, some parts of the outputs are still displayed in Italian. Samia Khalid, who is also attending the course, helped me in translating since her OpenGPG was entirely in English.

  [2] *http : //fedoraproject.org/wiki/Creating_GPG_Keys*

- Suggested improvements to the lab system

  No suggestions

- Suggested improvements to the lab instructions

  No suggestions

- Time estimation

  About 15 hours