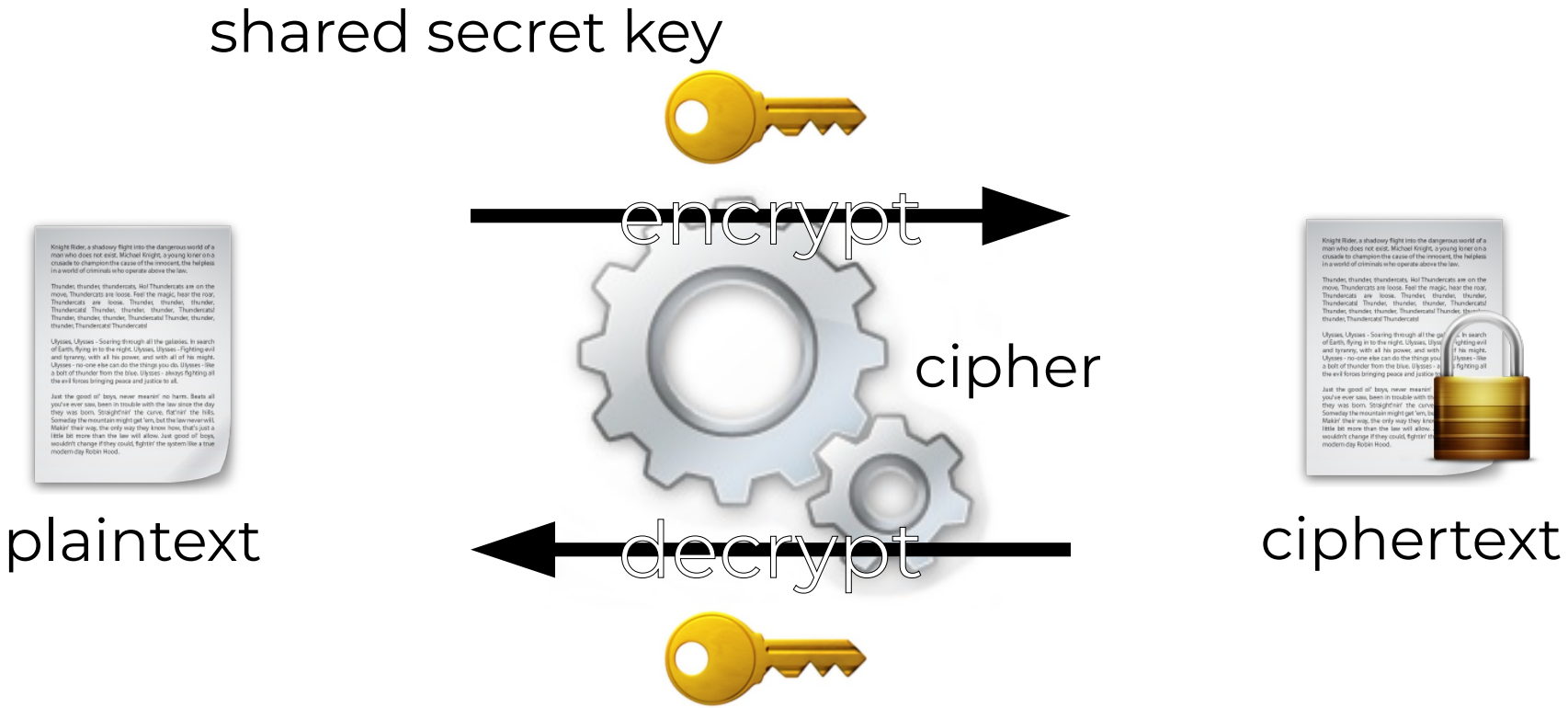
Public Key Cryptography, OpenPGP, and Enigmail

Cryptography is the art and science of transforming (encrypting) a message so only the intended recipient can read it

Symmetric Cryptography



Symmetric Cryptography

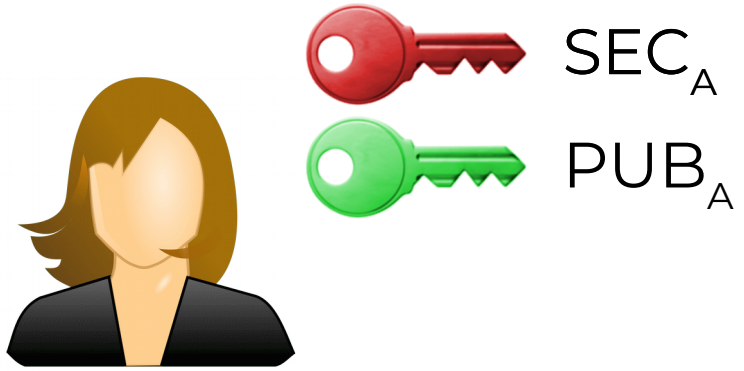
Examples of **symmetric ciphers**:

- Caesar (I cent. BCE)
- substitution (IV cent.)
- Vigenère (XVI cent.)
- Beaufort (XIX cent.)
- DES (1975)
- 3DES (1998)
- AES (1998)
- etc.

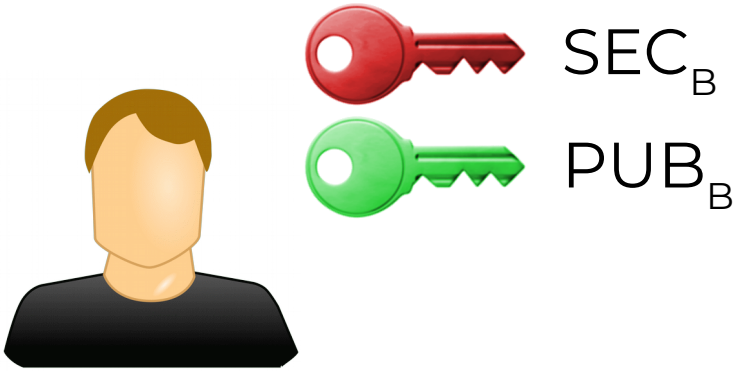
Symmetric Cryptography

Problem: deliver the key to the recipient!

Public Key Cryptography
(Asymmetric Cryptography)



Alice

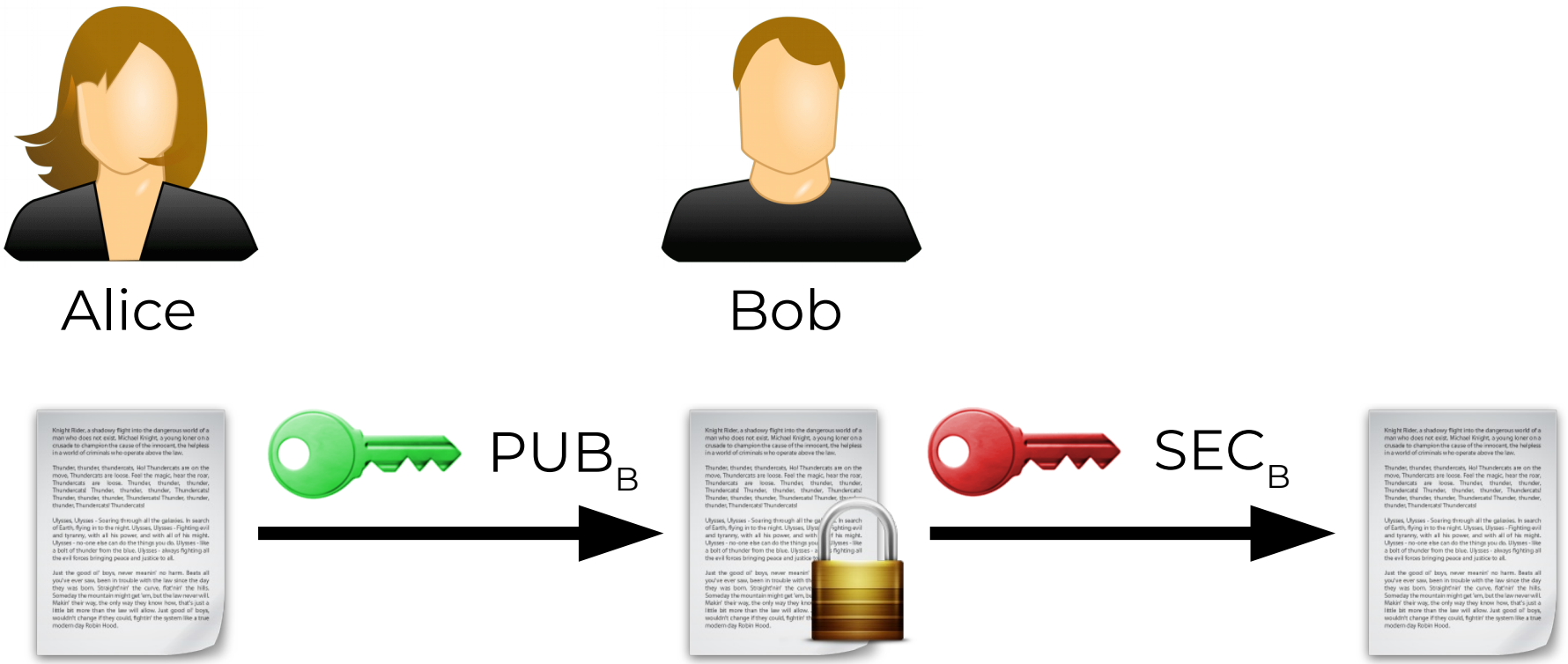


Bob

First, each participant generates a **key pair** composed of a **private key** and a **public key**

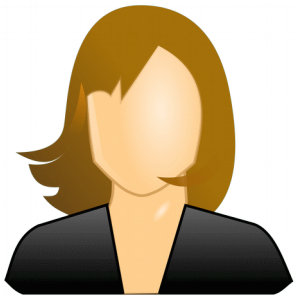
Public Key Cryptography

Encryption/Decryption
(for confidentiality)

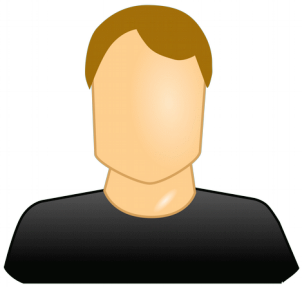


Public Key Cryptography

Digital signature
(for authentication & integrity)



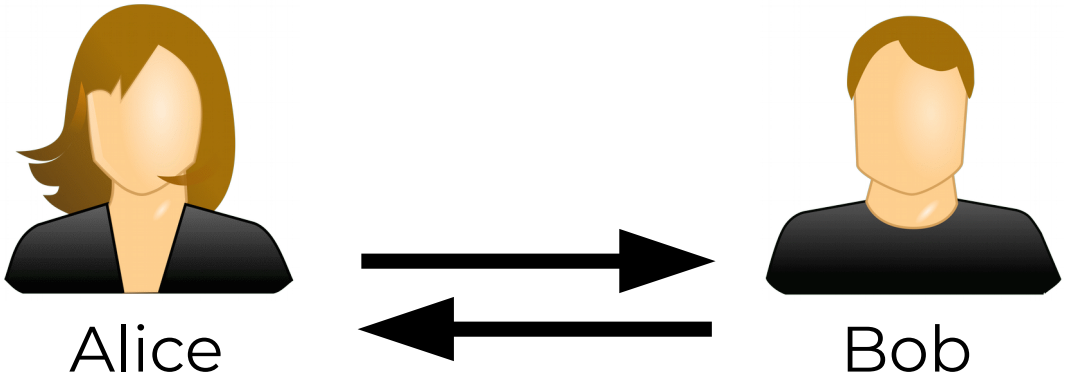
Alice



Bob

Public Key Cryptography

PKC is based on **one-way functions**



DH-RSA:

- discrete logarithm problem

  e.g. $453^{x} \pmod{21997} = 5787$ x = **?**

- prime factorization

  e.g. prime factors of 7774733 = **?**

Public Key Cryptography

Birth of **Public Key Cryptography**:

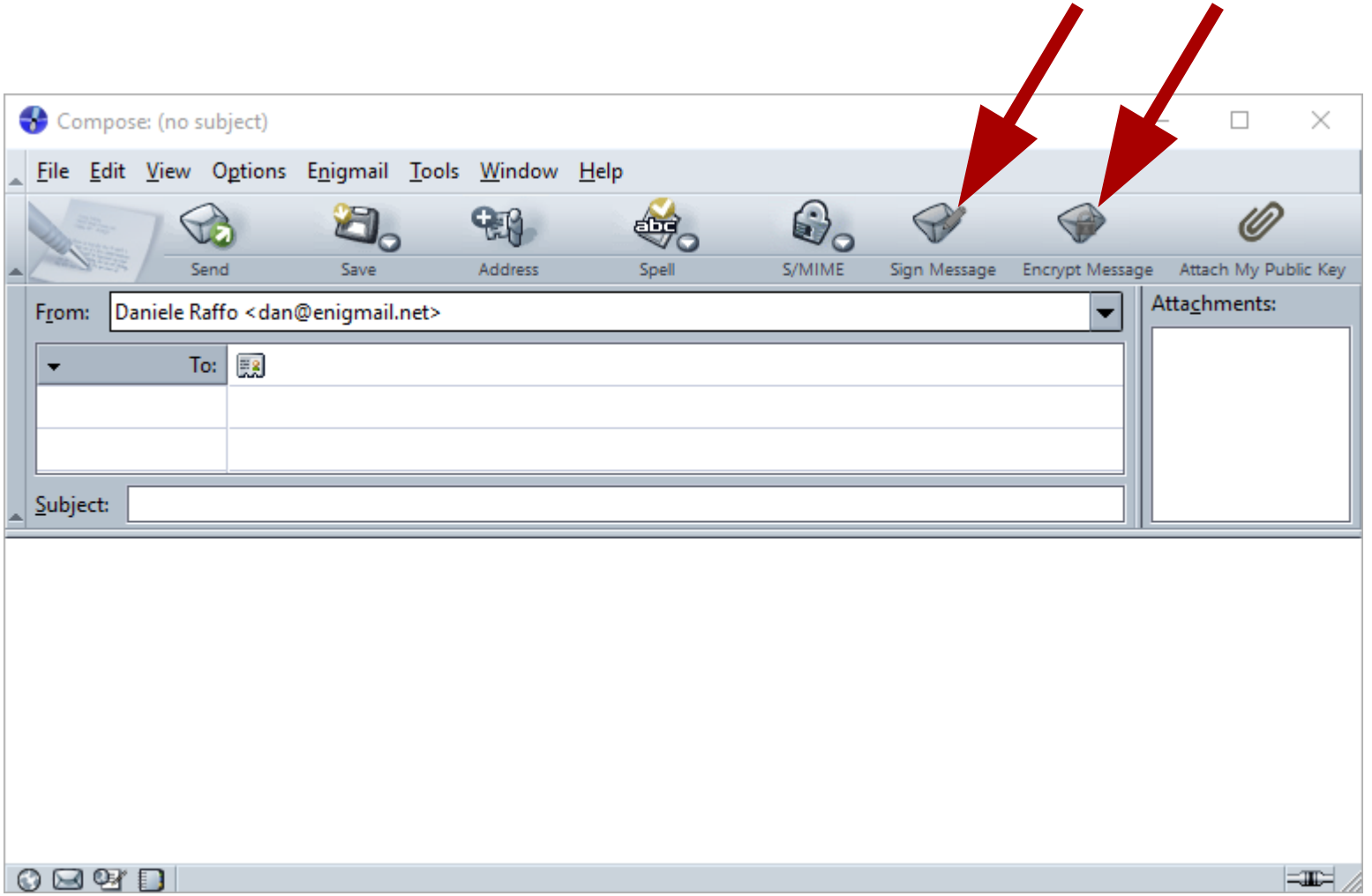
- 1976: Diffie-Hellman-Merkle key exchange
- 1977: Rivest-Shamir-Adleman, RSA cipher

➔ 1973: Ellis & Cocks (UK GCHQ) invent PKC, but discovery was classified until 1997!

Public Key Cryptography

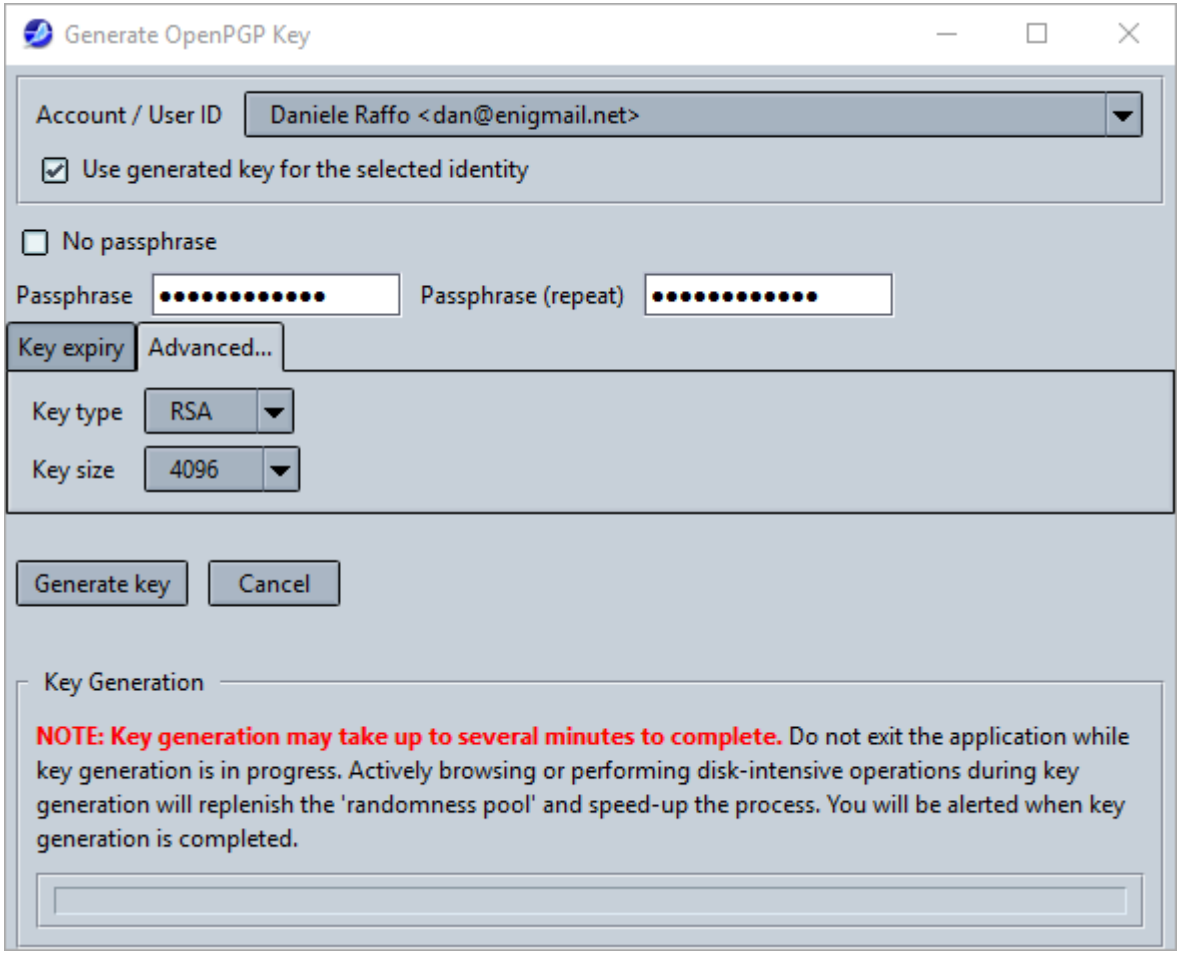
- 1991: **PGP** (Pretty Good Privacy)
- 1998: OpenPGP standard
- 1999: **GnuPG** / **GPG** (GNU Privacy Guard)
- 2001: **Enigmail**, a plugin for Thunderbird
- 2014: ProtonMail

Enigmail


Compose: (no subject)
File Edit View Options Enigmail Tools Window Help
Send
Save
Address
Spell
S/MIME
Sign Message
Encrypt Message
Attach My Public Key
From: Daniele Raffo <dan@enigmail.net>
To:
Subject:
Attachments:

Enigmail

First operation: create a key pair



Enigmail

Public key file

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

mQENBFFxC8kBCAC/oryc2v7UuCY0q7BJTm9oMZssVK0Unl9hh3mEd3z8jevlrDZ9
S4c9Z6SwK+BGL84rG9k2EkY/nYDI/+koBF43QT8LWHHUI1M+wFZ4myquNtUsPsq2
HT32YhoGLfSpKOIxxbniodsDzljR5tzO8Z3oYzNIHj5XKTmVBRDkwgQqODVcvxq8
RlNGR4Z+l1/7NFCRFUQ7fFLO3zSef1shqs5i95Q+QxySfIiGyrw0F59WOC4nrFFL
Kt8EhMAs8/c9WGQyWHQubX5PfxKrA+vYhXAtlFwDHQHbZ5VerIhCa15LNkH+WB1A
9DWF/6ocOF1ABMumiXriFdwPLTyLujumtV47ABEBAAG0IERhbmllbGUgUmFmZm8g
PGRhbkBlbmlnbWFpbC5uZXQ+iQE+BBMBAgAoBQJRcQvJAhsjBQkJZgGABgsJCAcD
AgYVCAIJCgsEFgIDAQIeAQIXgAAKCRCJ1WTtptUNvF0kB/9+fd6v7ExWmq5qx/B1
Iq/NIxgI+dwORBBy89VGV3NexxANOYKQti2y631YVv8s7qWjHzuIlPZ5pKq7OcHd
xY8fNtTQE92+eYxifMJj7uRqIloFDoMihpZAhA4kzsbyZl8YnPs1b16LQdhCEjF5
7QMXrk2hnVOPIqz/sxt++auTnTlAo/Z6bTkIrour68DCvS4YebIDjyzX2hObFE2T
17PPjuIYrRCyIlAB6U2kxypcRiC3IOLWfDXZrn8Qf/eQ6yt6zpWbc4DC6rZU9HmW
IrldsMcCeQsjJVpbzvfWthfQvMwjnXjIcaLLw7obcUOMSIBFhecozRFZCNknU8Hp
N/TMuQENBFFxC8kBCACzjNGMEUu5/hX/kRy9cETfmHvy3ntvb0Yq5p317A5poahZ
ZFuTGKA3ANy4syAxiYsA+jWk9xB0C8t6sqXtQUP6TjY63p3aKeJcq4SYEMfgKRq6
BZUj56rAkY87yX16PhkByEVK5pthCgfv8nbpCW7sczu0MG2o+mKTgpeuByhLzzS4
xf+WNeHi0R5WwX2+aJ2BhZT56YF5ZOCu6TWNwipmXpc5bnr9OKczgwcke/cqSM9C
7klDQZ2yV4Lbgokik9oU0sWeFr+UDLQxaSClv/l12tJJYyXHDOXlMPeBGkPu6TOC
KCjbr1FtKYx/Dc81SL4zoylMLmboGJTljAW2vkD/ABEBAAGJASUEGAECAA8FAlFx
C8kCGwwFCQlmAYAACgkQidVk7abVDbxgtwf+Jt7d1YDpcq3Pg/E2l2yCmAttPQbS
MIAv0agJax2hSukPWV3zlT8BTE5nXFICxmy6H8mNo2arQMtploC6cr3Brccvyzeq
1JvNmWvVUMeo2pEjJDEFfIqy44vKKVZjoDQfH4ZT3XaXmZu2t3TYpBJjzGCDUFLb
thsyPU/1xvtE+cATNlZJbzwLdCL7iOn6FiVXQkJXmYAkfBPoOE1pRIxmcHBZuxj6
EuDVjy4fZ4U8EScHcj/BKyBO2hwqPbo+iNlhuaZ6JWvWv5T6q8cjTxwK7VZ/ndrm
Dk407BwUvG3eWS/kamvmBLYbCIPye+GBLvpGBXNCgkUi+iLb73e1pG8eiw==
=JEo8
-----END PGP PUBLIC KEY BLOCK-----
```

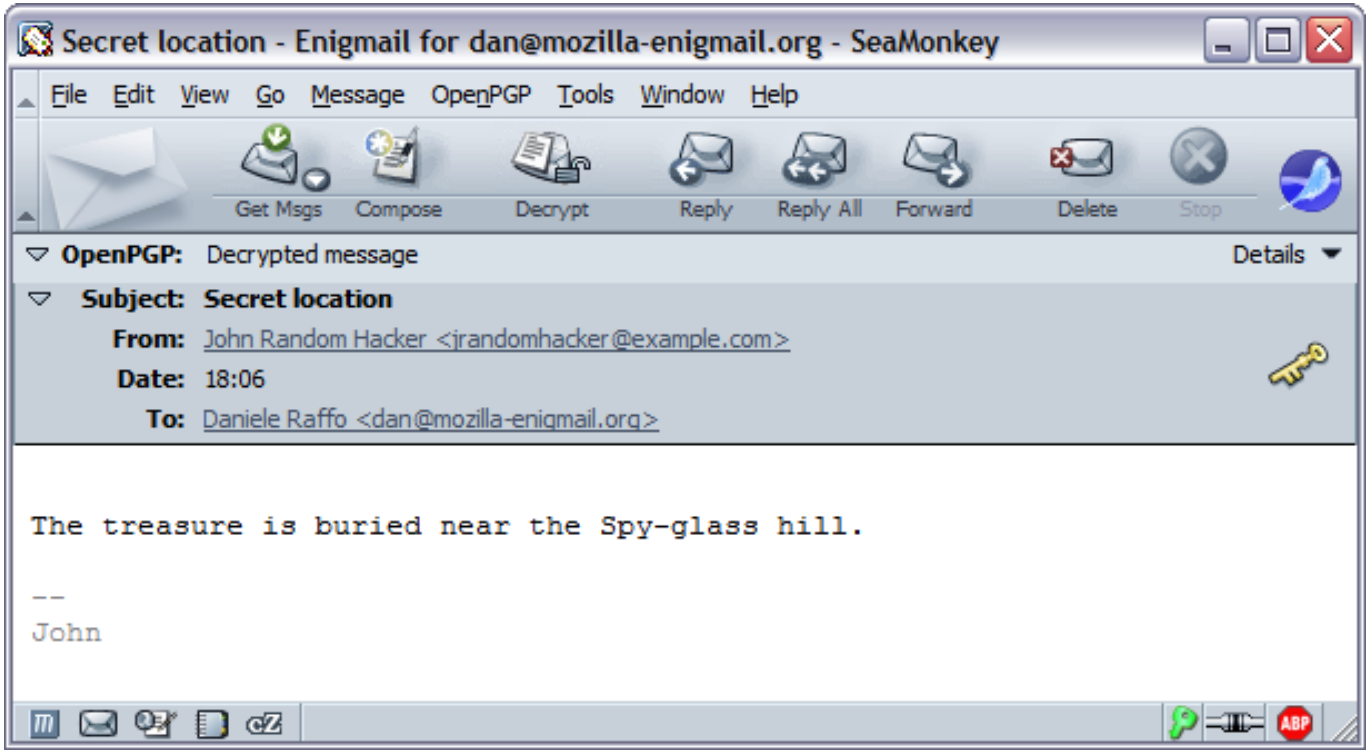
Enigmail

Private key file

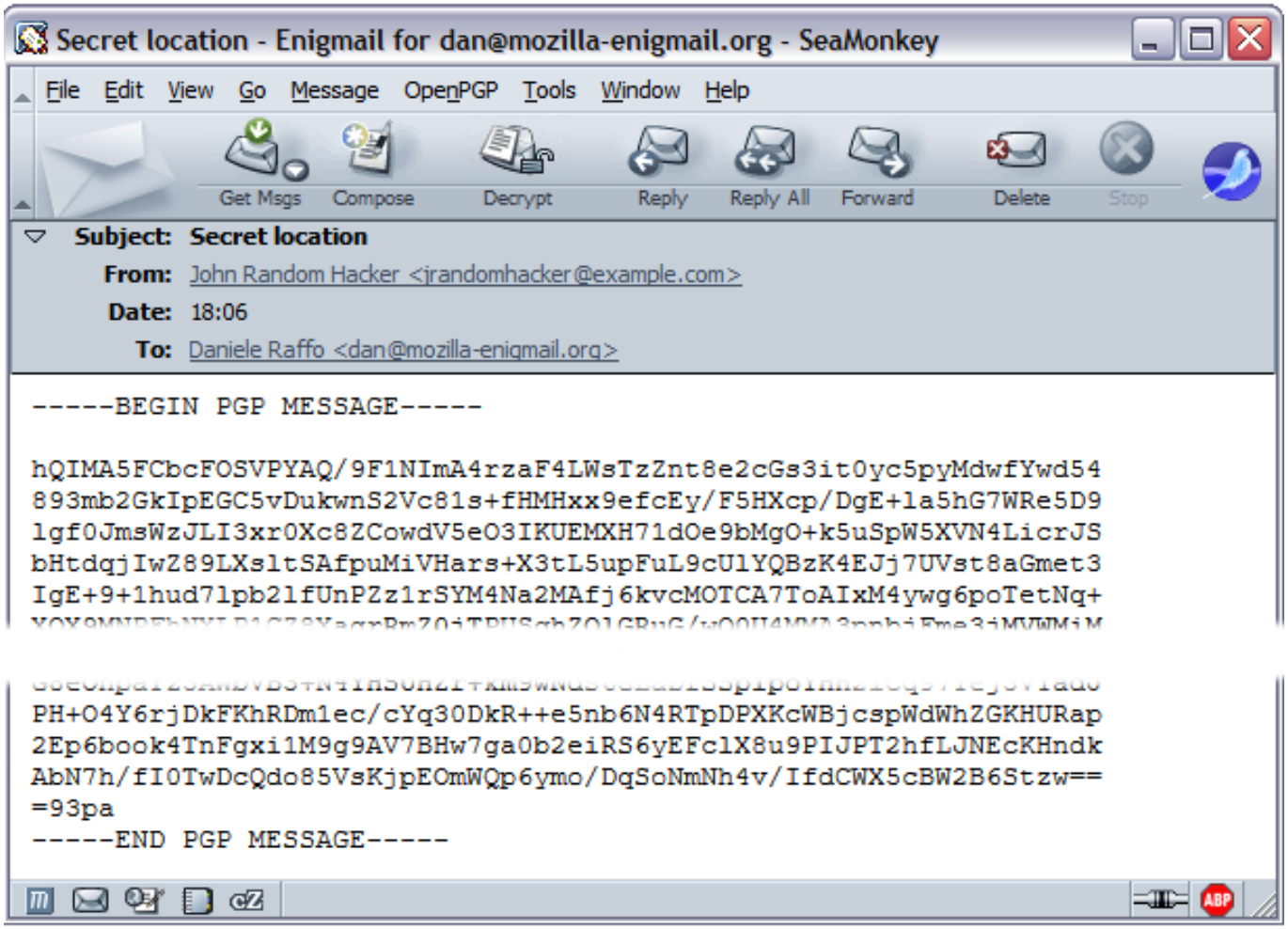
```
-----BEGIN PGP PRIVATE KEY BLOCK-----

mQGiBEgN3cERBAC+2os2hoACip4EiKxEzv+iVHOWaznOJIGZY9zY4y8C0BhUP++q
ccgO9vgNO1vIXApYvJctwX9HFJieNdlsBrWOR69hPBAbDo+3BbOKwJFYgq8akYnv
tBCOdCNfOFwQs/8XdOH25/Oig+UjKhgxwKjkdd1UCj7shdGioXOvjO13xwCgzrGa
k2oA9Bne3hW+jUPjJlU4UbkD/i7mbQfFwTgxcXfRfsVDnkmPc+QvKe00ajfRP31o
DbRCRL4GZCFTx4/DFy1jYbgYwl6MoCtSlufca3v5jpZbRgtKndcnlrauJO16EURs
LovKAJEkeCIcbTJTwnxMxCapTWhqIaitumZ6davIvV93UcDnQfYiCASzE5q/MD8L
lqsLA/9RvqoiAWzlq+MAL0MaEBTGee7YDTX08Ia1H3mEvxvjwuhPv54aTWIrbKfn
MFzkiFyUvQ5w3TwX8Fn17cuQNpCXTh00iG30GuZVl1aOl3fQXU/c9+vw2Rb0gvDF
BBlsnZ0MQns5bt6azIcLW44FzO2NKiK6/Y2XTiDVhtSAihTWLrQmRGFuaWVsZSBS
(...)
LunxO87fZF+JOoxs9F0IweA2nb1ga7fQ4Ud20ZVKfE4+vGCV5KXRNcOPbJL+vzuD
I7dMD+T05X8kK2x2HsaURdpKOZVhAuHIzEqn7E1UnUXnm4nVXg2bkAkBPQdfd97D
3bRLiE8EGBECAA8FAkgN3cECGwwFCQlmAYAACgkQW9ZLGa9iatRGlACeIyyIBTGj
wBa7+LHVnLQAoKbRuNotayAQzd7VOOKwKIZ+npLF
=vE7c
-----END PGP PRIVATE KEY BLOCK-----
```

Do not distribute your private key!

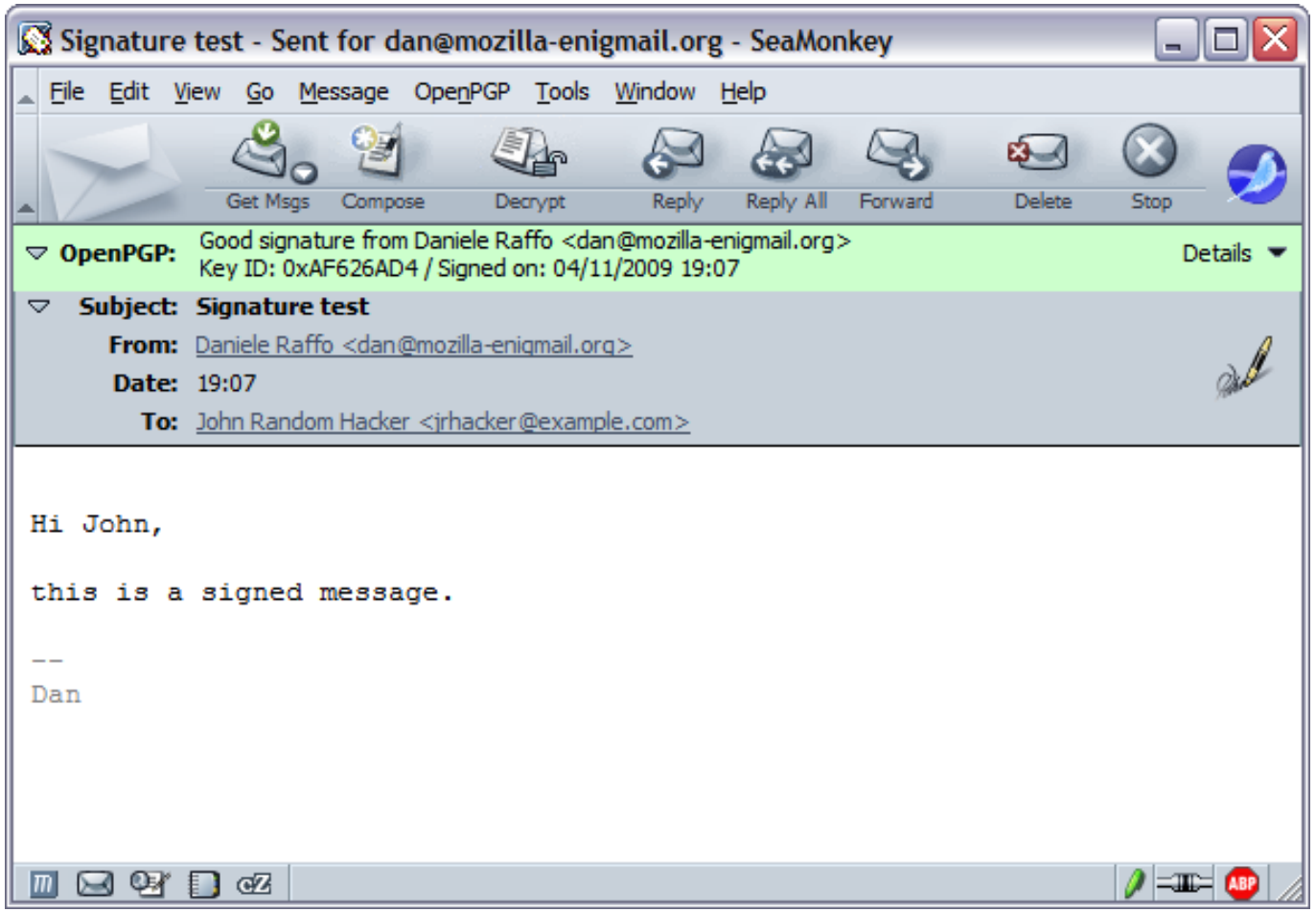
Enigmail


Secret location - Enigmail for dan@mozilla-enigmail.org - SeaMonkey
File Edit View Go Message OpenPGP Tools Window Help
Get Msgs
Compose
Decrypt
Reply
Reply All
Forward
Delete
Stop
OpenPGP: Decrypted message
Details
Subject: Secret location
From: John Random Hacker <jrandomhacker@example.com>
Date: 18:06
To: Daniele Raffo <dan@mozilla-enigmail.org>
The treasure is buried near the Spy-glass hill.
--
John

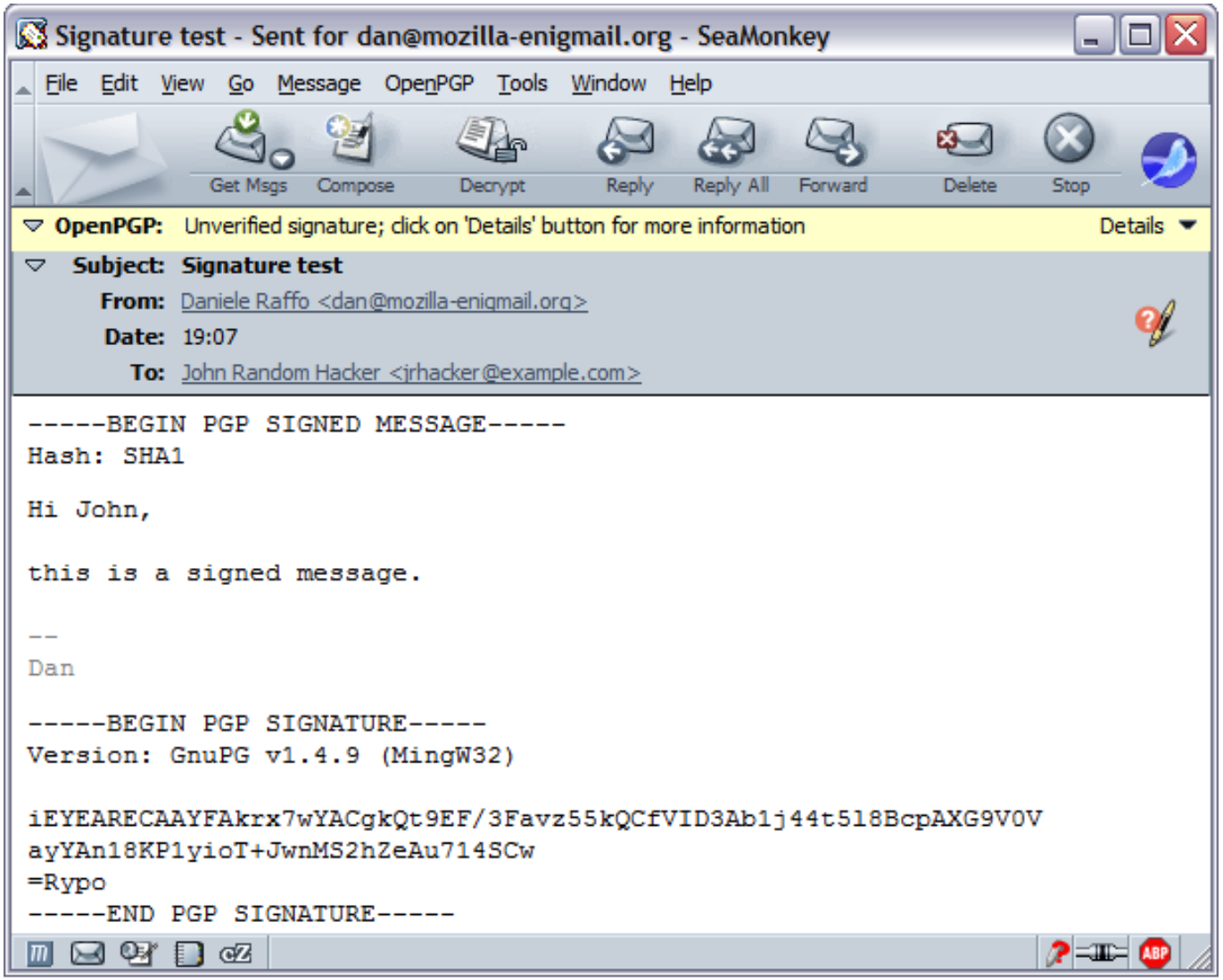
Enigmail


Secret location - Enigmail for dan@mozilla-enigmail.org - SeaMonkey
File Edit View Go Message OpenPGP Tools Window Help
Get Msgs Compose Decrypt Reply Reply All Forward Delete Stop
Subject: Secret location
From: John Random Hacker <jrandomhacker@example.com>
Date: 18:06
To: Daniele Raffo <dan@mozilla-enigmail.org>
-----BEGIN PGP MESSAGE-----
hQIMA5FCbcFOSVPYAQ/9F1NImA4rzaF4LWsTzZnt8e2cGs3it0yc5pyMdwfYwd54
893mb2GkIpEGC5vDukwnS2Vc81s+fHMHxx9efcEy/F5HXcp/DgE+1a5hG7WRe5D9
lgf0JmsWzJLI3xr0Xc8ZCowdV5eO3IKUEMXH71dOe9bMgO+k5uSpW5XVN4LicrJS
bHtdqjIwZ89LXsltSAfpuMiVHars+X3tL5upFuL9cUlYQBzK4EJj7UVst8aGmet3
IgE+9+1hud7lpb2lfUnPZz1rSYM4Na2MAfj6kvcMOTCA7ToAIxM4ywg6poTetNq+
PH+O4Y6rjDkFKhRDm1ec/cYq30DkR++e5nb6N4RTpDPXKcWBjcspWdWhZGKHURap
2Ep6book4TnFgxi1M9g9AV7BHw7ga0b2eiRS6yEFclX8u9PIJPT2hfLJNEcKHndk
AbN7h/fI0TwDcQdo85VsKjpEOmWQp6ymo/DqSoNmNh4v/IfdCWX5cBW2B6Stzw==
=93pa
-----END PGP MESSAGE-----

Enigmail

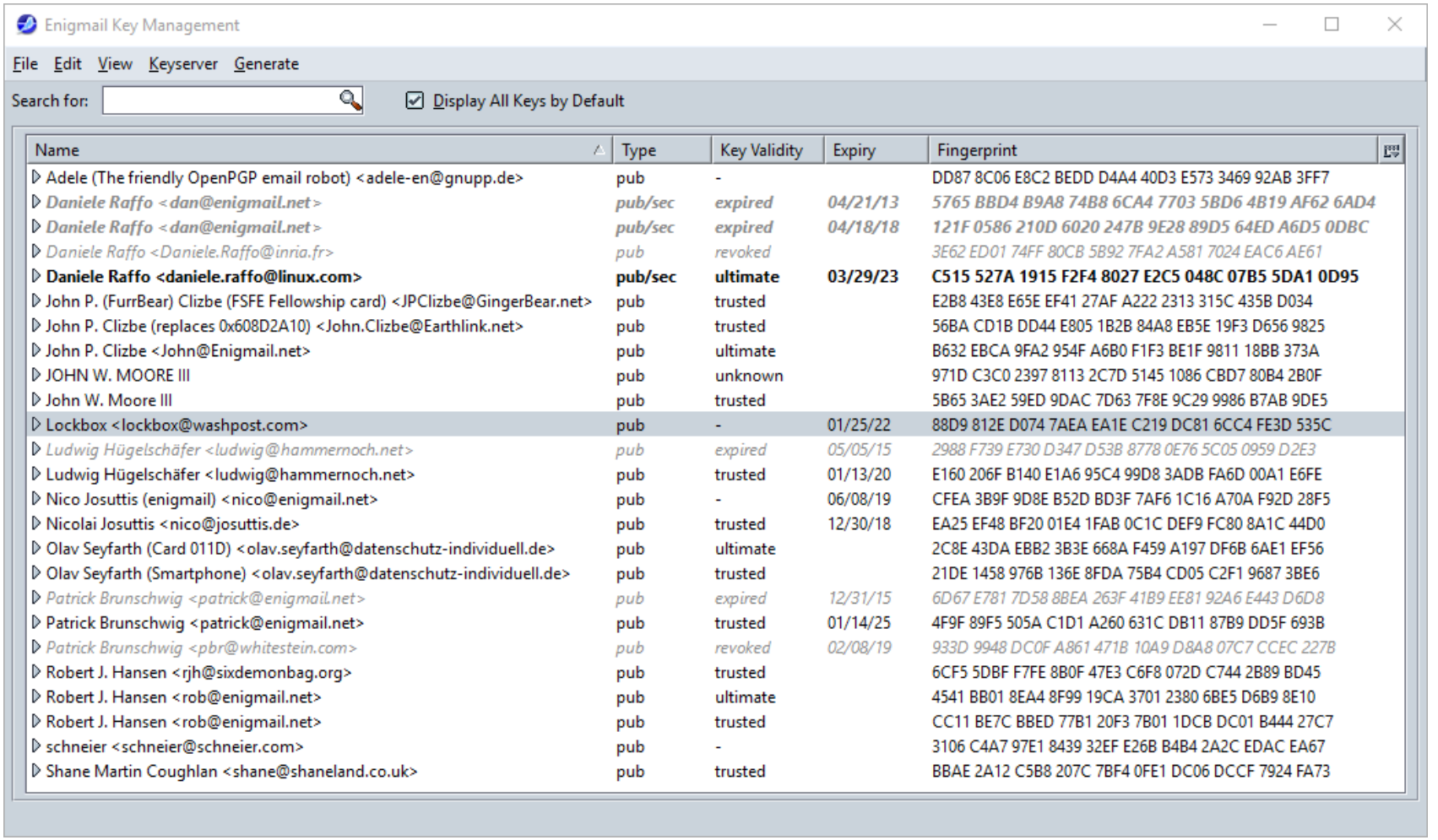

Signature test - Sent for dan@mozilla-enigmail.org - SeaMonkey
File Edit View Go Message OpenPGP Tools Window Help
Get Msgs Compose Decrypt Reply Reply All Forward Delete Stop
OpenPGP: Good signature from Daniele Raffo <dan@mozilla-enigmail.org>
Key ID: 0xAF626AD4 / Signed on: 04/11/2009 19:07
Details
Subject: Signature test
From: Daniele Raffo <dan@mozilla-enigmail.org>
Date: 19:07
To: John Random Hacker <jrhacker@example.com>
Hi John,
this is a signed message.
--
Dan

Enigmail


Signature test - Sent for dan@mozilla-enigmail.org - SeaMonkey
File Edit View Go Message OpenPGP Tools Window Help
Get Msgs Compose Decrypt Reply Reply All Forward Delete Stop
OpenPGP: Unverified signature; click on 'Details' button for more information
Details
Subject: Signature test
From: Daniele Raffo <dan@mozilla-enigmail.org>
Date: 19:07
To: John Random Hacker <jrhacker@example.com>
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
Hi John,
this is a signed message.
--
Dan
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (MingW32)
iEYEARECAAYFAkrx7wYACgkQt9EF/3Favz55kQCfVID3Ab1j44t518BcpAXG9V0V
ayYAn18KP1yioT+JwnMS2hZeAu714SCw
=Rypo
-----END PGP SIGNATURE-----

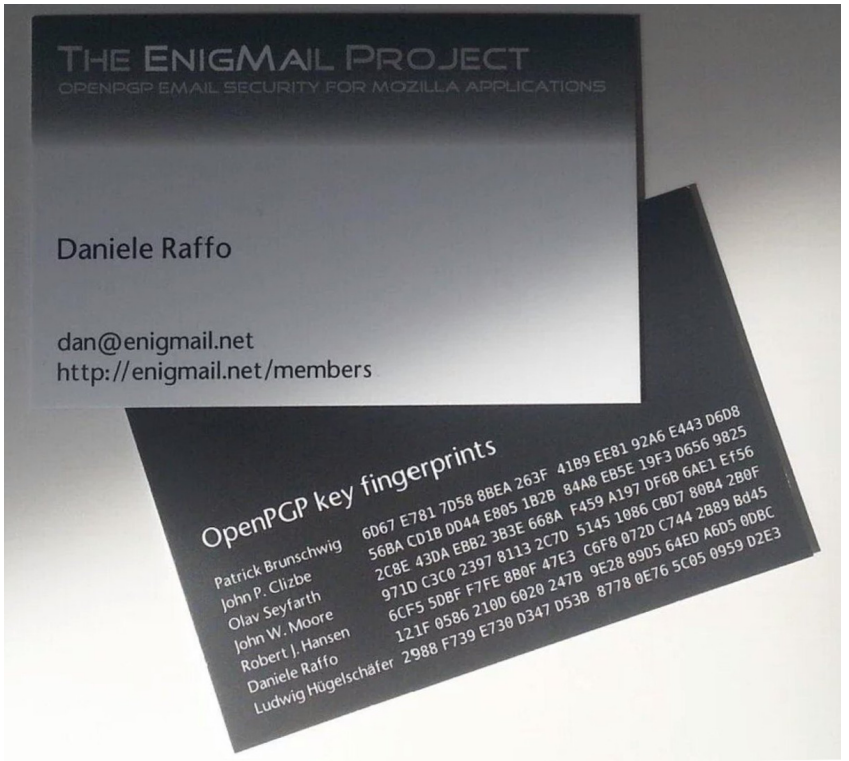
Enigmail

Your **keyring** contains all your collected keys



Public Key Cryptography

Check a public key's **fingerprint** to ensure that it belongs to the correct person



Public Key Cryptography

How to obtain someone's PGP public key:

- by hand, via e-mail, from website, etc.
- from a keyserver
- via Web of Trust / key signing parties
- from Web Key Directory

Public Key Cryptography

Other uses of PKC:

- SSL/TLS (HTTPS)
- secure IM: WhatsApp, Signal, etc.
- digitally signed software
- SSH
- S/MIME email security

Public Key Cryptography

Different techniques for key authentication

S/MIME, HTTPS, signed software:
➔ public key is embedded in a certificate issued by a trusted CA

SSH, secure IM:
➔ trust on first use (optional fingerprint check)

Public Key Cryptography

Thanks for your attention!