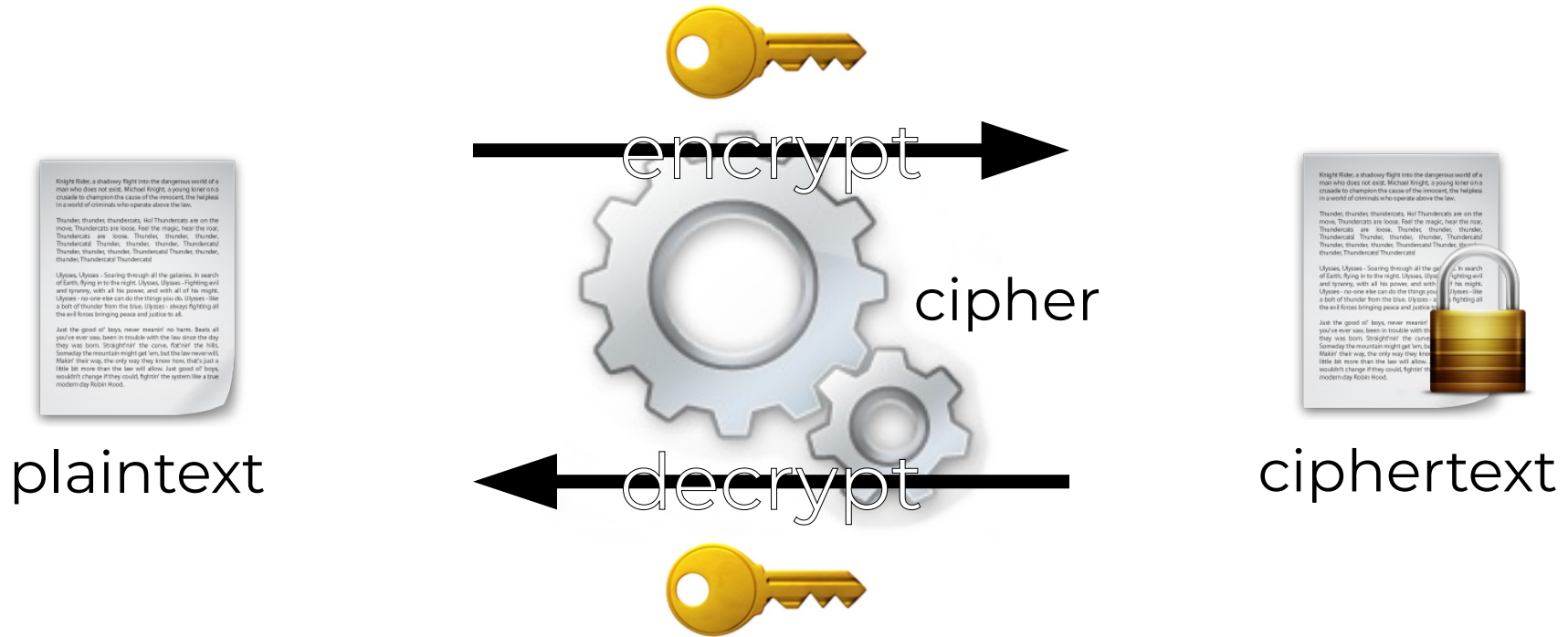


Public Key Cryptography, OpenPGP, and Enigmail

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

Symmetric Cryptography

shared secret key



Symmetric Cryptography

Examples of **symmetric ciphers**:

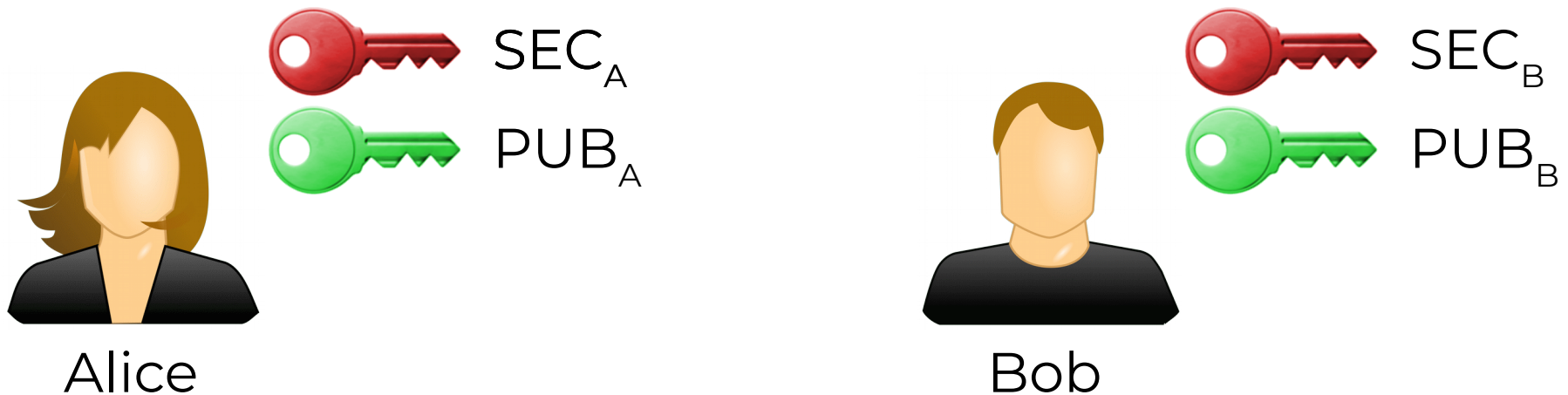
- Caesar (I cent. BCE)
- substitution (IV cent.)
- Vigenère (XVI cent.)
- Beaufort (XIX cent.)
- DES (1975)
- 3DES (1998)
- AES (1998)
- etc.



Symmetric Cryptography

Problem: deliver the key to the recipient!

Public Key Cryptography (Asymmetric Cryptography)



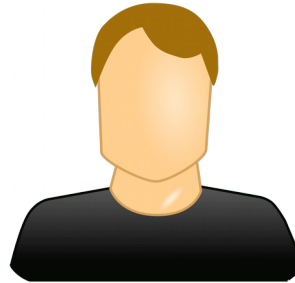
First, each participant generates a **key pair** composed of a **private key** and a **public key**

Public Key Cryptography

Encryption/Decryption (for confidentiality)



Alice



Bob

Knight Rider, a shadowy fight into the dangerous world of a man who does not exist. Michael Knight, a young biker on a crusade to champion the cause of the innocent, the helpless in a world of criminals who operate above the law.

Thunder, thunders, thunders, Ho! Thunders are on the move. Thunders are loose. Feel the magic, hear the roar. Thunders are loose. Thunder, thunders, thunders, Thunders! Thunder, thunders, thunders, Thunders! Thunder, thunders, thunders, Thunders! Thunder, thunders, thunders, Thunders! Thunder, thunders, thunders, Thunders!

Ulysses, Ulysses - Soaring through all the galaxies. In search of Earth. Flying in to the night. Ulysses, Ulysses - Fighting evil and tyranny, with all his power, and with all of his might. Ulysses - no one else can do the things you do. Ulysses - like a bolt of thunder from the blue. Ulysses - always fighting all the evil forces bringing noise and justice to all.

Just the good ol' boys, never messin' no harm. Beats all you've ever saw, been in trouble with the law since the day they was born. Straighten' the curve, fixin' the hole. Someday the mountain might get 'em, but the law never will. Make it their way, the only way they know how, that's just a little bit more than the law will allow. Just good ol' boys, wouldn't change if they could, fightin' the system like a true modern-day Robin Hood.



PUB_B



Knight Rider, a shadowy fight into the dangerous world of a man who does not exist. Michael Knight, a young biker on a crusade to champion the cause of the innocent, the helpless in a world of criminals who operate above the law.

Thunder, thunders, thunders, Ho! Thunders are on the move. Thunders are loose. Feel the magic, hear the roar. Thunders are loose. Thunder, thunders, thunders, Thunders! Thunder, thunders, thunders, Thunders! Thunder, thunders, thunders, Thunders! Thunder, thunders, thunders, Thunders!

Ulysses, Ulysses - Soaring through all the galaxies. In search of Earth. Flying in to the night. Ulysses, Ulysses - Fighting evil and tyranny, with all his power, and with all of his might. Ulysses - no one else can do the things you do. Ulysses - like a bolt of thunder from the blue. Ulysses - always fighting all the evil forces bringing noise and justice to all.

Just the good ol' boys, never messin' no harm. Beats all you've ever saw, been in trouble with the law since the day they was born. Straighten' the curve, fixin' the hole. Someday the mountain might get 'em, but the law never will. Make it their way, the only way they know how, that's just a little bit more than the law will allow. Just good ol' boys, wouldn't change if they could, fightin' the system like a true modern-day Robin Hood.



SEC_B



Knight Rider, a shadowy fight into the dangerous world of a man who does not exist. Michael Knight, a young biker on a crusade to champion the cause of the innocent, the helpless in a world of criminals who operate above the law.

Thunder, thunders, thunders, Ho! Thunders are on the move. Thunders are loose. Feel the magic, hear the roar. Thunders are loose. Thunder, thunders, thunders, Thunders! Thunder, thunders, thunders, Thunders! Thunder, thunders, thunders, Thunders! Thunder, thunders, thunders, Thunders!

Ulysses, Ulysses - Soaring through all the galaxies. In search of Earth. Flying in to the night. Ulysses, Ulysses - Fighting evil and tyranny, with all his power, and with all of his might. Ulysses - no one else can do the things you do. Ulysses - like a bolt of thunder from the blue. Ulysses - always fighting all the evil forces bringing noise and justice to all.

Just the good ol' boys, never messin' no harm. Beats all you've ever saw, been in trouble with the law since the day they was born. Straighten' the curve, fixin' the hole. Someday the mountain might get 'em, but the law never will. Make it their way, the only way they know how, that's just a little bit more than the law will allow. Just good ol' boys, wouldn't change if they could, fightin' the system like a true modern-day Robin Hood.

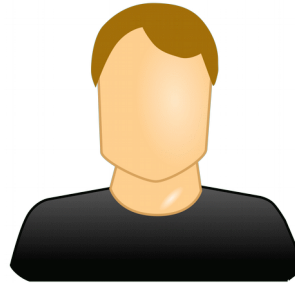


Public Key Cryptography

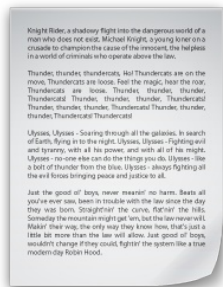
Digital signature (for authentication & integrity)



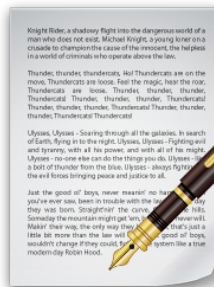
Alice



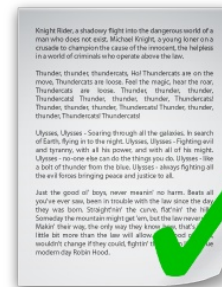
Bob



SEC_A

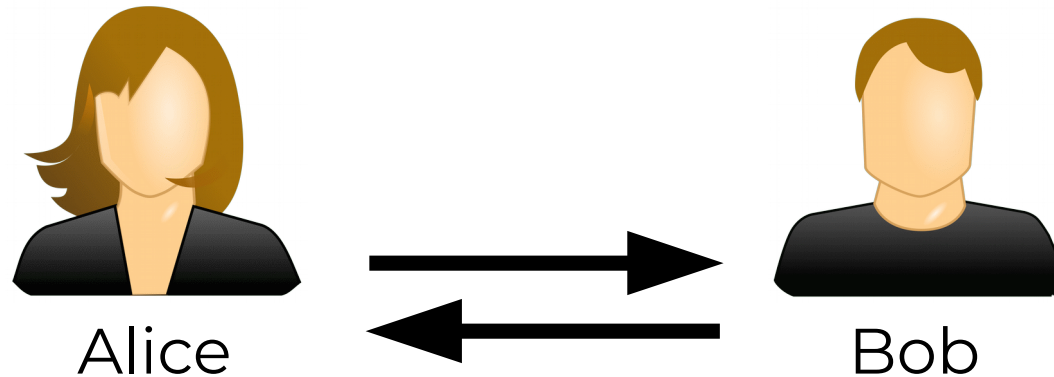


PUB_A



Public Key Cryptography

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



DH-RSA:

- discrete logarithm problem
e.g. $453^x \pmod{21997} = 5787 \quad x = ?$
- prime factorization
e.g. prime factors of $7774733 = ?$

Public Key Cryptography

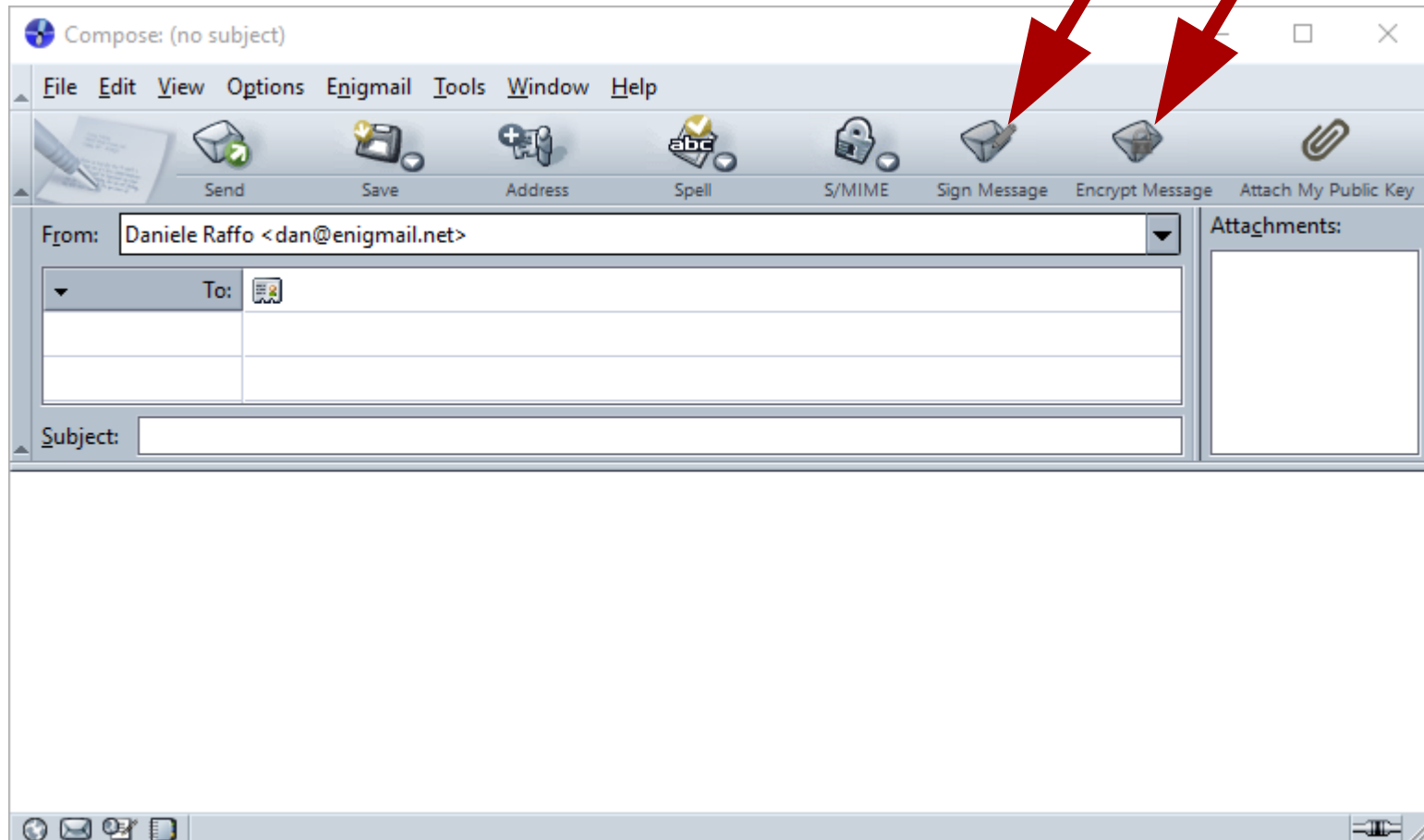
Birth of **Public Key Cryptography**:

- 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



Enigmail

First operation: create a key pair



Generate OpenPGP Key

Account / User ID: Daniele Raffo <dan@enigmail.net>

Use generated key for the selected identity

No passphrase

Passphrase: Passphrase (repeat):

Key expiry: Advanced...

Key type: RSA

Key size: 4096

Generate key Cancel

Key Generation

NOTE: Key generation may take up to several minutes to complete. Do not exit the application while key generation is in progress. Actively browsing or performing disk-intensive operations during key generation will replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is completed.



Enigmail

Public key file

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

```
mQENBFFxC8kBCAC/oryc2v7UuCY0q7BJTm9oMZssVK0Unl9hh3mEd3z8jev1rDZ9
S4c9Z6SwK+BGL84rG9k2EkY/nYDI/+koBF43QT8LWHHUI1M+wFZ4myquNtUsPsq2
HT32YhoGLfSpKOIxxbniodsDzljr5tzo8Z3oYzNIHj5XKTmVBRDkkgQqODVcvxq8
RlNGR4Z+l1/7NFCRFUQ7fFLO3zSef1shqs5i95Q+QxySfIiGyrw0F59WOC4nrFFL
Kt8EhMAS8/c9WGQyWHQubX5PfxKrA+vYhXat1FwDHQHbZ5VerIhCa15LNkH+WB1A
9DWF/6ocOF1ABMumiXriFdwPLTyLujumtV47ABEBAAG0IERhbml1bGUgUmFmZm8g
PGRhbkb1bmlnbWFpbC5uZXQ+iQE+BBMBAgAoBQJRcQvJAhsjBQkJZgGABgsJCAcD
AgYVCAIJCgsEFgIDAQIeAQIXgAAKCRcJ1WTtptUNvF0kB/9+fd6v7ExWmq5qx/B1
Iq/NixgI+dwORBBY89VGV3NexxANoyKQti2y631YVv8s7qWjHzuI1PZ5pKq70cHd
xY8fNtTQE92+eYxifMJj7uRqIloFDoMihpZAhA4kzsbyZ18YnPs1b16LQdhCEjF5
7QMXrk2hnVOPIqz/sxt++auTnTlAo/Z6bTkIrou68DCvS4YebIDjyzX2hObFE2T
17PPjuIYrRCyIlAB6U2kxypcRiC3IOLWfDXZrn8Qf/eQ6yt6zpwbc4DC6rZU9HmW
IrlDsMcCeQsjJVpbzvfWthfQvMwjnXjIcaLLw7obcUOMSIBFhecozRFZCNknU8Hp
N/TMuQENBFFxC8kBCACzjNGMEUu5/hX/kRy9cETfmHvy3ntvb0Yq5p317A5poahZ
ZFuTGKA3ANy4syAxiYsA+jWk9xB0C8t6sqXtQUP6TjY63p3aKeJc44SYEMfgKRq6
BZUj56rAkY87yX16PhkByEVK5pthCgfv8nbpCW7sczu0MG2o+mKTgpeuByhLzzS4
xf+WNeHi0R5WwX2+aJ2BhZT56YF5ZOCu6TWNwipmXpc5bnr90Kczgwcke/cqSM9C
7klDQZ2yV4Lbgokik9oU0sWeFr+UDLQxaSclv/112tJJYyXHD0X1MPEBGkPu6TOC
KCjbr1FtKYx/Dc81SL4zoYlMLmboGJTl1jAW2vkD/ABEBAAGJASUEGAECA8FA1Fx
C8kCGwWFCQlmAYAACgkQidV7abVDbxgtwf+Jt7d1YDpcq3Pg/E212yCmAttPQbS
MIAv0agJax2hSukPWV3z1T8BTE5nXFICxmy6H8mNo2arQMtploC6cr3Brccvzyeq
1JvNmWvVUMeo2pEjJDEFfIqy44vKKVZjoDQfH4ZT3XaXmZu2t3TYpBJjzGCDUFLb
thsyPU/1xvtE+cATN1ZJbzwLdCL7iOn6FiVXQkJXmYakfBPoOE1pRIxmcHBZuxj6
EuDVjy4fZ4U8EScHcj/BKyBO2hwqPbo+iNlhuaZ6JWvWv5T6q8cjTxwK7VZ/ndrm
Dk407BwUvG3eWS/kamvmBLYbCIPye+GBLvpGBXNCgkUi+iLb73elP8eiw==
=JEo8
```

-----END PGP PUBLIC KEY BLOCK-----



Enigmail

Private key file

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

```
mQGIBegN3cERBAC+2os2hoACip4EiKxEzv+iVHOWaznOJIGZY9zY4y8C0BhUP++q  
ccgO9vgNO1vIXApYvJctwX9HFJieNdlsBrWOR69hPBAAbDo+3BbOKwJFYgq8akYnv  
tBCodCNfOFwQs/8XdoH25/Oig+UjKhgxwKjkddlUCj7shdGioXOvj013xwCgZrGa  
k2oA9Bne3hW+jUPjJlU4Ubkd/i7mbQfFwTgxcXfRfsVDnkmPc+QvKe00ajfRP31o  
DbRCRL4GZCFTx4/DFy1jYbgYwl6MoCtSlufca3v5jpbZbRgtKndcnlrauJO16EURS  
LovKAJEkeCIcbTJTwnxMxCapTWhqIaitumZ6davIvV93UcDnQfYiCASzE5q/MD8L  
lqsLA/9RvqoiAWz1q+MAL0MaEBTGee7YDTX08Ia1H3mEvxvjwuhPv54aTWIrbKfn  
MFzkiFyUvQ5w3TwX8Fn17cuQNpCXTh00iG30GuZV11a013fQXU/c9+vw2Rb0gvDF  
BB1snZ0MQns5bt6azIcLW44FzO2NKiK6/Y2XTiDVhtSAihtWLRqMRFuaWVsZSBS  
(...)  
LunxO87fZF+JOoxs9F0IweA2nb1ga7fQ4Ud20ZVKfE4+vGCV5KXRNcOPbJL+vzuD  
I7dMD+T05X8kK2x2HsaURdpKOZVhAuHIzEqn7E1UnUXnm4nVXg2bkAkBPQdfd97D  
3bRLiE8EGBECAA8FAkgN3cECGwwFCQlmAYAACgkQW9ZLGA9iatRGLACeIyyIBTGj  
wBa7+LHVnLQAoKbRuNotayAQzd7VOOKwKIZ+npLF  
=vE7c
```

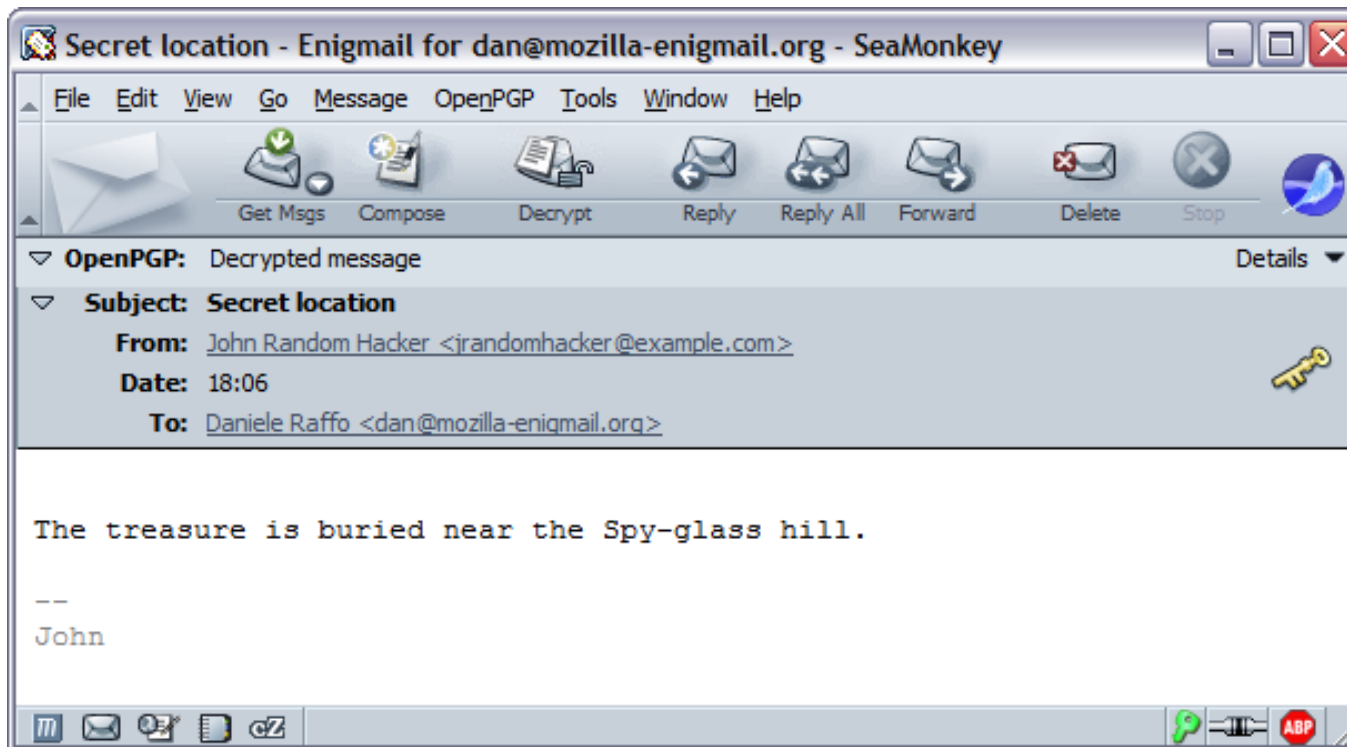
```
-----END PGP PRIVATE KEY BLOCK-----
```



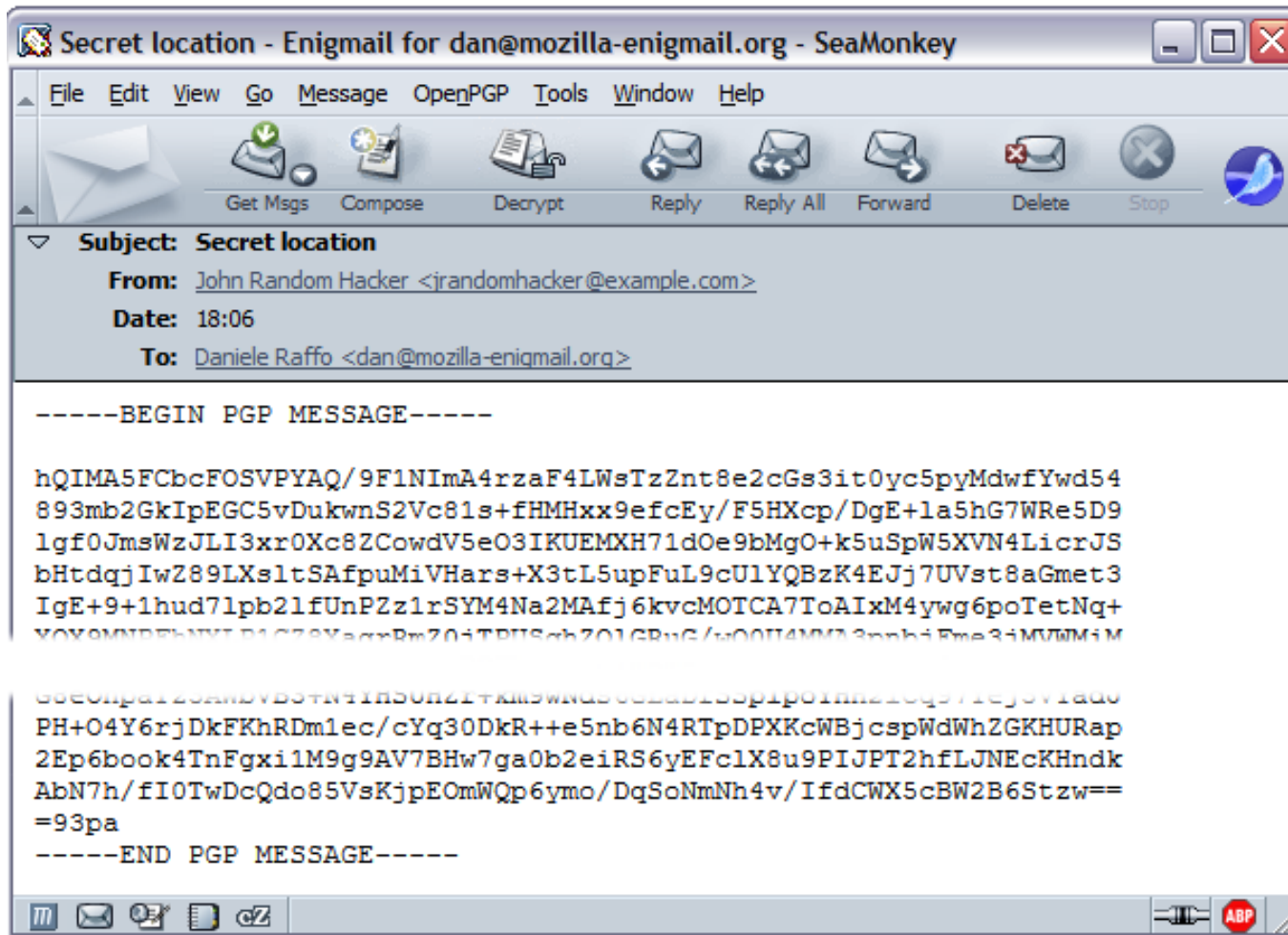
Do not distribute your private key!



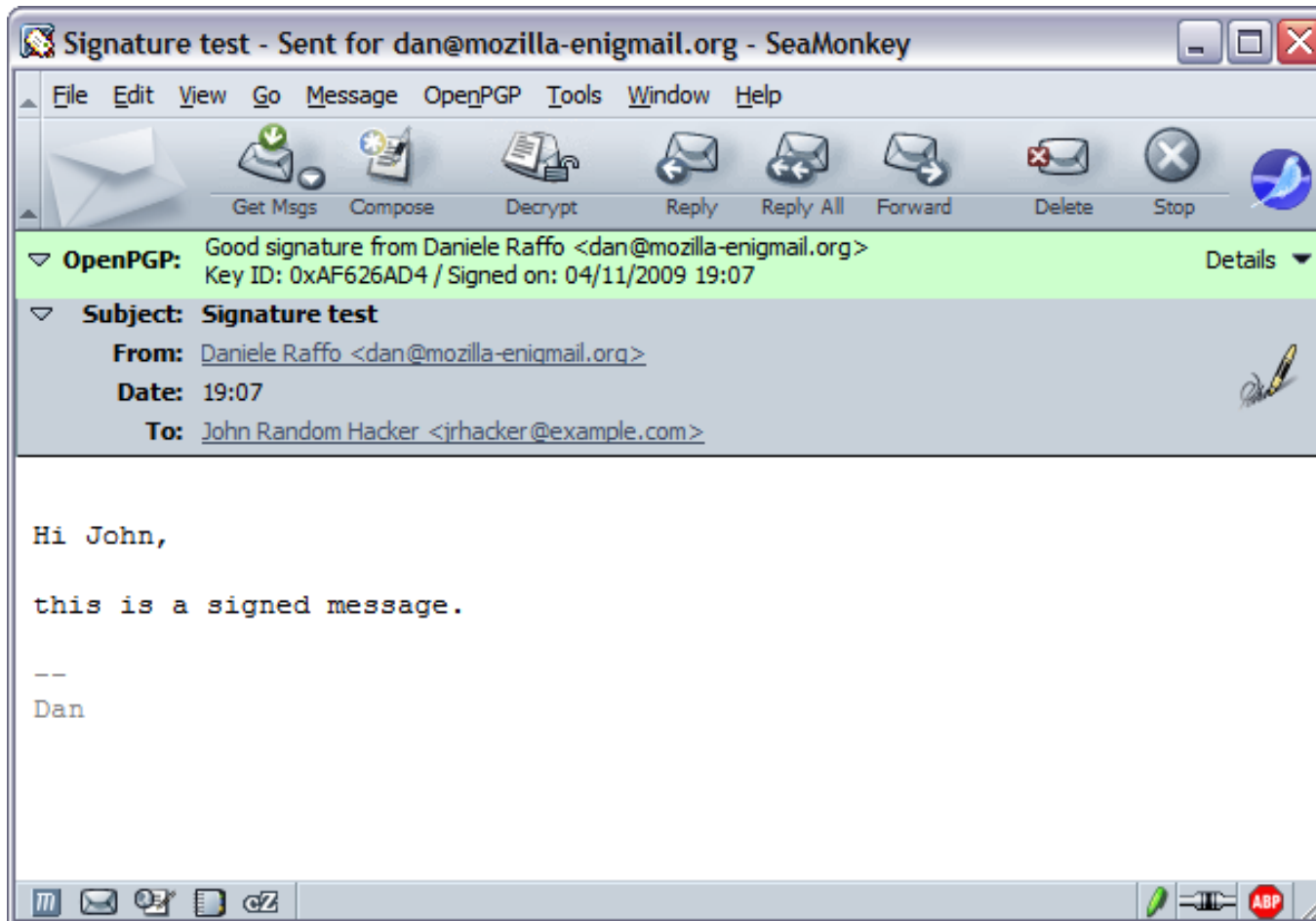
Enigmail



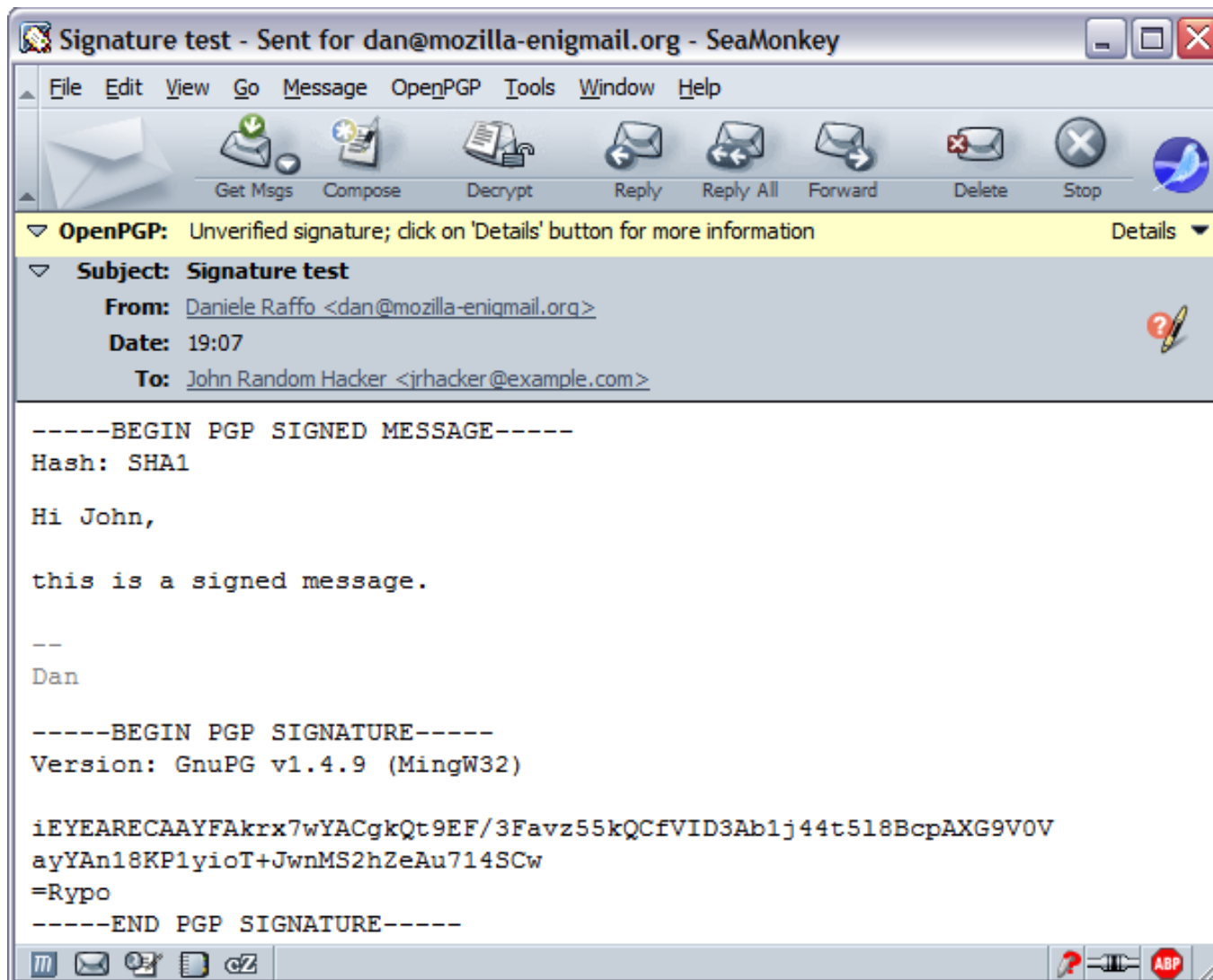
Enigmail



Enigmail

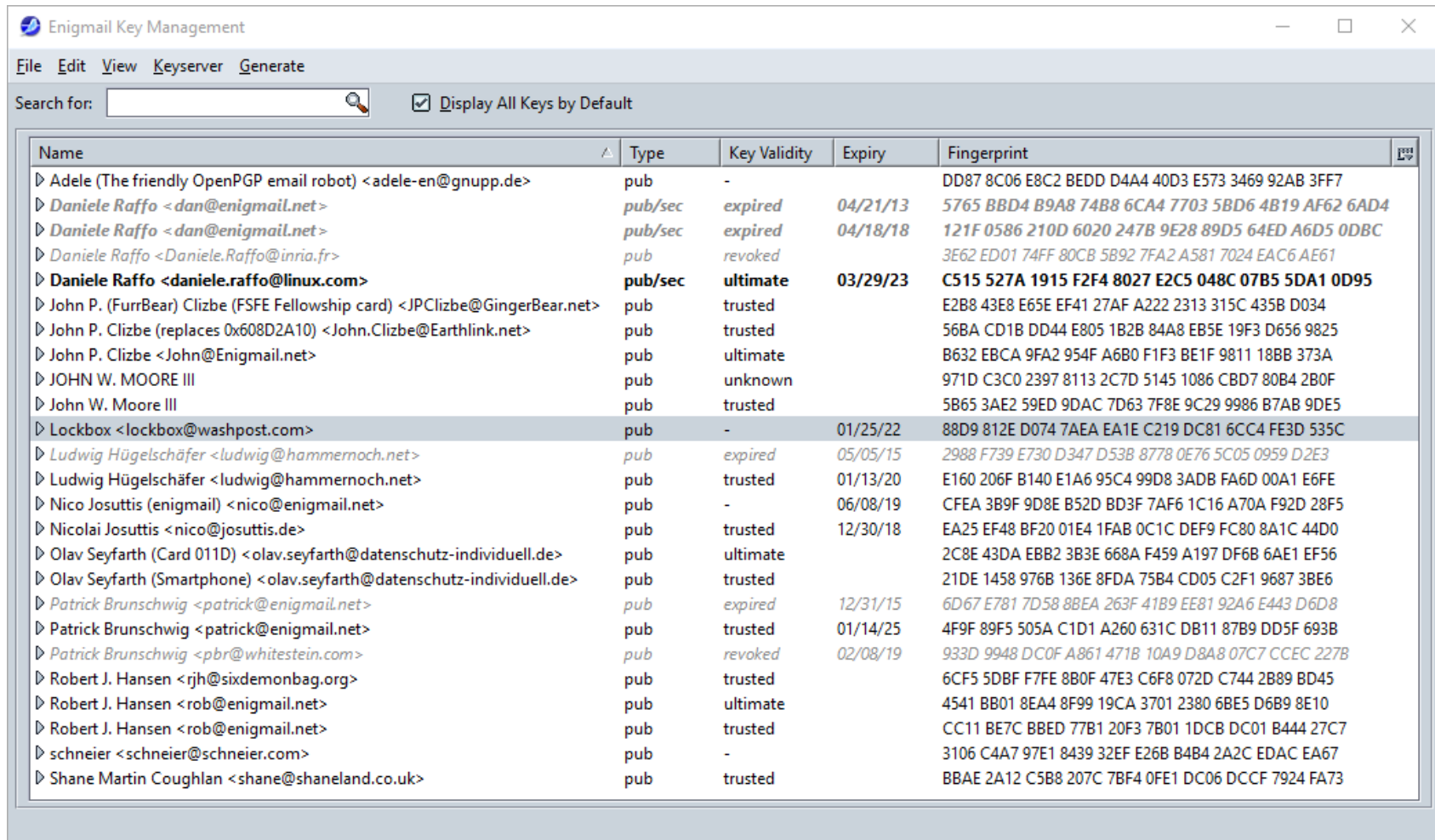


Enigmail



Enigmail

Your **keyring** contains all your collected keys



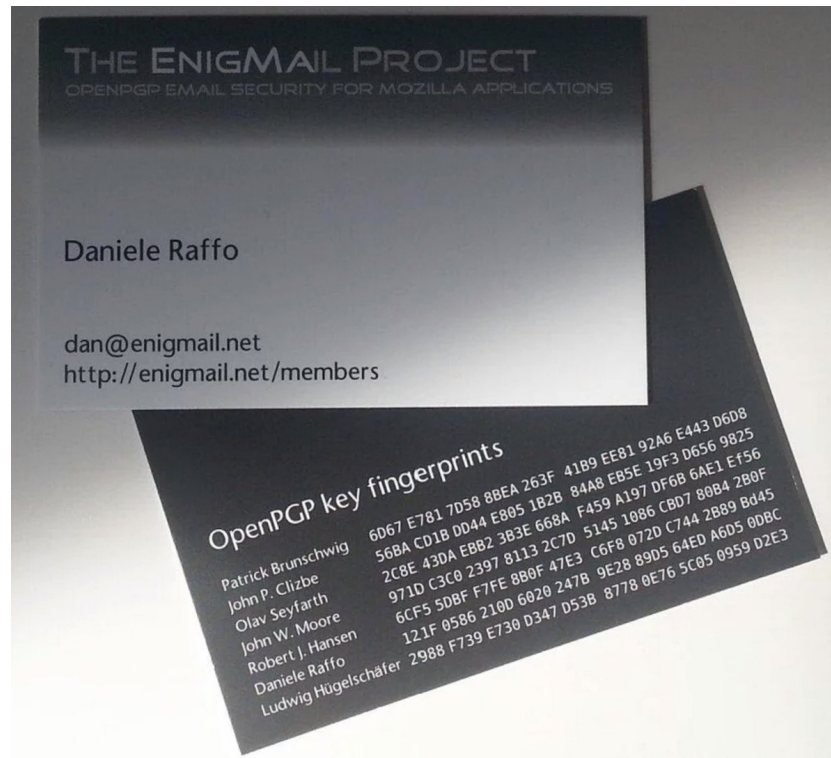
The screenshot shows the Enigmail Key Management application window. It features a menu bar with 'File', 'Edit', 'View', 'Keyserver', and 'Generate'. Below the menu is a search bar and a checkbox labeled 'Display All Keys by Default'. The main area contains a table with the following columns: Name, Type, Key Validity, Expiry, and Fingerprint. The table lists various keys, including those for Adele, Daniele Raffo, John P. Clizbe, John W. Moore III, Lockbox, Ludwig Hügelschäfer, Nico Josuttis, Nicolai Josuttis, Olav Seyfarth, Patrick Brunschwig, Robert J. Hansen, and Shane Martin Coughlan.

Name	Type	Key Validity	Expiry	Fingerprint
▶ Adele (The friendly OpenPGP email robot) <adele-en@gnupp.de>	pub	-		DD87 8C06 E8C2 BEDD D4A4 40D3 E573 3469 92AB 3FF7
▶ Daniele Raffo <dan@enigmail.net>	pub/sec	expired	04/21/13	5765 BBD4 B9A8 74B8 6CA4 7703 5BD6 4B19 AF62 6AD4
▶ Daniele Raffo <dan@enigmail.net>	pub/sec	expired	04/18/18	121F 0586 210D 6020 247B 9E28 89D5 64ED A6D5 0DBC
▶ Daniele Raffo <Daniele.Raffo@inria.fr>	pub	revoked		3E62 ED01 74FF 80CB 5B92 7FA2 A581 7024 EAC6 AE61
▶ Daniele Raffo <daniele.raffo@linux.com>	pub/sec	ultimate	03/29/23	C515 527A 1915 F2F4 8027 E2C5 048C 07B5 5DA1 0D95
▶ John P. (FurrBear) Clizbe (FSFE Fellowship card) <JPClizbe@GingerBear.net>	pub	trusted		E2B8 43E8 E65E EF41 27AF A222 2313 315C 435B D034
▶ John P. Clizbe (replaces 0x608D2A10) <John.Clizbe@Earthlink.net>	pub	trusted		56BA CD1B DD44 E805 1B2B 84A8 EB5E 19F3 D656 9825
▶ John P. Clizbe <John@Enigmail.net>	pub	ultimate		B632 EBCA 9FA2 954F A6B0 F1F3 BE1F 9811 18BB 373A
▶ JOHN W. MOORE III	pub	unknown		971D C3C0 2397 8113 2C7D 5145 1086 CBD7 80B4 2B0F
▶ John W. Moore III	pub	trusted		5B65 3AE2 59ED 9DAC 7D63 7F8E 9C29 9986 B7AB 9DE5
▶ Lockbox <lockbox@washpost.com>	pub	-	01/25/22	88D9 812E D074 7AEA EA1E C219 DC81 6CC4 FE3D 535C
▶ Ludwig Hügelschäfer <ludwig@hammernoeh.net>	pub	expired	05/05/15	2988 F739 E730 D347 D53B 8778 0E76 5C05 0959 D2E3
▶ Ludwig Hügelschäfer <ludwig@hammernoeh.net>	pub	trusted	01/13/20	E160 206F B140 E1A6 95C4 99D8 3ADB FA6D 00A1 E6FE
▶ Nico Josuttis (enigmail) <nico@enigmail.net>	pub	-	06/08/19	CFEA 3B9F 9D8E B52D BD3F 7AF6 1C16 A70A F92D 28F5
▶ Nicolai Josuttis <nico@josuttis.de>	pub	trusted	12/30/18	EA25 EF48 BF20 01E4 1FAB 0C1C DEF9 FC80 8A1C 44D0
▶ Olav Seyfarth (Card 011D) <olav.seyfarth@datenschutz-individuell.de>	pub	ultimate		2C8E 43DA EBB2 3B3E 668A F459 A197 DF6B 6AE1 EF56
▶ Olav Seyfarth (Smartphone) <olav.seyfarth@datenschutz-individuell.de>	pub	trusted		21DE 1458 976B 136E 8FDA 75B4 CD05 C2F1 9687 3BE6
▶ Patrick Brunschwig <patrick@enigmail.net>	pub	expired	12/31/15	6D67 E781 7D58 8BEA 263F 41B9 EE81 92A6 E443 D6D8
▶ Patrick Brunschwig <patrick@enigmail.net>	pub	trusted	01/14/25	4F9F 89F5 505A C1D1 A260 631C DB11 87B9 DD5F 693B
▶ Patrick Brunschwig <pbr@whitestein.com>	pub	revoked	02/08/19	933D 9948 DC0F A861 471B 10A9 D8A8 07C7 CCEC 2278
▶ Robert J. Hansen <rjh@sixdemonbag.org>	pub	trusted		6CF5 5DBF F7FE 8B0F 47E3 C6F8 072D C744 2B89 BD45
▶ Robert J. Hansen <rob@enigmail.net>	pub	ultimate		4541 BB01 8EA4 8F99 19CA 3701 2380 6BE5 D6B9 8E10
▶ Robert J. Hansen <rob@enigmail.net>	pub	trusted		CC11 BE7C BBED 77B1 20F3 7B01 1DCB DC01 B444 27C7
▶ schneier <schneier@schneier.com>	pub	-		3106 C4A7 97E1 8439 32EF E26B B4B4 2A2C EDAC EA67
▶ Shane Martin Coughlan <shane@shaneland.co.uk>	pub	trusted		BBAE 2A12 C5B8 207C 7BF4 0FE1 DC06 DCCF 7924 FA73



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!