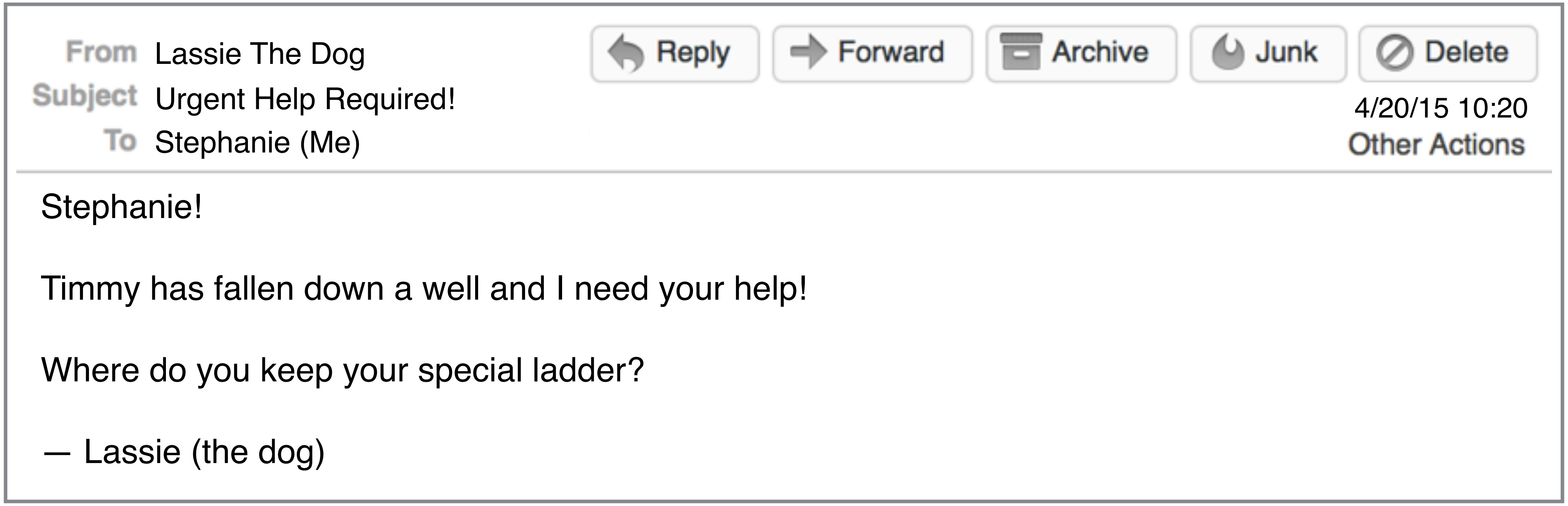
do you PGP?

(pretty good privacy)

@corcra
Stephanie Hyland

4/27/15, CryptoHarlem

suppose you receive an important message…



From Lassie The Dog
Subject Urgent Help Required!
To Stephanie (Me)

4/20/15 10:20

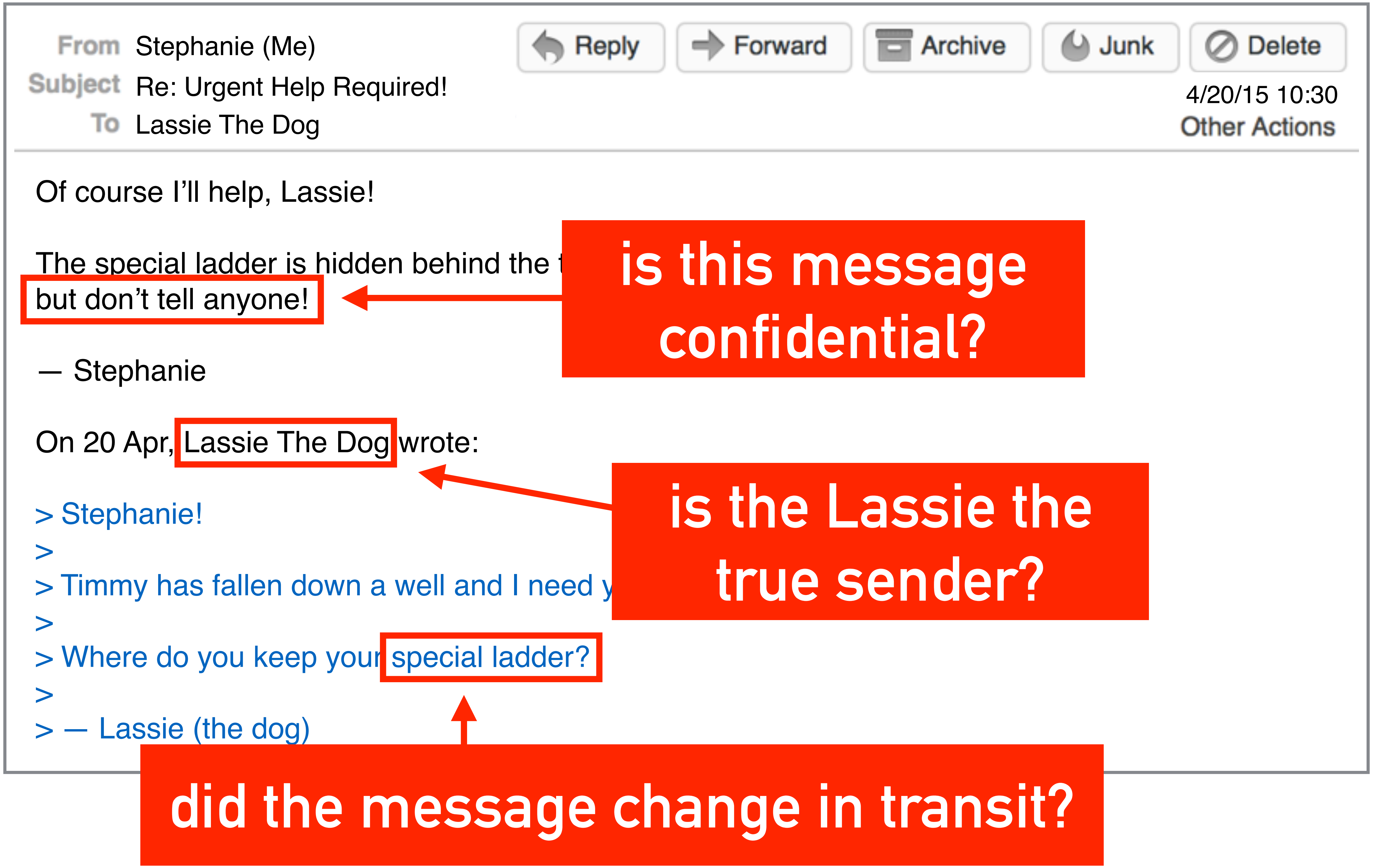
Stephanie!

Timmy has fallen down a well and I need your help!

Where do you keep your special ladder?

— Lassie (the dog)

DANGER!



From Stephanie (Me)
Subject Re: Urgent Help Required!
To Lassie The Dog

4/20/15 10:30

Of course I'll help, Lassie!

The special ladder is hidden behind the t
but don't tell anyone!

— Stephanie

On 20 Apr, Lassie The Dog wrote:

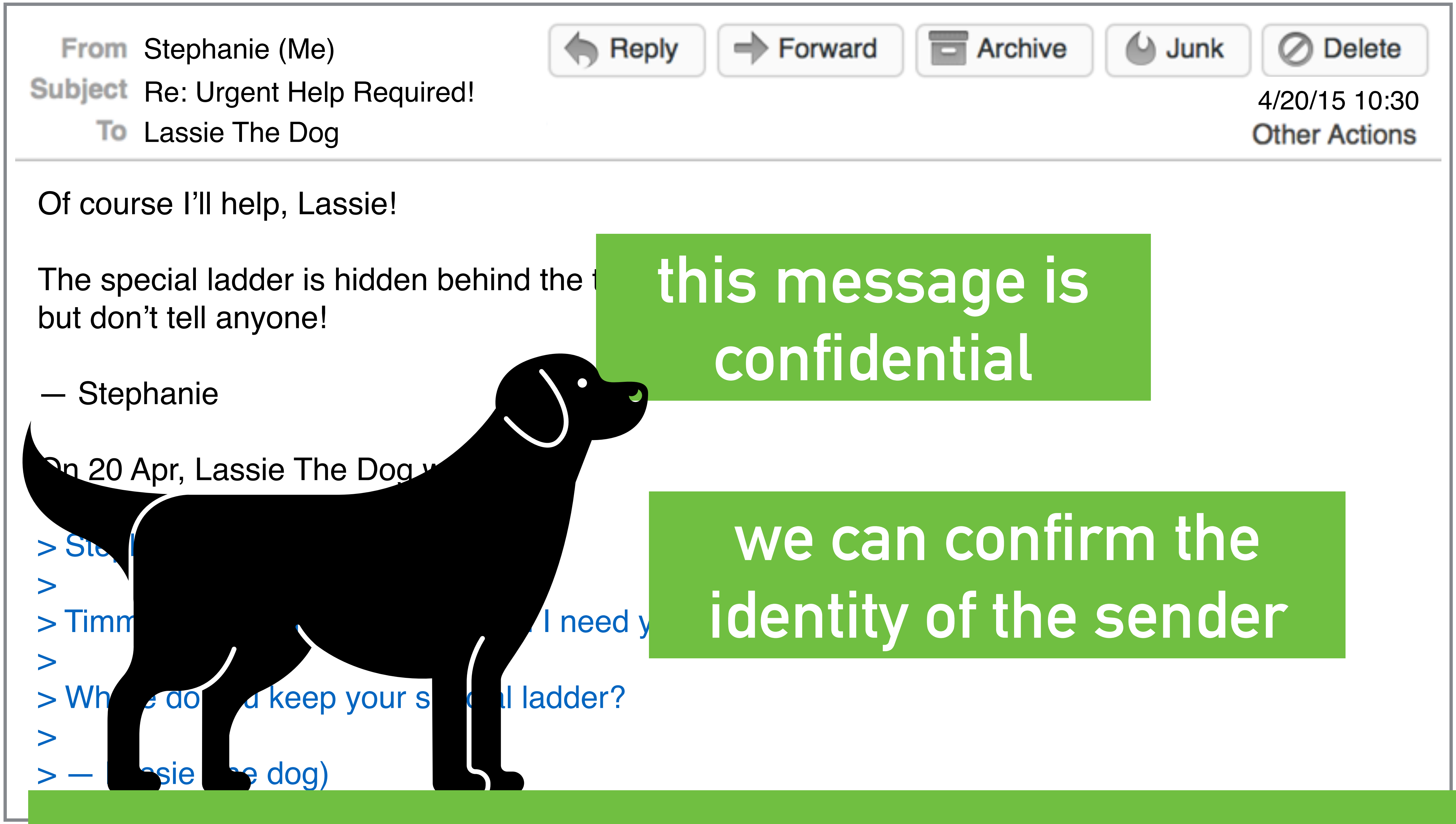
> Stephanie!
>
> Timmy has fallen down a well and I need y
>
> Where do you keep your special ladder?
>
> — Lassie (the dog)

is this message confidential?

is the Lassie the true sender?

did the message change in transit?

with PGP…



From Stephanie (Me)
Subject Re: Urgent Help Required!
To Lassie The Dog

4/20/15 10:30

Of course I'll help, Lassie!

The special ladder is hidden behind the t
but don't tell anyone!

— Stephanie

n 20 Apr, Lassie The Dog w

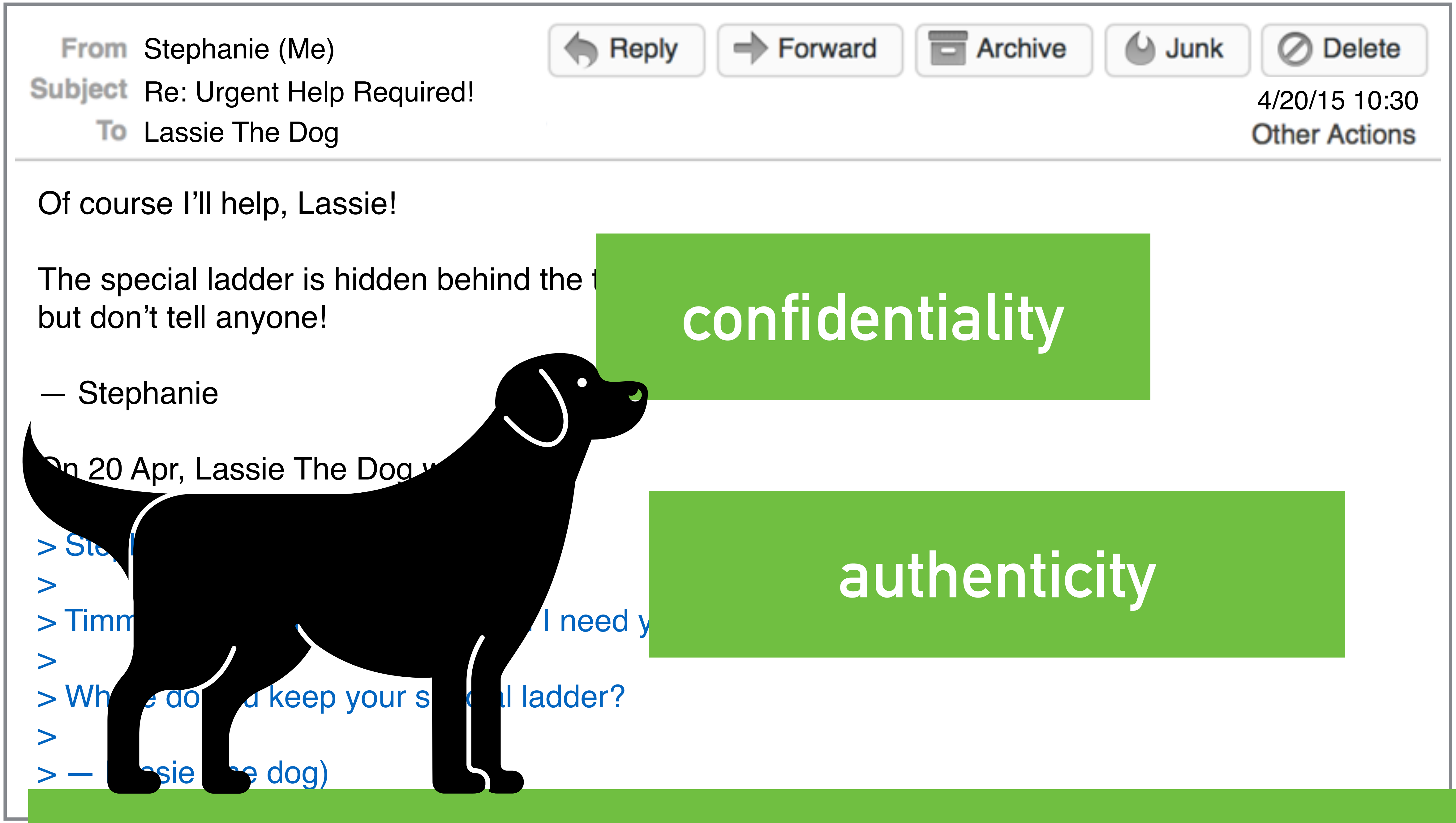
> Ste
>
> Timm I need y
>
> Wh e do u keep your s l ladder?
>
> — sie e dog)

this message is confidential

we can confirm the identity of the sender

we know if the message has been tampered with

with PGP…



From Stephanie (Me)
Subject Re: Urgent Help Required!
To Lassie The Dog

4/20/15 10:30

Of course I'll help, Lassie!

The special ladder is hidden behind the t
but don't tell anyone!

— Stephanie

On 20 Apr, Lassie The Dog w

> Ste
>
> Timm I need y
>
> Wh e do u keep your s al ladder?
>
> — sie e dog)

confidentiality

authenticity

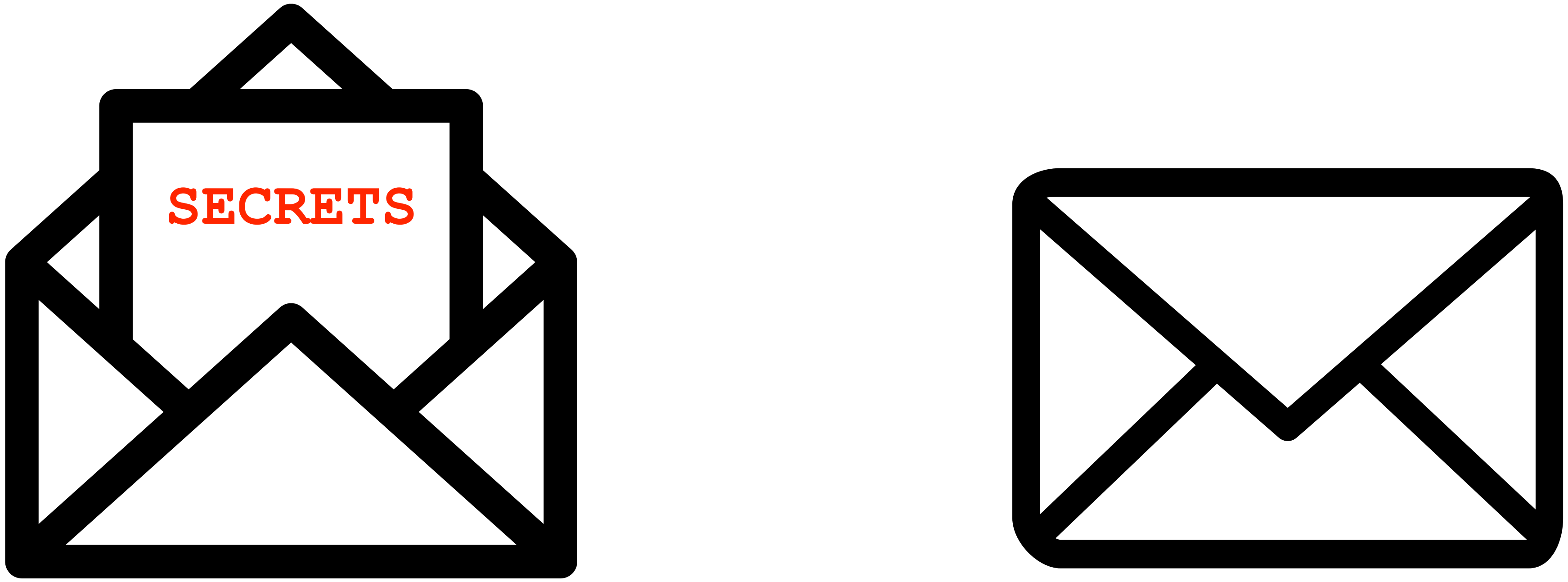
integrity

confidentiality

(preventing information disclosure to an unauthorized third party)

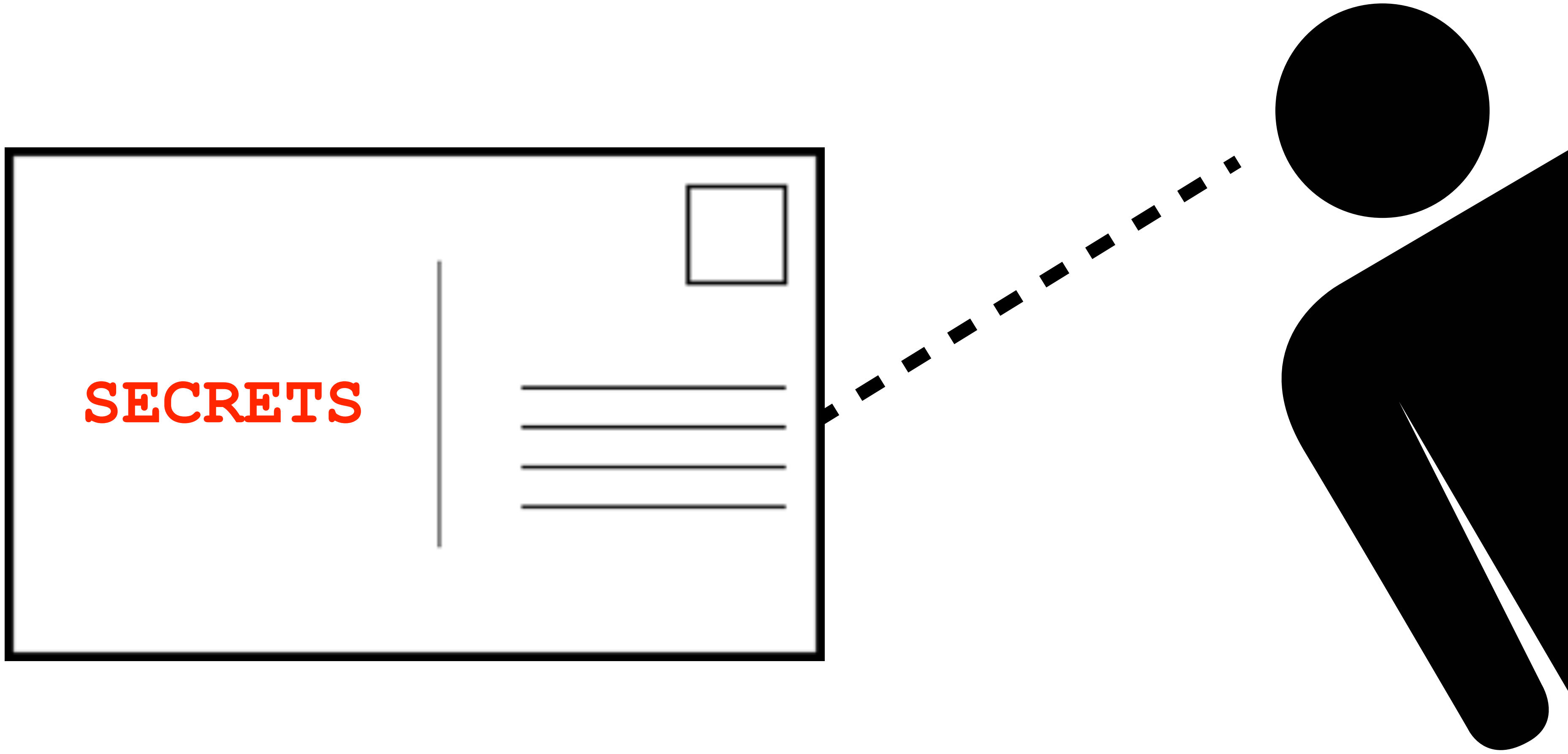
→ encrypt messages

a problem with email



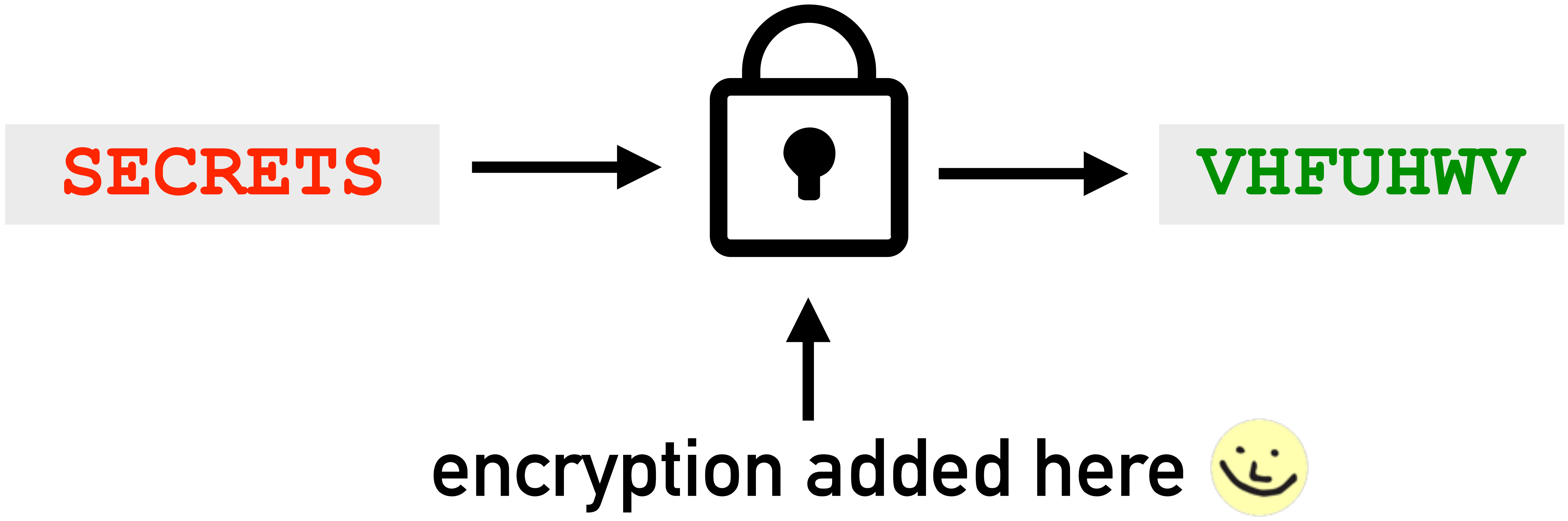
what you expect

a problem with email



what you get

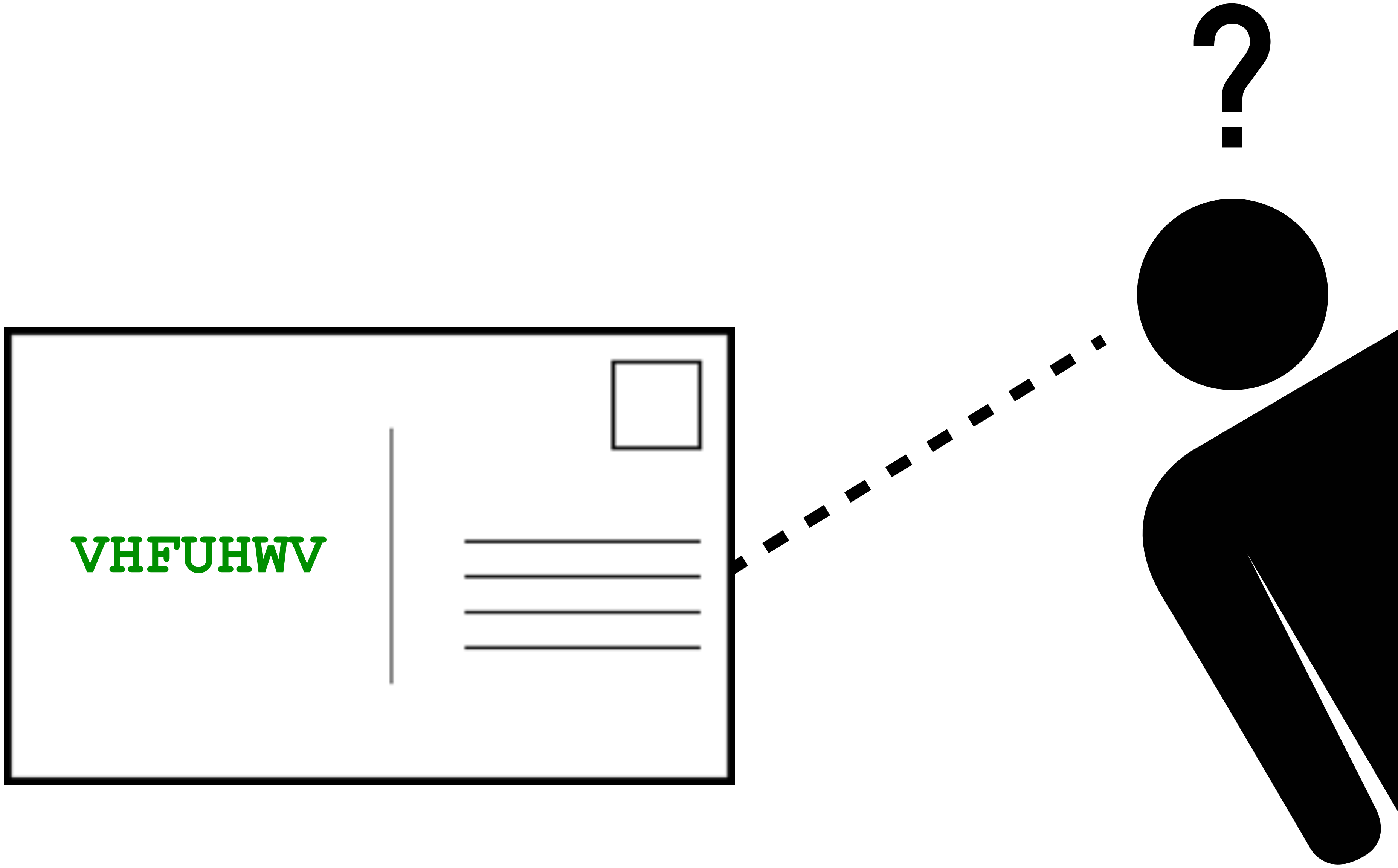
encryption to the rescue



SECRETS

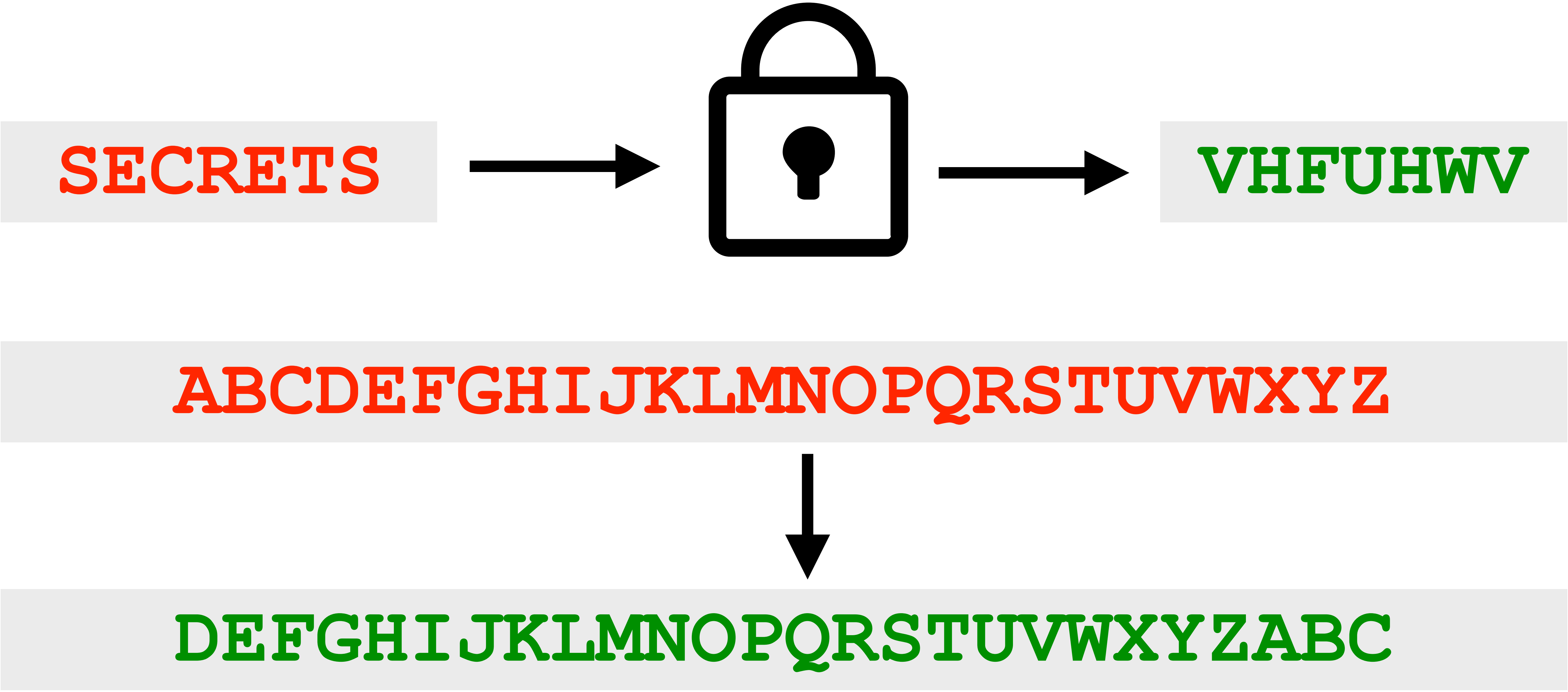
VHFUHWV

encryption added here


VHFUHWV
?

(shift/Caesar cipher)

a simple example



SECRETS → VHFUHWV

ABCDEFGHIJKLMNOPQRSTUVWXYZ

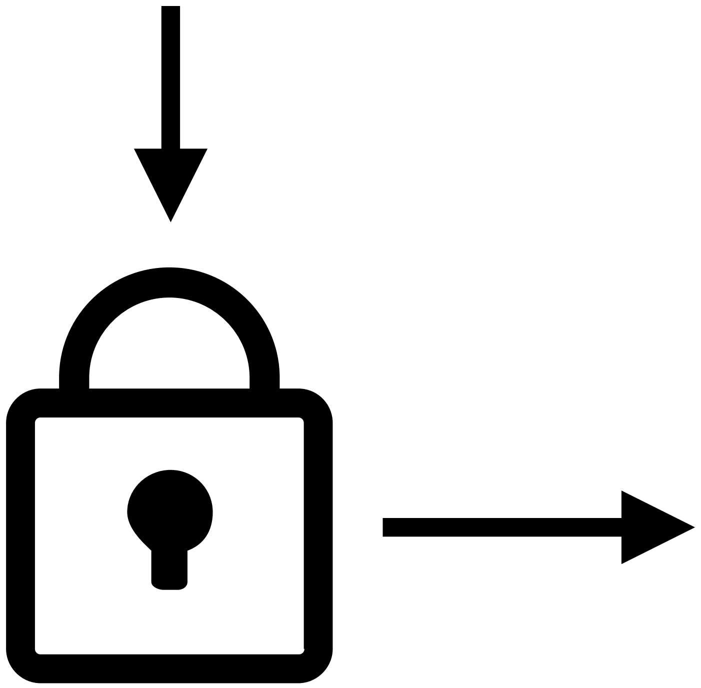
↓

DEFGHIJKLMNOPQRSTUVWXYZABC

Both parties must know the key (+3 letters)

a less simple example

SECRETS

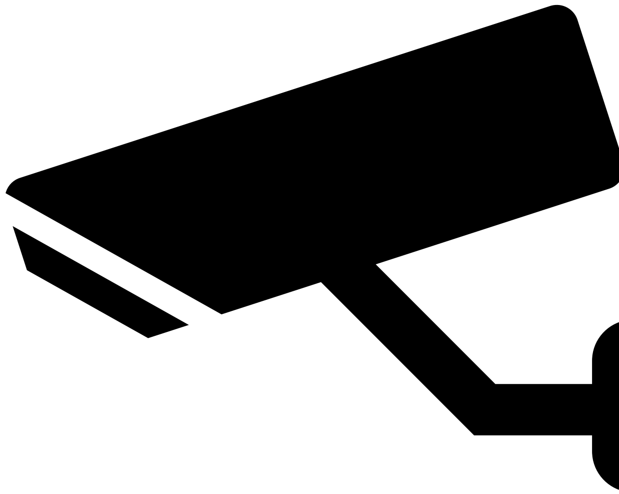


```
-----BEGIN PGP MESSAGE-----

hQIMA8zmAMTbigv/AQ//fZff4m+QocNXVnk+6ryvzran/ocuugo+zvvjfUzlle/B
lfHzI8tDkE/XXEdt3rKUywtwngGKvNp8f17OdJphZDlrqLYQwWyp6hAbBOZoO4V/
qn1cOUv47uXSM3SxORHj/JLCQASrTzMmd7MIBwMUwZNrrUPuJy3DPtdiBaFautO8
/D5RVJZpa81iUPJoOUAPB3LCVk1E+S8Xx3aPVgP1wHcskPWC3xGDdlg1rKT2PAc5
3vhps5OkeeUTrSboR2PdvEbswzxNscsDBesXv0I3r3EVZRqLrFp85ZYkSEVtqryH
jvYXtNHlPdRkPAqnQ/gwOguK4wjdc8B5/JJK/VoNevCwAnejZyECqIUfW9nkrw60
hAFZN5uhAqJwkkbRVrfnmJGZSqZqqkzboebxqw8v1UF7drmvgM5QdQVAXEHrV0HO
t5CRPLjxDVZh5o3eP5pCDh9JG/U43pEK84LV09gBbW/gljwMk7M6KAtzHMRBffoE
/W7wRgeIAkXLJjvb90wOsDAY3q5CpLKw4/+gZKl6rAdmSSJOJ0HZjh9A9ksrjmog
3VI+k0VMcBZqBW/yL2iXv4Ed2v/y1GRLepfnAuE83n+H4yrj+R2nPPWwzsAvc1de
8wppzcYJCSDjyOgZEIYRUTLtqibp80eaS1u82XwjaUOCyQ7us8/A2rTT0afsgGLS
TgHmJOnn7tIkrptOPMTVUpgIs1vxkDDAWD0dIZG+W+dZFfuNibo3oOWurFiJJapV
IMIY/CXRr7kL0t/xXdjpeRsj5nRlFZinOxCMNzVv+A==
=l6hy
-----END PGP MESSAGE-----
```

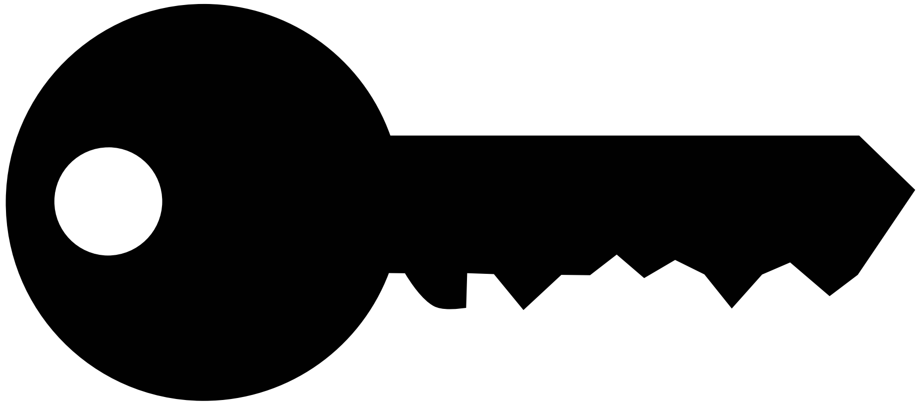
Without the right key,
this is extremely difficult to decrypt.

share a key,
communicate!

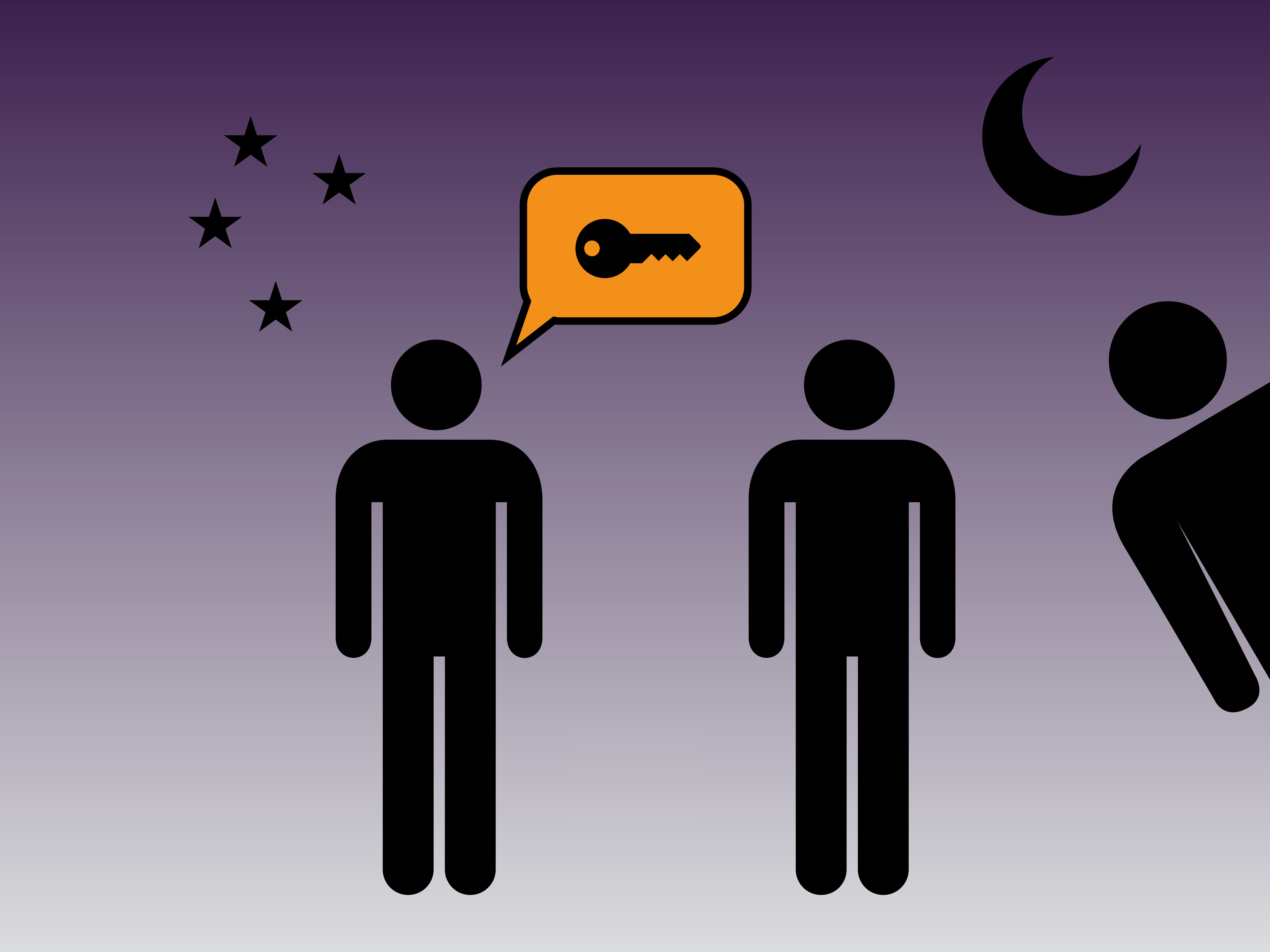
problem solved...?



unfortunately...



sharing secret information is hard



PGP uses public key cryptography

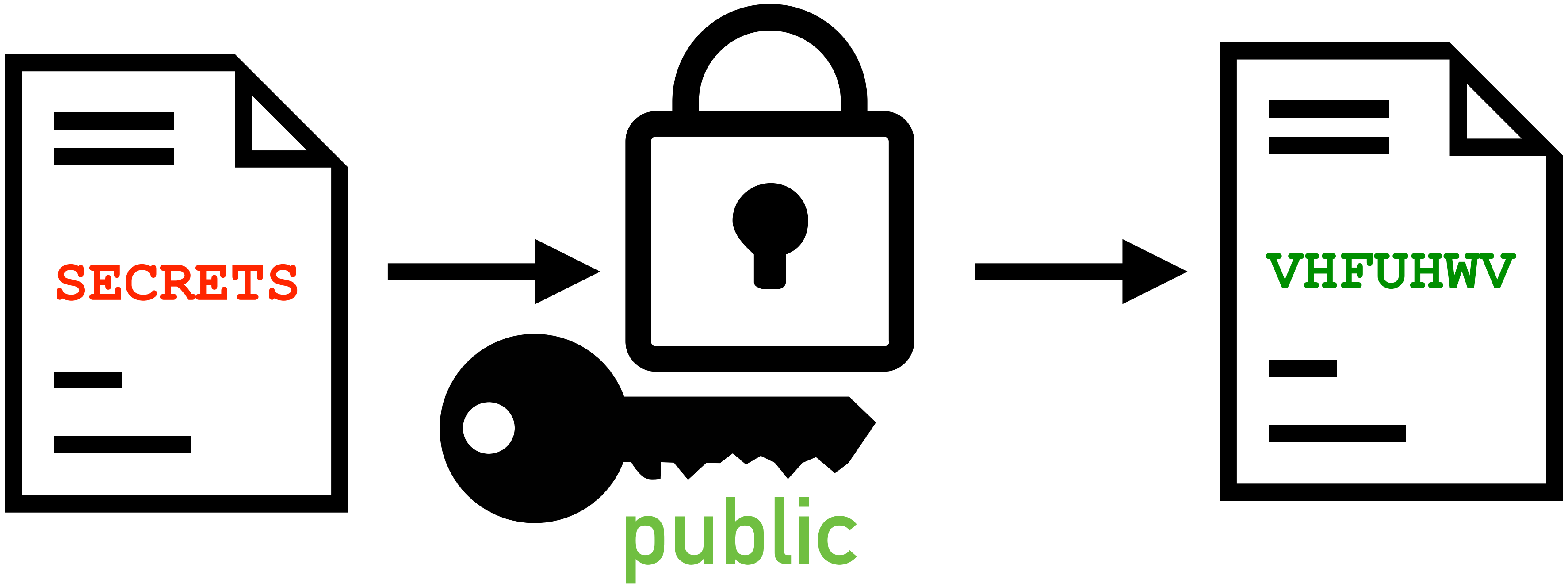
private key

public key

not secret,
easy to share!

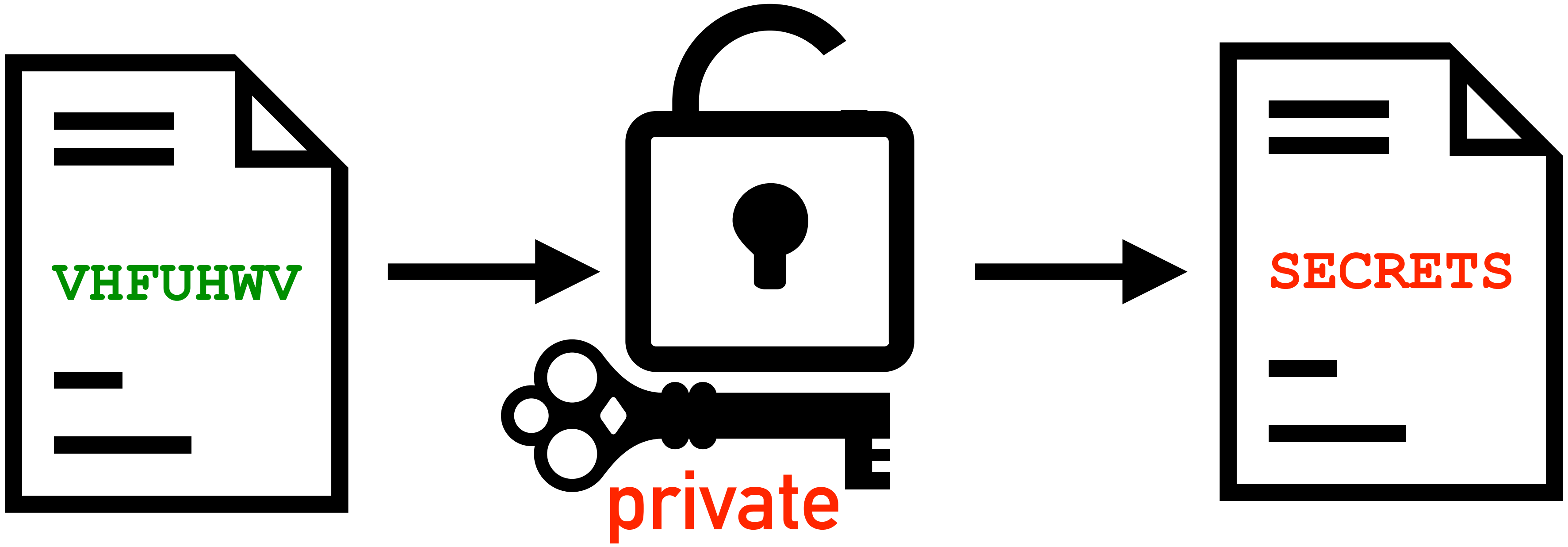
PGP uses public key cryptography

If someone knows my public key,
they can encrypt a message only I can read.



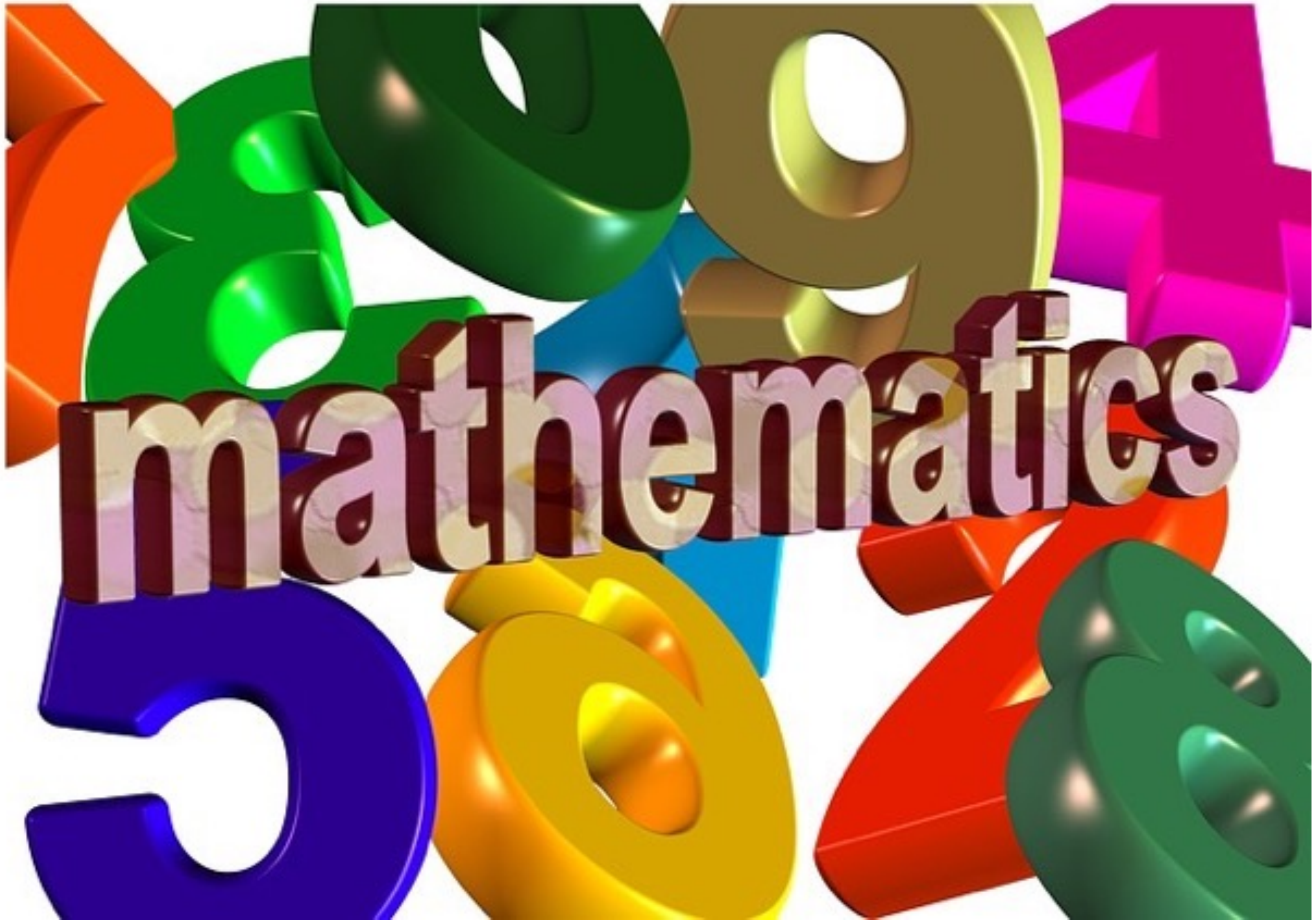
PGP uses public key cryptography

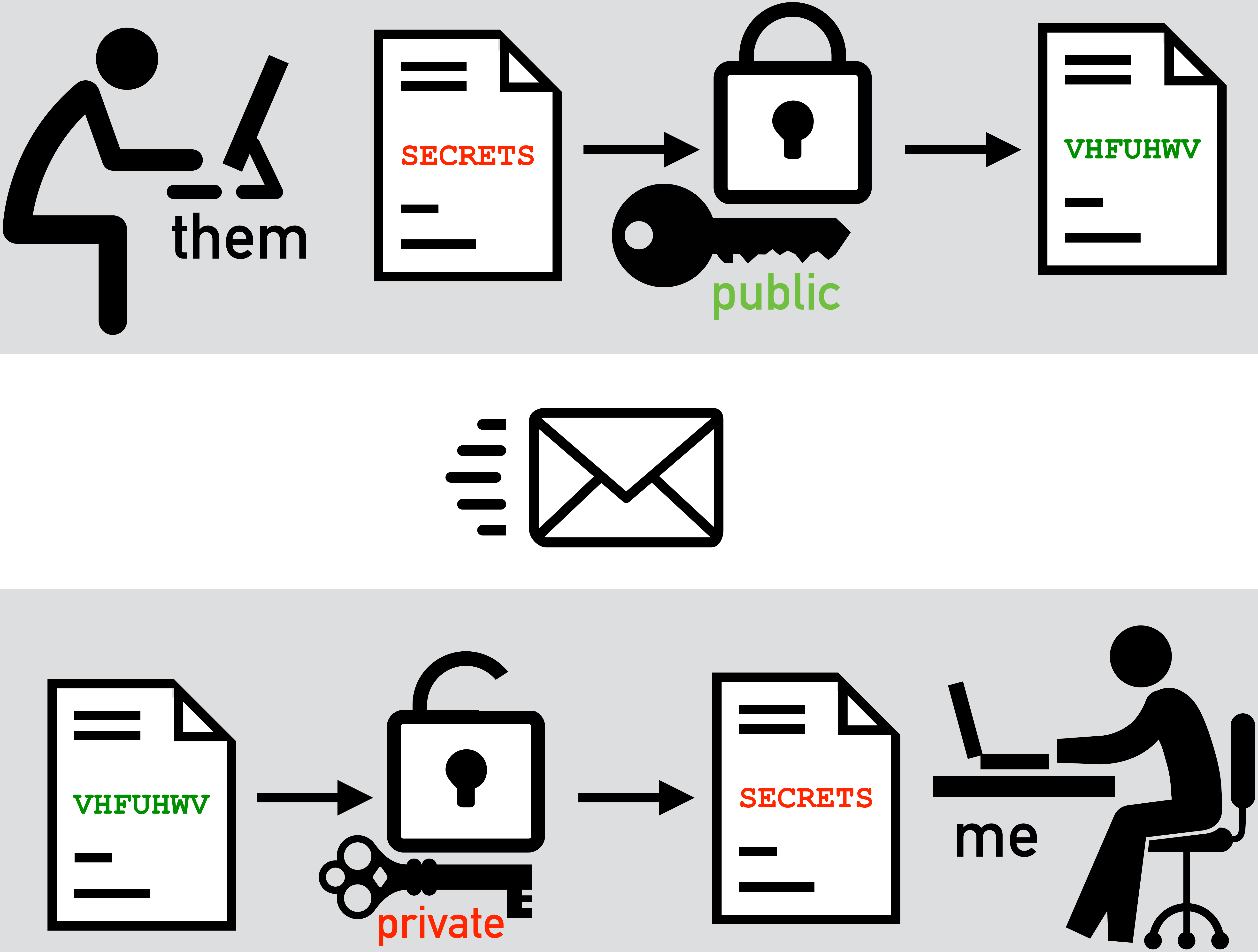
If I know my private key,
I can decrypt the message.



(anyone with my private key can decrypt the message!)

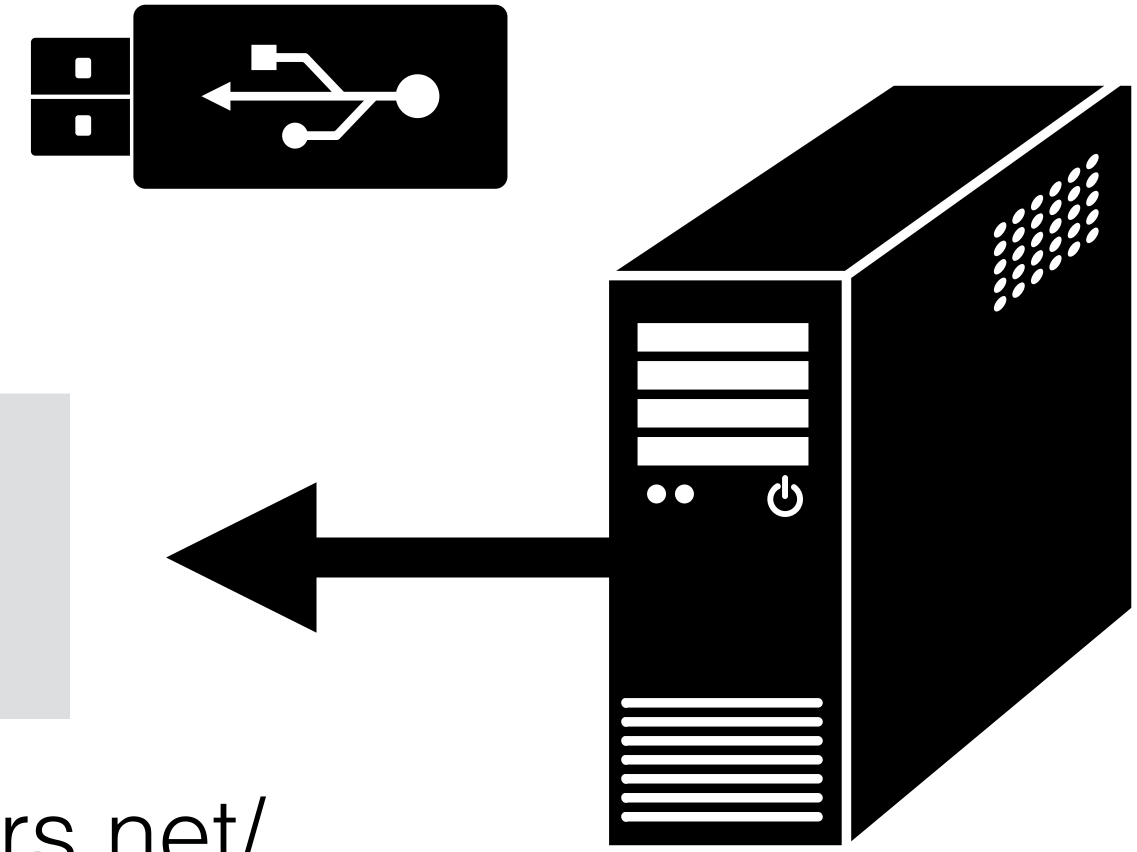
how is this possible?!




them
SECRETS
public
VHFUHWV
VHFUHWV
private
SECRETS
me

how does someone get my public key?

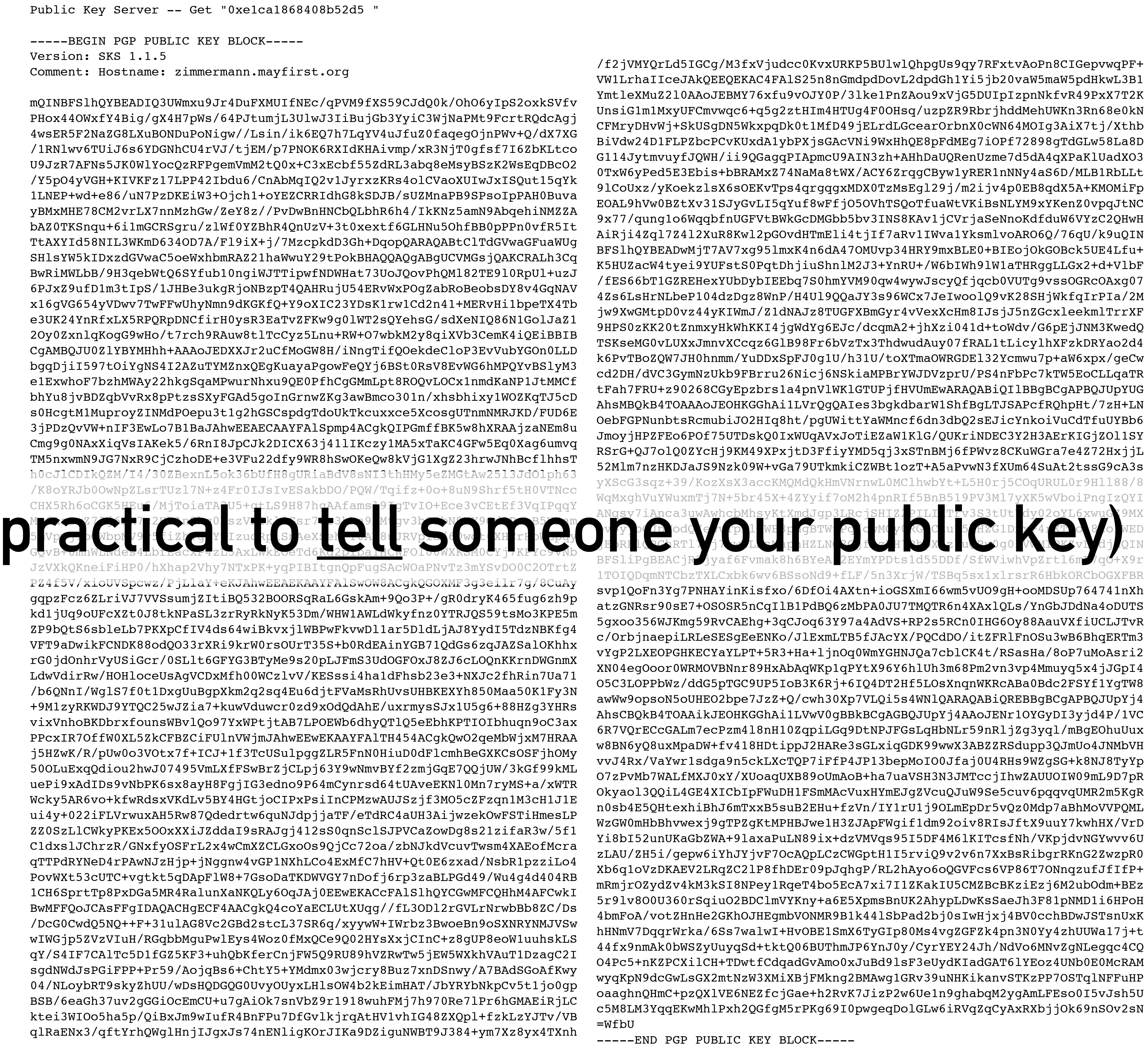
I give it to them



They download it from a key server

e.g. https://sks-keyservers.net/

(usually done through the PGP program)



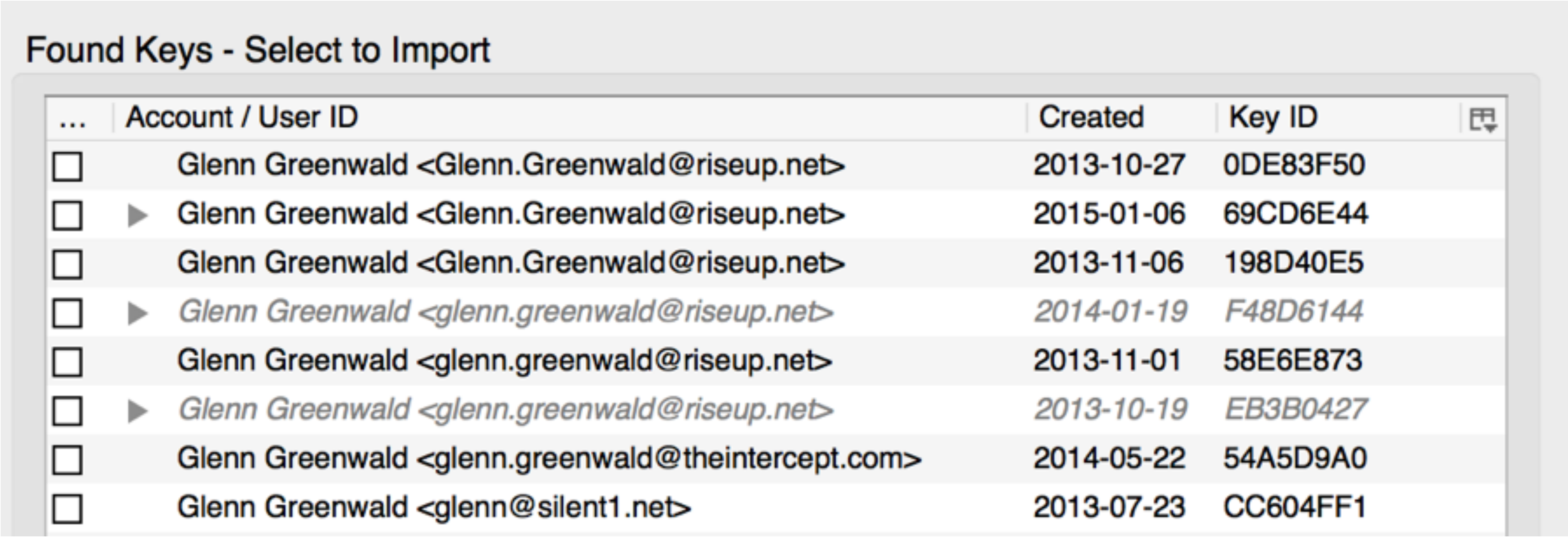
Public Key Server -- Get "0xe1ca1868408b52d5 "

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.5
Comment: Hostname: zimmermann.mayfirst.org

mQINBFSlhQYBEADIQ3UWmxu9Jr4DuFXMUIfNEc/qPVM9fXS59CJdQ0k/OhO6yIpS2oxkSVfv
PHox44OWxfY4Big/gX4H7pWs/64PJtumjL3UlwJ3IiBujGb3YyiC3WjNaPMt9FcrtRQdcAgj
4wsER5F2NaZG8LXuBONDuPoNigw//Lsin/ik6EQ7h7LqYV4uJfuZ0faqegOjnPWv+Q/dX7XG
/1RNlwv6TUiJ6s6YDGNhCU4rVJ/tjEM/p7PNOK6RXIdKHAivmp/xR3NjT0gfsf7I6ZbKLtco
U9JzR7AFNs5JK0WlYocQzRFPgemVmM2tQ0x+C3xEcbf55ZdRL3abq8eMsyBSzK2WsEqDBcO2
/Y5pO4yVGH+KIVKFz17LPP42Ibdu6/CnAbMqIQ2v1JyrxzKRs4olCVaoXUIwJxISQut15qYk
1LNEP+wd+e86/uN7PzDKEiW3+Ojch1+oYEZCRRIdhG8kSDJB/sUZMnaPB9SPsoIpPAH0Buva
yBMxMHE78CM2vrLX7nnMzhGw/ZeY8z//PvDwBnHNCbQLbhR6h4/IkKNz5amN9AbqehiNMZZA
bAZ0TKSnqu+6i1mGCRSgru/zlWf0YZBhR4QnUzV+3t0xextf6GLHNu5OhfBB0pPPn0vfR5It
TtAXYId58NIL3WKmD634OD7A/Fl9iX+j/7MzcpkdD3Gh+DqopQARAQABtClTdGVwaGFuaWUg
SHlsYW5kIDxzdGVwaC5oeWxhbmRAZ21haWwuY29tPokBHAQQAQgABgUCVMGsjQAKCRALh3Cq
BwRiMWLbB/9H3qebWtQ6SYfub10ngiWJTTipwfNDWHat73UoJQovPhQMl82TE9l0RpUl+uzJ
6PJxZ9ufD1m3tIpS/1JHBe3ukgRjoNBzpT4QAHRujU54ERvWxPOgZabRoBeobsDY8v4GqNAV
x16gVG654yVDwv7TwFFwUhyNmn9dKGKfQ+Y9oXIC23YDsK1rw1Cd2n41+MERvHi1bpeTX4Tb
e3UK24YnRfxLX5RPQRpDNCfirH0ysR3EaTvZFKw9g0lWT2sQYehsG/sdXeNIQ86N1GolJaZ1
2Oy0ZxnlqKogG9wHo/t7rch9RAuw8tlTcCyz5Lnu+RW+O7wbkM2y8qiXVb3CemK4iQEiBBIB
CgAMBQJU0ZlYBYMHhh+AAAoJEDXXJr2uCfMoGW8H/iNngTifQOekdeCloP3EvVubYGOn0LLD
bgqDjiI597tOiYgNS4I2AZuTYMZnxQEgKuayaPgowFeQYj6BSt0RsV8EvWG6hMPQYvBSlyM3
e1ExwhoF7bzhMWAy22hkgSqaMPwurNhxu9QE0PfhCgGMmLpt8ROQvLOCx1nmdKaNP1JtMMCf
bhYu8jvBDZqbVvRx8pPtzsSXyFGAd5goInGrnwZKg3awBmco301n/xhsbhixy1WOZKqTJ5cD
s0HcgtM1MuproyZINMdPOepu3t1g2hGSCspdgTdoUkTkcuxxce5XcosgUTnmNMRJKD/FUD6E
3jPDzQvVW+nIF3EwLo7B1BaJAhwEEAECAAYFAlSpmp4ACgkQIPGmffBK5w8hXRAAjzaNEm8u
Cmg9g0NAxXiqVsIAKek5/6RnI8JpCJk2DICX63j41lIKczy1MA5xTaKC4GFw5Eq0Xag6umvq
TM5nxwmN9JG7NxR9CjCzhoDE+e3VFu22dfy9WR8hSwOKeQw8kVjG1XgZ23hrwJNhBcflhhsT
h0cJlCDIkQZM/I4/30ZBexnL5ok36bUfH8gURiaBdV8sNI3thHMy5eZMGtAw25l3JdOlph63
/K8oYRJb0OwNpZLsrTUzl7N+z4Fr0IJsIvESakbDO/PQW/Tqifz+0o+8uN9Shrf5tH0VTNcc
CHX5Rh6oCGK5HEu[illegible]/MjToiaTA[illegible]U5+[illegible]tLS9H87h[illegible]AAfams[illegible]9[illegible]gTvIO+Ece3vCEtEf3VqIPqqY
[illegible]
[illegible]
GQvB+6mnWLNdes4LbfEacxP4zL5AxLwkEOeTd6Kq2pIbaIHCWFOl00WXKSM0CYj7KPYc9VNb
JzVXkQKneiFiHP0/hXhap2Vhy7NTxPK+yqPIBItgnQpFugSAcWOaPNvTz3mYSvDO0C2OTrtZ
PZ4f5V/xioUVSpcwz/PjLlaY+eKJAhwEEAEKAAYFAlSwOW8ACgkQGOXMF3g3eilr7g/8CuAy
gqpzFcz6ZLriVJ7VVSsumjZItiBQ532BOORSqRaL6GskAm+9Qo3P+/gR0dryK465fug6zh9p
kd1jUq9oUFcXZt0J8tkNPaSL3zrRyRkNyK53Dm/WHW1AWLdWkyfnz0YTRJQS59tsMo3KPE5m
ZP9bQtS6sbleLb7PKXpCfIV4ds64wiBkvxjlWBPwFkvwDl1ar5DldLjAJ8YydI5TdzNBKfg4
VFT9aDwikFCNDK88odQO33rXRi9krW0rsOUrT35S+b0RdEAinYGB71QdGs6zqJAZSalOKhhx
rG0jdOnhrVyUSiGcr/0SLlt6GFYG3BTyMe9s20pLJFmS3UdOGFOxJ8ZJ6cLOQnKKrnDWGnmX
LdwVdirRw/HOHloceUsAgVCDxMfh00WCzlvV/KESssi4ha1dFhsb23e3+NXJc2fhRin7Ua71
/b6QNnI/WglS7f0t1DxgUuBgpXkm2q2sq4Eu6djtFVaMsRhUvsUHBKEXYh850Maa50K1Fy3N
+9M1zyRKWDJ9YTQC25wJZia7+kuwVduwcr0zd9xOdQdAhE/uxrmysSJx1U5g6+88HZg3YHRs
vixVnhoBKDbrxfounsWBvlQo97YxWPtjtAB7LPOEWb6dhyQTlQ5eEbhKPTIOIbhuqn9oC3ax
PPcxIR7OffW0XL5ZkCFBZCiFUlnVWjmJAhwEEwEKAAYFAlTH454ACgkQwO2qeMbWjxM7HRAA
j5HZwK/R/pUw0o3VOtx7f+ICJ+1f3TcUSulpggZLR5FnN0HiuD0dFlcmhBeGXKCsOSFjhOMy
50OLuExqQdiou2hwJ07495VmLXfFSwBrZjCLpj63Y9wNmvBYf2zmjGqE7QQjUW/3kGf99kML
uePi9xAdIDs9vNbPK6sx8ayH8FgjIG3edno9P64mCynrsd64tUAveEKNl0Mn7ryMS+a/xWTR
Wcky5AR6vo+kfwRdsxVKdLv5BY4HGtjoCIPxPsiInCPMzwAUJSzjf3MO5cZFzqn1M3cH1J1E
ui4y+022iFLVrwuxAH5Rw87Qdedrtw6quNJdpjjaTF/eTdRC4aUH3AijwzekOwFSTiHmesLP
ZZ0SzLlCWkyPKEx5OOxXXiJZddaI9sRAJgj412sS0qnSclSJPVCaZowDg8s21zifaR3w/5f1
C1dxslJChrzR/GNxfyOSFrL2x4wCmXZCLGxoOs9QjCc72oa/zbNJkdVcuvTwsm4XAEofMcra
qTTPdRYNeD4rPAwNJzHjp+jNggnw4vGP1NXhLCo4ExMfC7hHV+Qt0E6zxad/NsbR1pzziLo4
PovWXt53cUTC+vgtkt5qDApFlW8+7GsoDaTKDWVGY7nDofj6rp3zaBLPGd49/Wu4g4d404RB
1CH6SprtTp8PxDGa5MR4RalunXaNKQLy6OqJAj0EEwEKACcFAlSlhQYCGwMFCQHhM4AFCwkI
BwMFFQoJCAsFFgIDAQACHgECF4AACgkQ4coYaECLUtXUqg//fL3ODl2rGVLrNrwbBb8ZC/Ds
/DcG0CwdQ5NQ++F+31ulAG8Vc2GBd2stcL37SR6q/xyywW+IWrbz3BwoeBn9oSXNRYNMJVSw
wIWGjp5ZVzVIuH/RGqbbMguPwlEys4Woz0fMxQCe9Q02HYsXxjCInC+z8gUP8eoW1uuhskLS
qY/S4IF7CAlTc5D1fGZ5KF3+uhQbKferCnjFW5Q9RU89hVZRwTw5jEW5WXkhVAuT1DzagC2I
sgdNWdJsPGiFPP+Pr59/AojqBs6+ChtY5+YMdmx03wjcry8Buz7xnDSnwy/A7BAdSGoAfKwy
04/NLoybRT9skyZhUU/wDsHQDGQG0UvyOUyxLHlsOW4b2kEimHAT/JbYRYbNkpCv5t1jo0gp
BSB/6eaGh37uv2gGGiOcEmCU+u7gAiOk7snVbZ9r1918wuhFMj7h970Re7lPr6hGMAEiRjLC
ktei3WIOo5ha5p/QiBxJm9wIufR4BnFPu7DfGvlkjrqAtHV1vhIG48ZXQpl+fzkLzYJTv/VB
qlRaENx3/qftYrhQWglHnjIJgxJs74nENligKOrJIKa9DZiguNWBT9J384+ym7Xz8yx4TXnh
/f2jVMYQrLd5IGCg/M3fxVjudcc0KvxURKP5BUlwlQhpgUs9qy7RFxtvAoPn8CIGepvwqPF+
VW1LrhaIIceJAkQEEQEKAC4FAlS25n8nGmdpdDovL2dpdGh1Yi5jb20vaW5maW5pdHkwL3B1
YmtleXMuZ2l0AAoJEBMY76xfu9vOJY0P/3lke1PnZAou9xVjG5DUIpIzpnNkfvR49PxX7T2K
UnsiG1m1MxyUFCmvwqc6+q5g2ztHIm4HTUg4F0OHsq/uzpZR9RbrjhddMehUWKn3Rn68e0kN
CFMryDHvWj+SkUSgDN5WkxpqDk0t1MfD49jELrdLGcearOrbnX0cWN64MOIg3AiX7tj/Xthb
BiVdw24D1FLPZbcPCvKUxdA1ybPXjsGAcVNi9WxHhQE8pFdMEg7iOPf72898gTdGLw58La8D
Gl14JytmvuyfJQWH/ii9QGagqPIApmcU9AIN3zh+AHhDaUQRenUzme7d5dA4qXPaKlUadXO3
0TxW6yPed5E3Ebis+bBRAMxZ74NaMa8tWX/ACY6ZrqgCByw1yRER1nNNy4aS6D/MLB1RbLLt
9lCoUxz/yKoekzlsX6sOEKvTps4qrgqgxMDX0TzMsEgl29j/m2ijv4p0EB8qdX5A+KMOMiFp
EOAL9hVw0BZtXv31SJyGvLI5qYuf8wFfjO5OVhTSQoTfuaWtVKiBsNLYM9xYKenZ0vpqJtNC
9x77/qung1o6WqqbfnUGFVtBWkGcDMGbb5bv3INS8KAv1jCVrjaSeNnoKdfduW6VYzC2QHwH
AiRji4Zql7Z4l2XuR8Kwl2pGOvdHTmEli4tjIf7aRv1IWva1YksmlvoARO6Q/76qU/k9uQIN
BFSlhQYBEADwMjT7AV7xg95lmxK4n6dA47OMUvp34HRY9mxBLE0+BIEojOkGOBck5UE4Lfu+
K5HUZacW4tyei9YUFstS0PqtDhjiuShnlM2J3+YnRU+/W6bIWh9lW1aTHRggLLGx2+d+VlbF
/fES66bT1GZREHexYUbDybIEEbq7S0hmYVM90qw4wywJscyQfjqcb0VUTg9vssOGRcOAxg07
4Zs6LsHrNLbeP104dzDgz8WnP/H4Ul9QQaJY3s96WCx7JeIwoolQ9vK28SHjWkfqIrPIa/2M
jw9XwGMtpD0vz44yKIWmJ/Z1dNAJz8TUGFXBmGyr4vVexXcHm8IJsjJ5nZGcxleekmlTrrXF
9HPS0zKK20tZnmxyHkWhKKI4jgWdYg6EJc/dcqmA2+jhXzi041d+toWdv/G6pEjJNM3KwedQ
TSKseMG0vLUXxJmnvXCcqz6GlB98Fr6bVzTx3ThdwudAuy07fRAL1tLicylhXFzkDRYao2d4
k6PvTBoZQW7JH0hnmm/YuDDxSpFJ0g1U/h31U/toXTmaOWRGDEl32Ycmwu7p+aW6xpx/geCw
cd2DH/dVC3GymNzUkb9FBrru26Nicj6NSkiaMPBrYWJDVzprU/PS4nFbPc7kTW5EoCLLqaTR
tFah7FRU+z90268CGyEpzbrs1a4pnVlWKlGTUPjfHVUmEwARAQABiQIlBBgBCgAPBQJUpYUG
AhsMBQkB4TOAAAoJEOHKGGhAi1LVrQgQAIes3bgkdbarW1ShfBgLTJSAPcfRQhpHt/7zH+LN
OebFGPNunbtsRcmubiJO2HIq8ht/pgUWittYaWMncf6dn3dbQ2sEJicYnkoiVuCdTfuUYBb6
JmoyjHPZFEo6POf75UTDskQ0IxWUqAVxJoTiEZaW1KlG/QUKriNDEC3Y2H3AErKIGjZOl1SY
RSrG+QJ7olQ0ZYcHj9KM49XPxjtD3FfiyYMD5qj3xSTnBMj6fPWvz8CKuWGra7e4Z72HxjjL
52Mlm7nzHKDJaJS9Nzk09W+vGa79UTkmkiCZWBt1ozT+A5aPvwN3fXUm64SuAt2tssG9cA3s
yXScG3sqz+39/KozXsX3accKMQMdQkHmVNrnwL0MClhwbYt+L5H0rj5COqURUL0r9Hl188/8
WqMxghVuYWuxmTj7N+5br45X+4ZYyif7oM2h4pnRIf5BnB519PV3Ml7yXK5wVboiPngIzQYI
ANqsy7iAnca3uwAwhcbMhsyKtXmdJgp3LRcjSHIZ[illegible]PILI[illegible]Tv3S3tUt[illegible]dy02oYL6xwu[illegible]9MX
[illegible]WED
[illegible]QIN
BFSliPgBEACjR[illegible]jyaf6Fvmak8h6BYeA[illegible]2EYmYPDts1d55DDf/SfWViwhVpZrtl6m[illegible]/qO+X9r
1TOIQDqmNTCbzTXLCxbk6wv6BSsoNd9+fLF/5n3XrjW/TSBq5sx1xlrsrR6HbkORCbOGXFBR
svp1QoFn3Yg7PNHAYinKisfxo/6DfOi4AXtn+ioGSXmI66wm5vUO9gH+ooMDSUp764741nXh
atzGNRsr90sE7+OSOSR5nCqIlB1PdBQ6zMbPA0JU7TMQTR6n4XAxlQLs/YnGbJDdNa4oDUTS
5gxoo356WJKmg59RvCAEhg+3qCJoq63Y97a4AdVS+RP2s5RCn0IHG6Oy88AauVXfiUCLJTvR
c/OrbjnaepiLRLeSESgEeENKo/JlExmLTB5fJAcYX/PQCdDO/itZFRlFnOSu3wB6BhqERTm3
vYgP2LXEOPGHKECYaYLPT+5R3+Ha+ljnOq0WmYGHNJQa7cblCK4t/RSasHa/8oP7uMoAsri2
XN04egOoor0WRMOVBNnr89HxAbAqWKp1qPYtX96Y6hlUh3m68Pm2vn3vp4Mmuyq5x4jJGpI4
O5C3LOPPbWz/ddG5pTGC9UP5IoB3K6Rj+6IQ4DT2Hf5LOsXnqnWKRcABa0Bdc2FSYf1YgTW8
awWw9opsoN5oUHEO2bpe7JzZ+Q/cwh30Xp7VLQi5s4WNlQARAQABiQREBBgBCgAPBQJUpYj4
AhsCBQkB4TOAAikJEOHKGGhAi1LVwV0gBBkBCgAGBQJUpYj4AAoJENr1OYGyDI3yjd4P/1VC
6R7VQrECcGALm7ecPzm4l8nH10ZqpiLGq9DtNPJFGsLqHbNLr59nRljZg3yql/mBgEOhuUux
w8BN6yQ8uxMpaDW+fv418HDtippJ2HARe3sGLxiqGDK99wwX3ABZZRSdupp3QJmUo4JNMbVH
vvJ4Rx/VaYwr1sdga9n5ckLXcTQP7iFfP4JP13bepMoIO0Jfaj0U4RHs9WZgSG+k8NJ8TyYp
O7zPvMb7WALfMXJ0xY/XUoaqUXB89oUmAoB+ha7uaVSH3N3JMTccjIhwZAUUOIW09mL9D7pR
Okyaol3QQiL4GE4XICbIpFWuDH1FSmMAcVuxHYmEJgZVcuQJuW9Se5cuv6pqqvqUMR2m5KgR
n0sb4E5QHtexhiBhJ6mTxxB5suB2EHu+fzVn/IY1rU1j9OLmEpDr5vQz0Mdp7aBhMoVVPQML
WzGW0mHbBhvwexj9gTPZgKtMPHBJwe1H3ZJApFWgif1dm92oiv8RIsJftX9uuY7kwhHX/VrD
Yi8bI52unUKaGbZWA+9laxaPuLN89ix+dzVMVqs95I5DF4M6lKITcsfNh/VKpjdvNGYwvv6U
zLAU/ZH5i/gepw6iYhJYjvF7OcAQpLCzCWGptH1I5rviQ9v2v6n7XxBsRibgrRKnG2ZwzpR0
Xb6q1oVzDKAEV2LRqZC2lP8fhDEr09pJqhgP/RL2hAyo6oQGVFcs6VP86T7ONnqzufJfIfP+
mRmjrOZydZv4kM3kSI8NPey1RqeT4bo5EcA7xi7I1ZKakIU5CMZBcBKziEzj6M2ubOdm+BEz
5r9lv8O0U360rSqiuO2BDClmVYKny+a6E5XpmsBnUK2AhypLDwKsSaeJh3F81pNMD1i6HPoH
4bmFoA/votZHnHe2GKhOJHEgmbVONMR9B1k44lSbPad2bj0sIwHjxj4BV0cchBDwJSTsnUxK
hHNmV7DqqrWrka/6Ss7walwI+HvOBE1SmX6TyGIp80Ms4vgZGFZk4pn3N0Yy4zhUUWa17j+t
44fx9nmAk0bWSZyUuyqSd+tktQ06BUThmJP6YnJ0y/CyrYEY24Jh/NdVo6MNvZgNLegqc4CQ
O4Pc5+nKZPCXilCH+TDwtfCdqadGvAmo0xJuBd9lsF3eUydKIadGAT6lYEoz4UNb0E0McRAM
wyqKpN9dcGwLsGX2mtNzW3XMiXBjFMkng2BMAwg1GRv39uNHKikanvSTKzPP7OSTqlNFFuHP
oaaghnQHmC+pzQXlVE6NEZfcjGae+h2RvK7JizP2w6Ue1n9ghabqM2ygAmLFEso0I5vJsh5U
c5M8LM3YqqEKwMhlPxh2QGfgM5rPKg69I0pwgeqDolGLw6iRVqZqCyAxRXbjjOk69nSOv2sN
=WfbU
-----END PGP PUBLIC KEY BLOCK-----
```

(it is not practical to tell someone your public key)

DANGER!

Anyone can upload a key to a key server, claiming to be anyone!



Found Keys - Select to Import

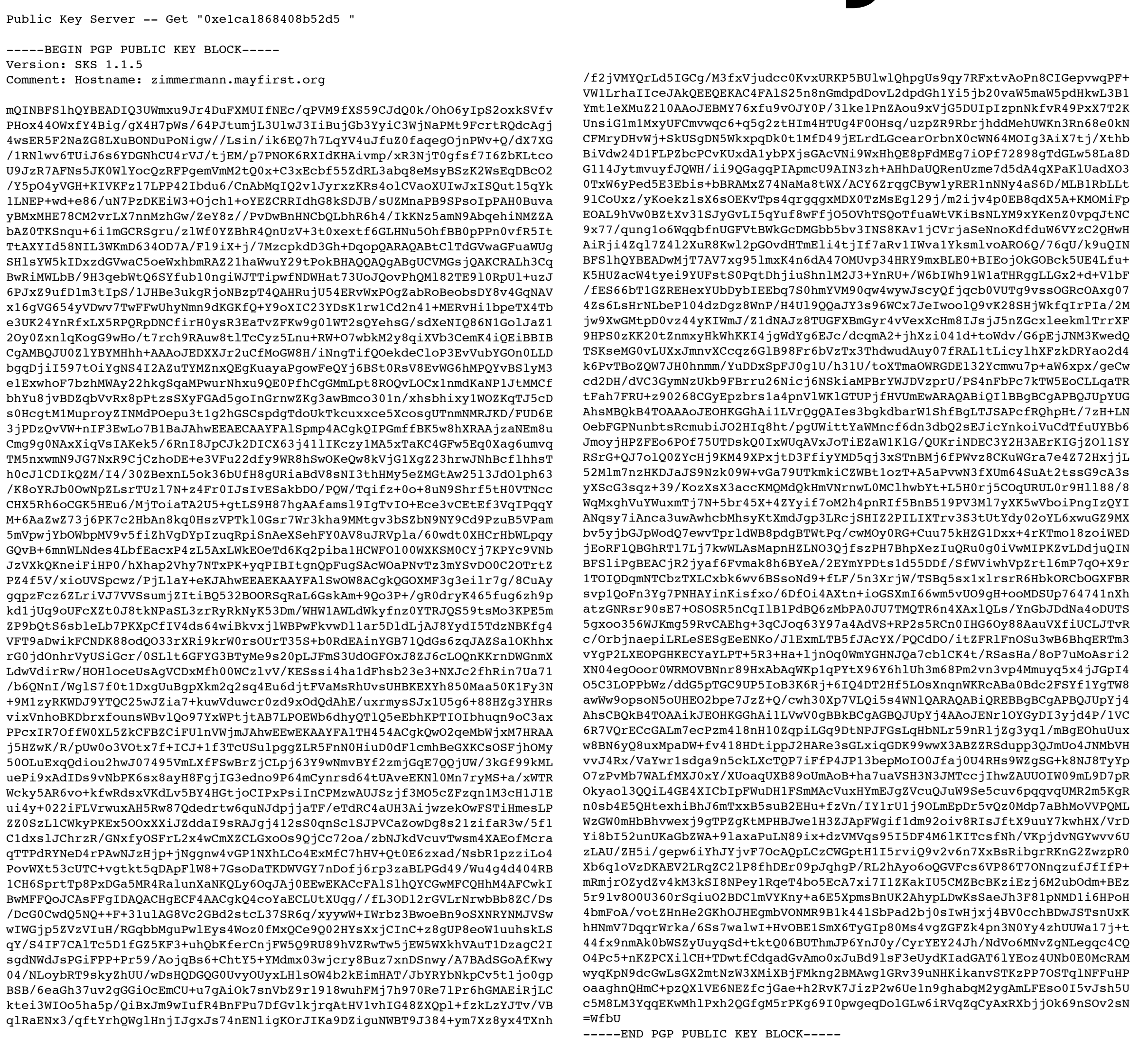
...	Account / User ID	Created	Key ID
□	Glenn Greenwald <Glenn.Greenwald@riseup.net>	2013-10-27	0DE83F50
□ ▶	Glenn Greenwald <Glenn.Greenwald@riseup.net>	2015-01-06	69CD6E44
□	Glenn Greenwald <Glenn.Greenwald@riseup.net>	2013-11-06	198D40E5
□ ▶	*Glenn Greenwald <glenn.greenwald@riseup.net>*	*2014-01-19*	*F48D6144*
□	Glenn Greenwald <glenn.greenwald@riseup.net>	2013-11-01	58E6E873
□ ▶	*Glenn Greenwald <glenn.greenwald@riseup.net>*	*2013-10-19*	*EB3B0427*
□	Glenn Greenwald <glenn.greenwald@theintercept.com>	2014-05-22	54A5D9A0
□	Glenn Greenwald <glenn@silent1.net>	2013-07-23	CC604FF1

Which key belongs to the person I want?

trusting keys

(important for preventing impersonation)

fingerprints are key identifiers



```
Public Key Server -- Get "0xe1ca1868408b52d5 "

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.5
Comment: Hostname: zimmermann.mayfirst.org

mQINBFSlhQYBEADIQ3UWmxu9Jr4DuFXMUIfNEc/qPVM9fXS59CJdQ0k/OhO6yIpS2oxkSVfv
PHox44OWxfY4Big/gX4H7pWs/64PJtumjL3UlwJ3IiBujGb3YyiC3WjNaPMt9FcrtRQdcAgj
4wsER5F2NaZG8LXuBONDuPoNigw//Lsin/ik6EQ7h7LqYV4uJfuZ0faqegOjnPWv+Q/dX7XG
/1RNlwv6TUiJ6s6YDGNhCU4rVJ/tjEM/p7PNOK6RXIdKHAivmp/xR3NjT0gfsf7I6ZbKLtco
U9JzR7AFNs5JK0WlYocQzRFPgemVmM2tQ0x+C3xEcbf55ZdRL3abq8eMsyBSzK2WsEqDBcO2
/Y5pO4yVGH+KIVKFz17LPP42Ibdu6/CnAbMqIQ2v1JyrxzKRs4olCVaoXUIwJxISQut15qYk
1LNEP+wd+e86/uN7PzDKEiW3+Ojch1+oYEZCRRIdhG8kSDJB/sUZMnaPB9SPsoIpPAH0Buva
yBMxMHE78CM2vrLX7nnMzhGw/ZeY8z//PvDwBnHNCbQLbhR6h4/IkKNz5amN9AbqehiNMZZA
bAZ0TKSnqu+6i1mGCRSgru/zlWf0YZBhR4QnUzV+3t0xextf6GLHNu5OhfBB0pPPn0vfR5It
TtAXYId58NIL3WKmD634OD7A/Fl9iX+j/7MzcpkdD3Gh+DqopQARAQABtClTdGVwaGFuaWUg
SHlsYW5kIDxzdGVwaC5oeWxhbmRAZ21haWwuY29tPokBHAQQAQgABgUCVMGsjQAKCRALh3Cq
BwRiMWLbB/9H3qebWtQ6SYfub10ngiWJTTipwfNDWHat73UoJQovPhQMl82TE9l0RpUl+uzJ
6PJxZ9ufD1m3tIpS/1JHBe3ukgRjoNBzpT4QAHRujU54ERvWxPOgZabRoBeobsDY8v4GqNAV
x16gVG654yVDwv7TwFFwUhyNmn9dKGKfQ+Y9oXIC23YDsK1rw1Cd2n41+MERvHi1bpeTX4Tb
e3UK24YnRfxLX5RPQRpDNCfirH0ysR3EaTvZFKw9g0lWT2sQYehsG/sdXeNIQ86N1GolJaZ1
2Oy0ZxnlqKogG9wHo/t7rch9RAuw8tlTcCyz5Lnu+RW+O7wbkM2y8qiXVb3CemK4iQEiBBIB
CgAMBQJU0ZlYBYMHhh+AAAoJEDXXJr2uCfMoGW8H/iNngTifQOekdeCloP3EvVubYGOn0LLD
bgqDjiI597tOiYgNS4I2AZuTYMZnxQEgKuayaPgowFeQYj6BSt0RsV8EvWG6hMPQYvBSlyM3
e1ExwhoF7bzhMWAy22hkgSqaMPwurNhxu9QE0PfhCgGMmLpt8ROQvLOCx1nmdKaNP1JtMMCf
bhYu8jvBDZqbVvRx8pPtzsSXyFGAd5goInGrnwZKg3awBmco301n/xhsbhixy1WOZKqTJ5cD
s0HcgtM1MuproyZINMdPOepu3t1g2hGSCspdgTdoUkTkcuxxce5XcosgUTnmNMRJKD/FUD6E
3jPDzQvVW+nIF3EwLo7B1BaJAhwEEAECAAYFAlSpmp4ACgkQIPGmffBK5w8hXRAAjzaNEm8u
Cmg9g0NAxXiqVsIAKek5/6RnI8JpCJk2DICX63j41lIKczy1MA5xTaKC4GFw5Eq0Xag6umvq
TM5nxwmN9JG7NxR9CjCzhoDE+e3VFu22dfy9WR8hSwOKeQw8kVjG1XgZ23hrwJNhBcflhhsT
h0cJlCDIkQZM/I4/30ZBexnL5ok36bUfH8gURiaBdV8sNI3thHMy5eZMGtAw25l3JdOlph63
/K8oYRJb0OwNpZLsrTUzl7N+z4Fr0IJsIvESakbDO/PQW/Tqifz+0o+8uN9Shrf5tH0VTNcc
CHX5Rh6oCGK5HEu6/MjToiaTA2U5+gtLS9H87hgAAfamsl9IgTvIO+Ece3vCEtEf3VqIPqqY
M+6AaZwZ73j6PK7c2HbAn8kq0HszVPTkl0Gsr7Wr3kha9MMtgv3bSZbN9NY9Cd9PzuB5VPam
5mVpwjYbOWbpMV9v5fiZhVgDYpIzuqRpiSnAeXSehFY0AV8uJRVpla/60wdt0XHCrHbWLpqy
GQvB+6mnWLNdes4LbfEacxP4zL5AxLWkEOeTd6Kq2piba1HCWFOl00WXKSM0CYj7KPYc9VNb
JzVXkQKneiFiHP0/hXhap2Vhy7NTxPK+yqPIBItgnQpFugSAcWOaPNvTz3mYSvDO0C2OTrtZ
PZ4f5V/xioUVSpcwz/PjLlaY+eKJAhwEEAEKAAYFAlSwOW8ACgkQGOXMF3g3eilr7g/8CuAy
gqpzFcz6ZLriVJ7VVSsumjZItiBQ532BOORSqRaL6GskAm+9Qo3P+/gR0dryK465fug6zh9p
kd1jUq9oUFcXZt0J8tkNPaSL3zrRyRkNyK53Dm/WHW1AWLdWkyfnz0YTRJQS59tsMo3KPE5m
ZP9bQtS6sbleLb7PKXpCfIV4ds64wiBkvxjlWBPwFkvwDl1ar5DldLjAJ8YydI5TdzNBKfg4
VFT9aDwikFCNDK88odQO33rXRi9krW0rsOUrT35S+b0RdEAinYGB71QdGs6zqJAZSalOKhhx
rG0jdOnhrVyUSiGcr/0SLlt6GFYG3BTyMe9s20pLJFmS3UdOGFOxJ8ZJ6cLOQnKKrnDWGnmX
LdwVdirRw/HOHloceUsAgVCDxMfh00WCzlvV/KESssi4ha1dFhsb23e3+NXJc2fhRin7Ua71
/b6QNnI/WglS7f0t1DxgUuBgpXkm2q2sq4Eu6djtFVaMsRhUvsUHBKEXYh850Maa50K1Fy3N
+9M1zyRKWDJ9YTQC25wJZia7+kuwVduwcr0zd9xOdQdAhE/uxrmysSJx1U5g6+88HZg3YHRs
vixVnhoBKDbrxfounsWBvlQo97YxWPtjtAB7LPOEWb6dhyQTlQ5eEbhKPTIOIbhuqn9oC3ax
PPcxIR7OffW0XL5ZkCFBZCiFUlnVWjmJAhwEEwEKAAYFAlTH454ACgkQwO2qeMbWjxM7HRAA
j5HZwK/R/pUw0o3VOtx7f+ICJ+1f3TcUSulpggZLR5FnN0HiuD0dFlcmhBeGXKCsOSFjhOMy
50OLuExqQdiou2hwJ07495VmLXfFSwBrZjCLpj63Y9wNmvBYf2zmjGqE7QQjUW/3kGf99kML
uePi9xAdIDs9vNbPK6sx8ayH8FgjIG3edno9P64mCynrsd64tUAveEKNl0Mn7ryMS+a/xWTR
Wcky5AR6vo+kfwRdsxVKdLv5BY4HGtjoCIPxPsiInCPMzwAUJSzjf3MO5cZFzqn1M3cH1J1E
ui4y+022iFLVrwuxAH5Rw87Qdedrtw6quNJdpjjaTF/eTdRC4aUH3AijwzekOwFSTiHmesLP
ZZ0SzLlCWkyPKEx5OOxXXiJZddaI9sRAJgj412sS0qnSclSJPVCaZowDg8s21zifaR3w/5f1
C1dxslJChrzR/GNxfyOSFrL2x4wCmXZCLGxoOs9QjCc72oa/zbNJkdVcuvTwsm4XAEofMcra
qTTPdRYNeD4rPAwNJzHjp+jNggnw4vGP1NXhLCo4ExMfC7hHV+Qt0E6zxad/NsbR1pzziLo4
PovWXt53cUTC+vgtkt5qDApFlW8+7GsoDaTKDWVGY7nDofj6rp3zaBLPGd49/Wu4g4d404RB
1CH6SprtTp8PxDGa5MR4RalunXaNKQLy6OqJAj0EEwEKACcFAlSlhQYCGwMFCQHhM4AFCwkI
BwMFFQoJCAsFFgIDAQACHgECF4AACgkQ4coYaECLUtXUqg//fL3ODl2rGVLrNrwbBb8ZC/Ds
/DcG0CwdQ5NQ++F+31ulAG8Vc2GBd2stcL37SR6q/xyywW+IWrbz3BwoeBn9oSXNRYNMJVSw
wIWGjp5ZVzVIuH/RGqbbMguPwlEys4Woz0fMxQCe9Q02HYsXxjCInC+z8gUP8eoW1uuhskLS
qY/S4IF7CAlTc5D1fGZ5KF3+uhQbKferCnjFW5Q9RU89hVZRwTw5jEW5WXkhVAuT1DzagC2I
sgdNWdJsPGiFPP+Pr59/AojqBs6+ChtY5+YMdmx03wjcry8Buz7xnDSnwy/A7BAdSGoAfKwy
04/NLoybRT9skyZhUU/wDsHQDGQG0UvyOUyxLHlsOW4b2kEimHAT/JbYRYbNkpCv5t1jo0gp
BSB/6eaGh37uv2gGGiOcEmCU+u7gAiOk7snVbZ9r1918wuhFMj7h970Re7lPr6hGMAEiRjLC
ktei3WIOo5ha5p/QiBxJm9wIufR4BnFPu7DfGvlkjrqAtHV1vhIG48ZXQpl+fzkLzYJTv/VB
qlRaENx3/qftYrhQWglHnjIJgxJs74nENligKOrJIKa9DZiguNWBT9J384+ym7Xz8yx4TXnh
/f2jVMYQrLd5IGCg/M3fxVjudcc0KvxURKP5BUlwlQhpgUs9qy7RFxtvAoPn8CIGepvwqPF+
VW1LrhaIIceJAkQEEQEKAC4FAlS25n8nGmdpdDovL2dpdGh1Yi5jb20vaW5maW5pdHkwL3B1
YmtleXMuZ2l0AAoJEBMY76xfu9vOJY0P/3lke1PnZAou9xVjG5DUIpIzpnNkfvR49PxX7T2K
UnsiG1m1MxyUFCmvwqc6+q5g2ztHIm4HTUg4F0OHsq/uzpZR9RbrjhddMehUWKn3Rn68e0kN
CFMryDHvWj+SkUSgDN5WkxpqDk0t1MfD49jELrdLGcearOrbnX0cWN64MOIg3AiX7tj/Xthb
BiVdw24D1FLPZbcPCvKUxdA1ybPXjsGAcVNi9WxHhQE8pFdMEg7iOPf72898gTdGLw58La8D
G114JytmvuyfJQWH/ii9QGagqPIApmcU9AIN3zh+AHhDaUQRenUzme7d5dA4qXPaKlUadXO3
0TxW6yPed5E3Ebis+bBRAMxZ74NaMa8tWX/ACY6ZrqgCByw1yRER1nNNy4aS6D/MLB1RbLLt
9lCoUxz/yKoekzlsX6sOEKvTps4qrgqgxMDX0TzMsEgl29j/m2ijv4p0EB8qdX5A+KMOMiFp
EOAL9hVw0BZtXv31SJyGvLI5qYuf8wFfjO5OVhTSQoTfuaWtVKiBsNLYM9xYKenZ0vpqJtNC
9x77/qung1o6WqqbfnUGFVtBWkGcDMGbb5bv3INS8KAv1jCVrjaSeNnoKdfduW6VYzC2QHwH
AiRji4Zql7Z4l2XuR8Kwl2pGOvdHTmEli4tjIf7aRv1IWva1YksmlvoARO6Q/76qU/k9uQIN
BFSlhQYBEADwMjT7AV7xg95lmxK4n6dA47OMUvp34HRY9mxBLE0+BIEojOkGOBck5UE4Lfu+
K5HUZacW4tyei9YUFstS0PqtDhjiuShnlM2J3+YnRU+/W6bIWh9lW1aTHRggLLGx2+d+VlbF
/fES66bT1GZREHexYUbDybIEEbq7S0hmYVM90qw4wywJscyQfjqcb0VUTg9vssOGRcOAxg07
4Zs6LsHrNLbeP104dzDgz8WnP/H4Ul9QQaJY3s96WCx7JeIwoolQ9vK28SHjWkfqIrPIa/2M
jw9XwGMtpD0vz44yKIWmJ/Z1dNAJz8TUGFXBmGyr4vVexXcHm8IJsjJ5nZGcxleekmlTrrXF
9HPS0zKK20tZnmxyHkWhKKI4jgWdYg6EJc/dcqmA2+jhXzi041d+toWdv/G6pEjJNM3KwedQ
TSKseMG0vLUXxJmnvXCcqz6GlB98Fr6bVzTx3ThdwudAuy07fRAL1tLicylhXFzkDRYao2d4
k6PvTBoZQW7JH0hnmm/YuDDxSpFJ0g1U/h31U/toXTmaOWRGDEl32Ycmwu7p+aW6xpx/geCw
cd2DH/dVC3GymNzUkb9FBrru26Nicj6NSkiaMPBrYWJDVzprU/PS4nFbPc7kTW5EoCLLqaTR
tFah7FRU+z90268CGyEpzbrs1a4pnVlWKlGTUPjfHVUmEwARAQABiQIlBBgBCgAPBQJUpYUG
AhsMBQkB4TOAAAoJEOHKGGhAi1LVrQgQAIes3bgkdbarW1ShfBgLTJSAPcfRQhpHt/7zH+LN
OebFGPNunbtsRcmubiJO2HIq8ht/pgUWittYaWMncf6dn3dbQ2sEJicYnkoiVuCdTfuUYBb6
JmoyjHPZFEo6POf75UTDskQ0IxWUqAVxJoTiEZaW1KlG/QUKriNDEC3Y2H3AErKIGjZOl1SY
RSrG+QJ7olQ0ZYcHj9KM49XPxjtD3FfiyYMD5qj3xSTnBMj6fPWvz8CKuWGra7e4Z72HxjjL
52Mlm7nzHKDJaJS9Nzk09W+vGa79UTkmkiCZWBt1ozT+A5aPvwN3fXUm64SuAt2tssG9cA3s
yXScG3sqz+39/KozXsX3accKMQMdQkHmVNrnwL0MClhwbYt+L5H0rj5COqURUL0r9Hl188/8
WqMxghVuYWuxmTj7N+5br45X+4ZYyif7oM2h4pnRIf5BnB519PV3Ml7yXK5wVboiPngIzQYI
ANqsy7iAnca3uwAwhcbMhsyKtXmdJgp3LRcjSHIZ2PILIXTrv3S3tUtYdy02oYL6xwuGZ9MX
bv5yjbGJpWodQ7ewvTprldWB8pdgBTWtPq/cwMOy0RG+Cuu75kHZG1Dxx+4rKTmo18zoiWED
jEoRFlQBGhRTl7Lj7kwWLAsMapnHZLNO3QjfszPH7BhpXezIuQRu0g0iVwMIPKZvLDdjuQIN
BFSliPgBEACjR2jyaf6Fvmak8h6BYeA/2EYmYPDts1d55DDf/SfWViwhVpZrtl6mP7qO+X9r
1TOIQDqmNTCbzTXLCxbk6wv6BSsoNd9+fLF/5n3XrjW/TSBq5sx1xlrsrR6HbkORCbOGXFBR
svp1QoFn3Yg7PNHAYinKisfxo/6DfOi4AXtn+ioGSXmI66wm5vUO9gH+ooMDSUp764741nXh
atzGNRsr90sE7+OSOSR5nCqIlB1PdBQ6zMbPA0JU7TMQTR6n4XAxlQLs/YnGbJDdNa4oDUTS
5gxoo356WJKmg59RvCAEhg+3qCJoq63Y97a4AdVS+RP2s5RCn0IHG6Oy88AauVXfiUCLJTvR
c/OrbjnaepiLRLeSESgEeENKo/JlExmLTB5fJAcYX/PQCdDO/itZFRlFnOSu3wB6BhqERTm3
vYgP2LXEOPGHKECYaYLPT+5R3+Ha+ljnOq0WmYGHNJQa7cblCK4t/RSasHa/8oP7uMoAsri2
XN04egOoor0WRMOVBNnr89HxAbAqWKp1qPYtX96Y6hlUh3m68Pm2vn3vp4Mmuyq5x4jJGpI4
O5C3LOPPbWz/ddG5pTGC9UP5IoB3K6Rj+6IQ4DT2Hf5LOsXnqnWKRcABa0Bdc2FSYf1YgTW8
awWw9opsoN5oUHEO2bpe7JzZ+Q/cwh30Xp7VLQi5s4WNlQARAQABiQREBBgBCgAPBQJUpYj4
AhsCBQkB4TOAAikJEOHKGGhAi1LVwV0gBBkBCgAGBQJUpYj4AAoJENr1OYGyDI3yjd4P/1VC
6R7VQrECcGALm7ecPzm4l8nH10ZqpiLGq9DtNPJFGsLqHbNLr59nRljZg3yql/mBgEOhuUux
w8BN6yQ8uxMpaDW+fv418HDtippJ2HARe3sGLxiqGDK99wwX3ABZZRSdupp3QJmUo4JNMbVH
vvJ4Rx/VaYwr1sdga9n5ckLXcTQP7iFfP4JP13bepMoIO0Jfaj0U4RHs9WZgSG+k8NJ8TyYp
O7zPvMb7WALfMXJ0xY/XUoaqUXB89oUmAoB+ha7uaVSH3N3JMTccjIhwZAUUOIW09mL9D7pR
Okyaol3QQiL4GE4XICbIpFWuDH1FSmMAcVuxHYmEJgZVcuQJuW9Se5cuv6pqqvqUMR2m5KgR
n0sb4E5QHtexhiBhJ6mTxxB5suB2EHu+fzVn/IY1rU1j9OLmEpDr5vQz0Mdp7aBhMoVVPQML
WzGW0mHbBhvwexj9gTPZgKtMPHBJwe1H3ZJApFWgif1dm92oiv8RIsJftX9uuY7kwhHX/VrD
Yi8bI52unUKaGbZWA+9laxaPuLN89ix+dzVMVqs95I5DF4M6lKITcsfNh/VKpjdvNGYwvv6U
zLAU/ZH5i/gepw6iYhJYjvF7OcAQpLCzCWGptH1I5rviQ9v2v6n7XxBsRibgrRKnG2ZwzpR0
Xb6q1oVzDKAEV2LRqZC2lP8fhDEr09pJqhgP/RL2hAyo6oQGVFcs6VP86T7ONnqzufJfIfP+
mRmjrOZydZv4kM3kSI8NPey1RqeT4bo5EcA7xi7I1ZKakIU5CMZBcBKziEzj6M2ubOdm+BEz
5r9lv8O0U360rSqiuO2BDClmVYKny+a6E5XpmsBnUK2AhypLDwKsSaeJh3F81pNMD1i6HPoH
4bmFoA/votZHnHe2GKhOJHEgmbVONMR9B1k44lSbPad2bj0sIwHjxj4BV0cchBDwJSTsnUxK
hHNmV7DqqrWrka/6Ss7walwI+HvOBE1SmX6TyGIp80Ms4vgZGFZk4pn3N0Yy4zhUUWa17j+t
44fx9nmAk0bWSZyUuyqSd+tktQ06BUThmJP6YnJ0y/CyrYEY24Jh/NdVo6MNvZgNLegqc4CQ
O4Pc5+nKZPCXilCH+TDwtfCdqadGvAmo0xJuBd9lsF3eUydKIadGAT6lYEoz4UNb0E0McRAM
wyqKpN9dcGwLsGX2mtNzW3XMiXBjFMkng2BMAwg1GRv39uNHKikanvSTKzPP7OSTqlNFFuHP
oaaghnQHmC+pzQXlVE6NEZfcjGae+h2RvK7JizP2w6Ue1n9ghabqM2ygAmLFEso0I5vJsh5U
c5M8LM3YqqEKwMhlPxh2QGfgM5rPKg69I0pwgeqDolGLw6iRVqZqCyAxRXbjjOk69nSOv2sN
=WfbU
-----END PGP PUBLIC KEY BLOCK-----
```

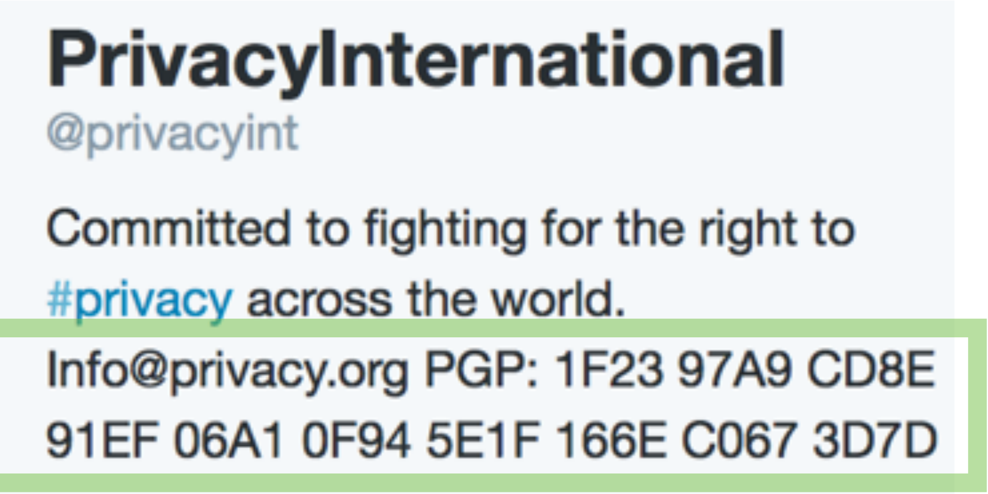
→

```
0F1D 8FA1
929F F077
7458 1191
E1CA 1868
408B 52D5
```

finding two keys with the same fingerprint is extremely difficult

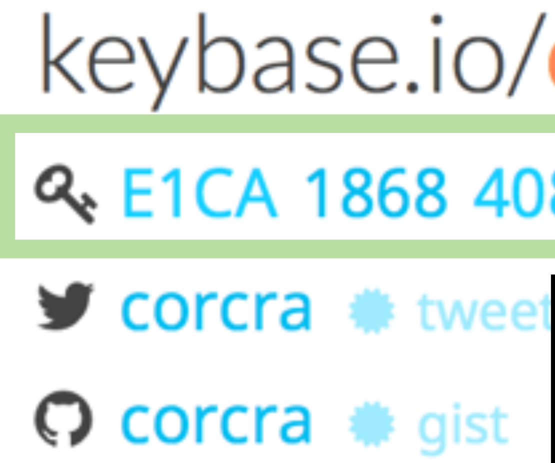
two reasons to trust a key

1: A public declaration of ownership



PrivacyInternational
@privacyint

Committed to fighting for the right to #privacy across the world.
Info@privacy.org PGP: 1F23 97A9 CD8E 91EF 06A1 0F94 5E1F 166E C067 3D7D

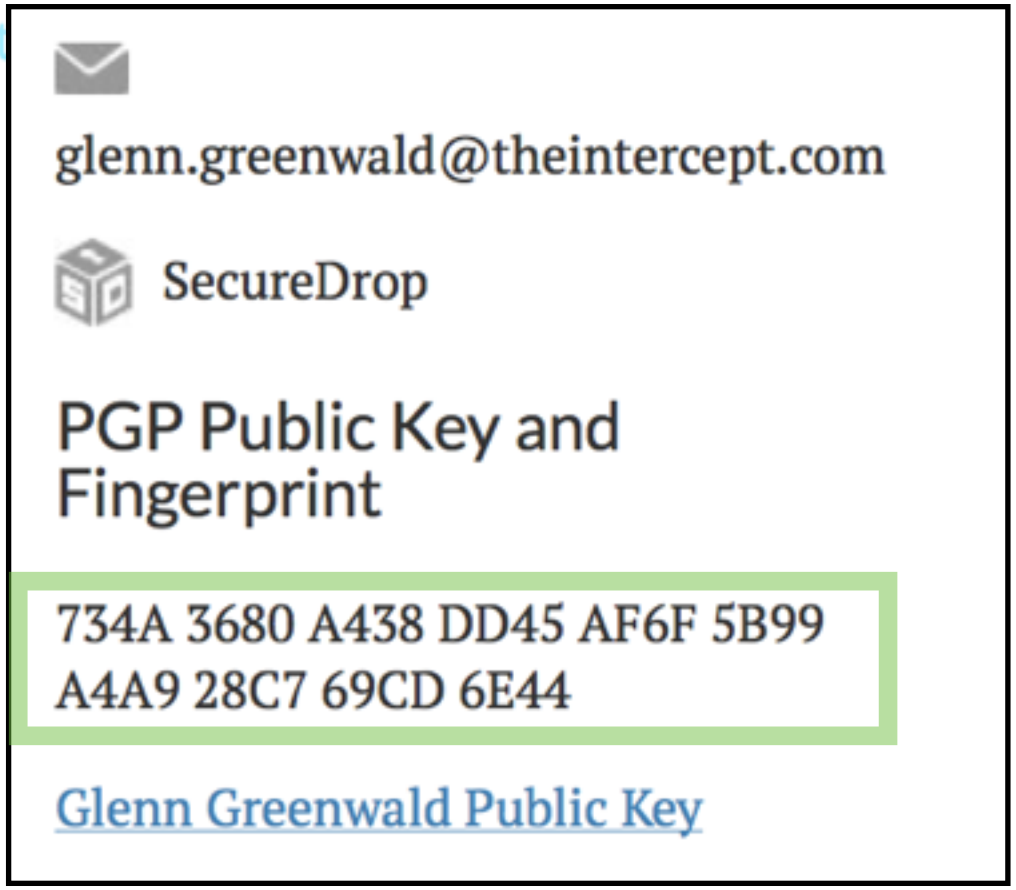


keybase.io/corcra

E1CA 1868 408B 52D5

corcra tweet

corcra gist



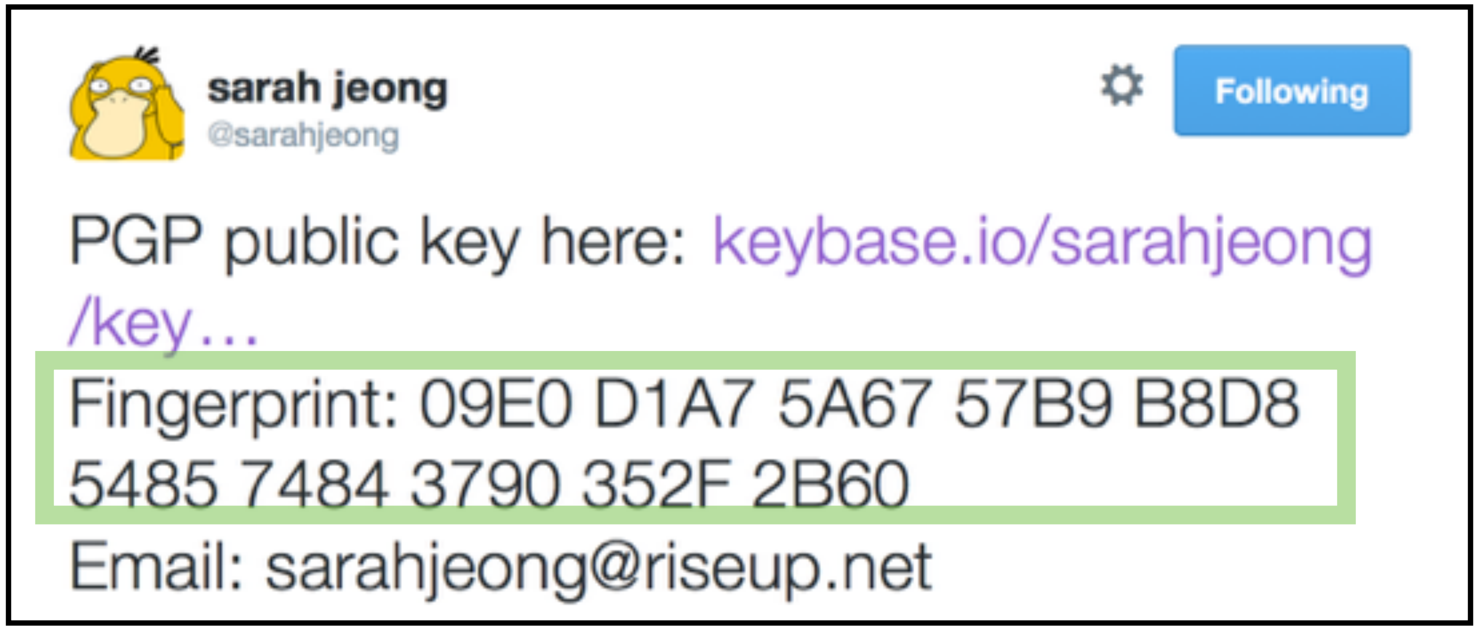
glenn.greenwald@theintercept.com

SecureDrop

PGP Public Key and Fingerprint

734A 3680 A438 DD45 AF6F 5B99 A4A9 28C7 69CD 6E44

Glenn Greenwald Public Key

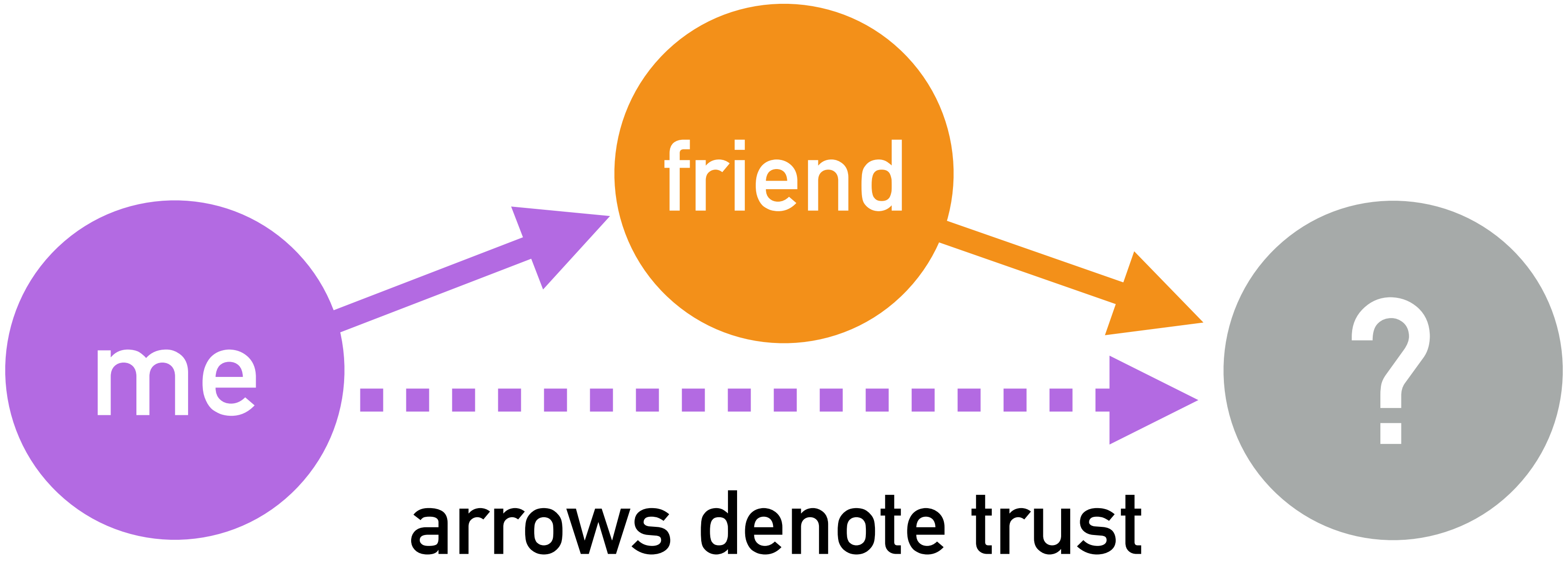


sarah jeong
@sarahjeong

PGP public key here: keybase.io/sarahjeong/key…
Fingerprint: 09E0 D1A7 5A67 57B9 B8D8 5485 7484 3790 352F 2B60
Email: sarahjeong@riseup.net

two reasons to trust a key

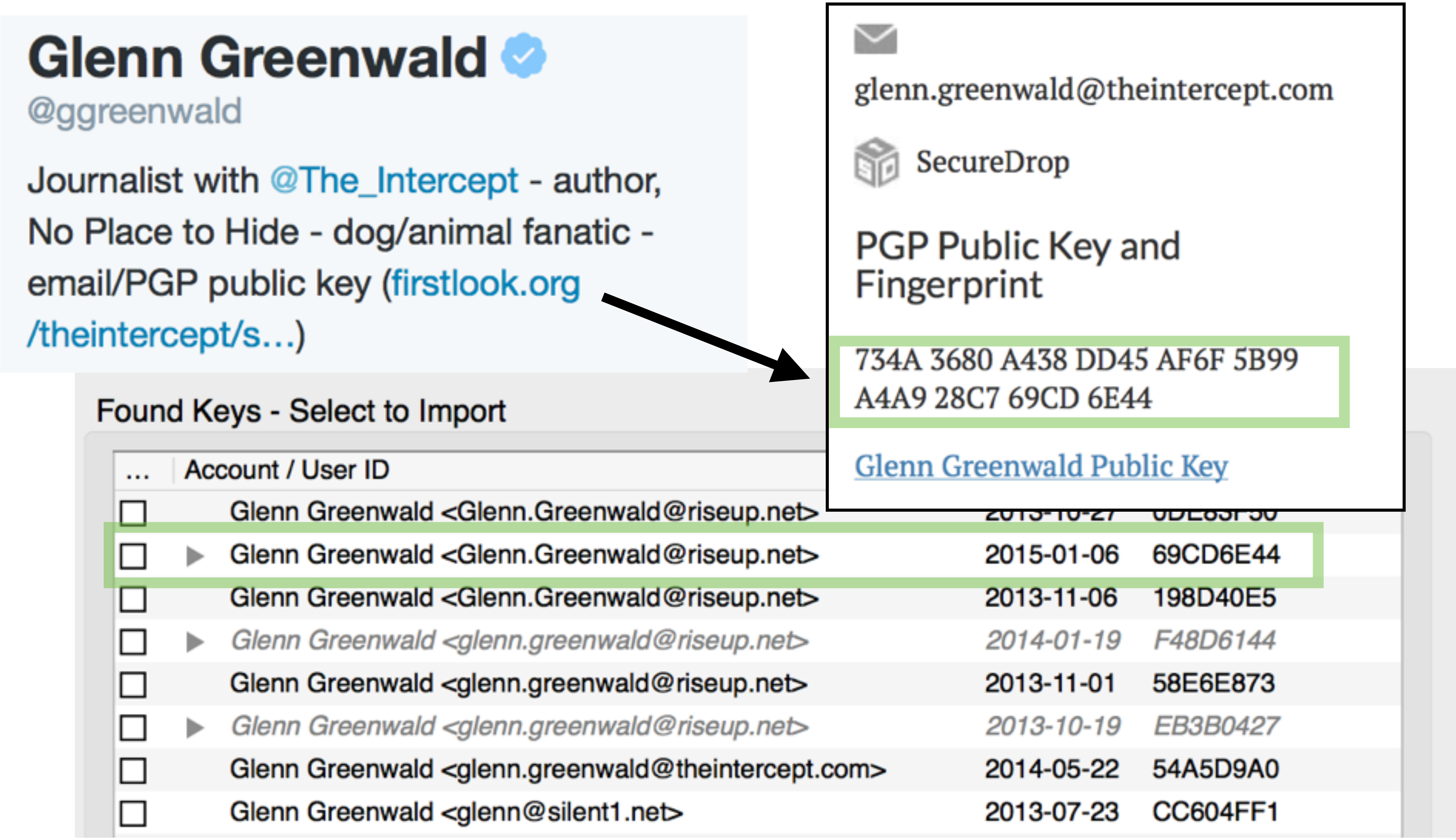
2: Confirmation from a trusted third party



PGP enables building a web of trust

(for more, see “keysigning”)

example: finding the right key



Glenn Greenwald

@ggreenwald

Journalist with @The_Intercept - author, No Place to Hide - dog/animal fanatic - email/PGP public key (firstlook.org/theintercept/s…)

glenn.greenwald@theintercept.com

SecureDrop

PGP Public Key and Fingerprint

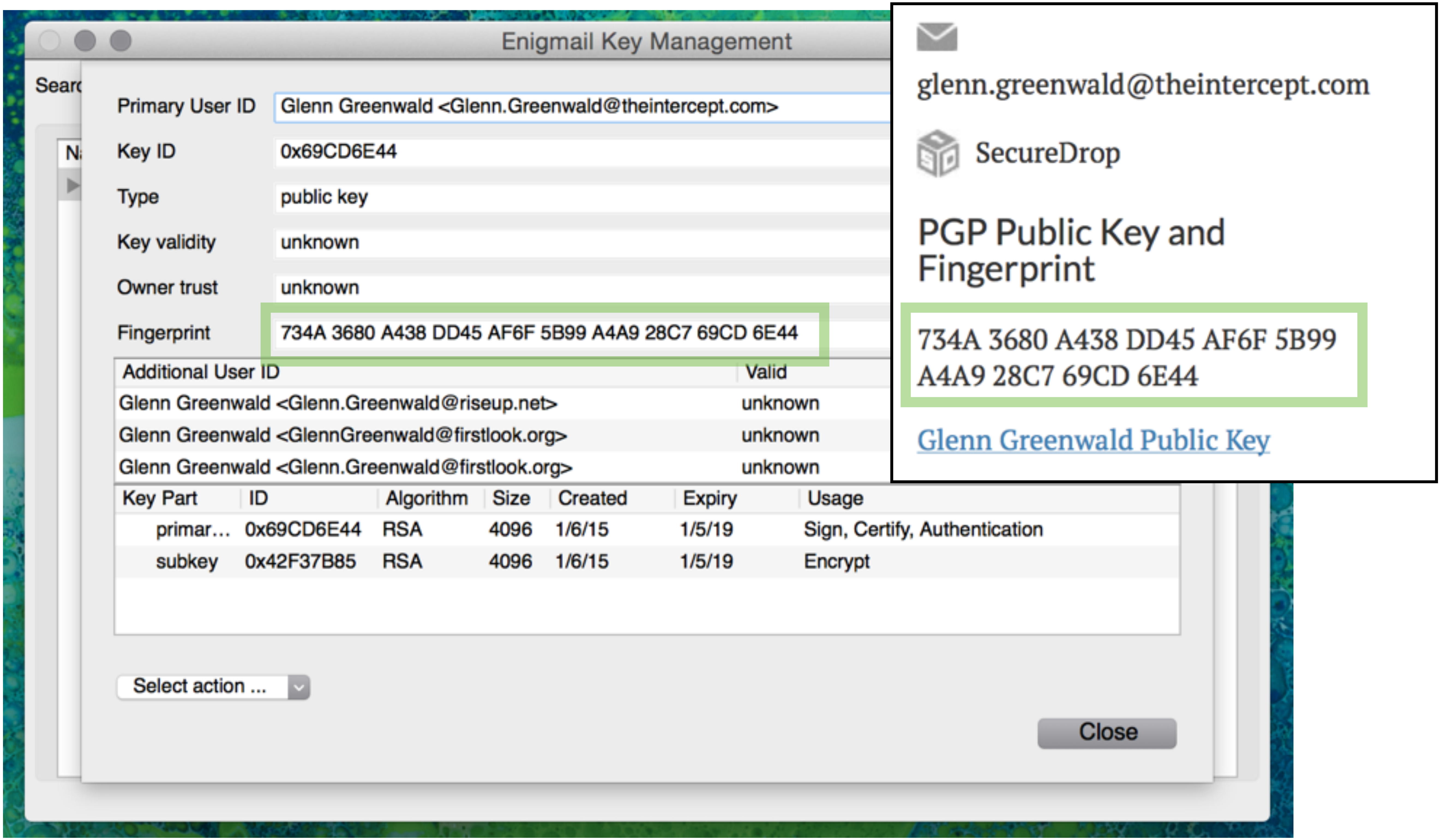
734A 3680 A438 DD45 AF6F 5B99
A4A9 28C7 69CD 6E44

Glenn Greenwald Public Key

Found Keys - Select to Import

…		Account / User ID		
□		Glenn Greenwald <Glenn.Greenwald@riseup.net>	2013-10-27	0DE83F50
□	▶	Glenn Greenwald <Glenn.Greenwald@riseup.net>	2015-01-06	69CD6E44
□		Glenn Greenwald <Glenn.Greenwald@riseup.net>	2013-11-06	198D40E5
□	▶	*Glenn Greenwald <glenn.greenwald@riseup.net>*	*2014-01-19*	*F48D6144*
□		Glenn Greenwald <glenn.greenwald@riseup.net>	2013-11-01	58E6E873
□	▶	*Glenn Greenwald <glenn.greenwald@riseup.net>*	*2013-10-19*	*EB3B0427*
□		Glenn Greenwald <glenn.greenwald@theintercept.com>	2014-05-22	54A5D9A0
□		Glenn Greenwald <glenn@silent1.net>	2013-07-23	CC604FF1

example: finding the right key



Enigmail Key Management

Primary User ID	Glenn Greenwald <Glenn.Greenwald@theintercept.com>
Key ID	0x69CD6E44
Type	public key
Key validity	unknown
Owner trust	unknown
Fingerprint	734A 3680 A438 DD45 AF6F 5B99 A4A9 28C7 69CD 6E44

Additional User ID	Valid
Glenn Greenwald <Glenn.Greenwald@riseup.net>	unknown
Glenn Greenwald <GlennGreenwald@firstlook.org>	unknown
Glenn Greenwald <Glenn.Greenwald@firstlook.org>	unknown

Key Part	ID	Algorithm	Size	Created	Expiry	Usage
primar...	0x69CD6E44	RSA	4096	1/6/15	1/5/19	Sign, Certify, Authentication
subkey	0x42F37B85	RSA	4096	1/6/15	1/5/19	Encrypt

glenn.greenwald@theintercept.com

SecureDrop

PGP Public Key and Fingerprint

734A 3680 A438 DD45 AF6F 5B99 A4A9 28C7 69CD 6E44

Glenn Greenwald Public Key

authenticity

(confirming the identity of
the purported sender)

&

integrity

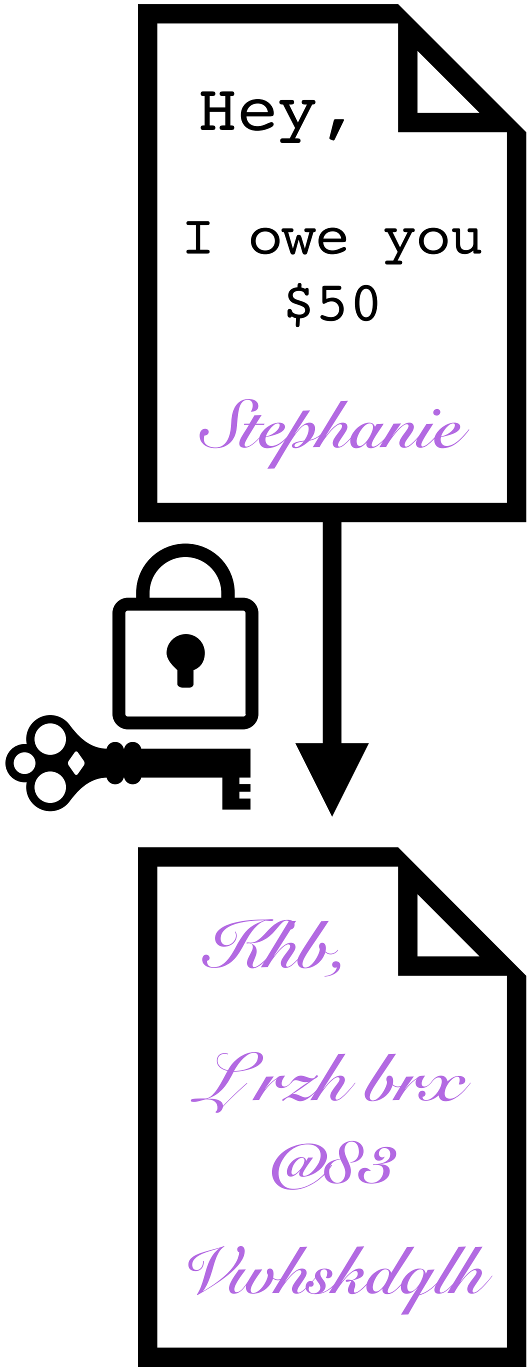
(ensuring the message was
not altered in transit)

→ sign messages

signing a message

My private key is unique to me

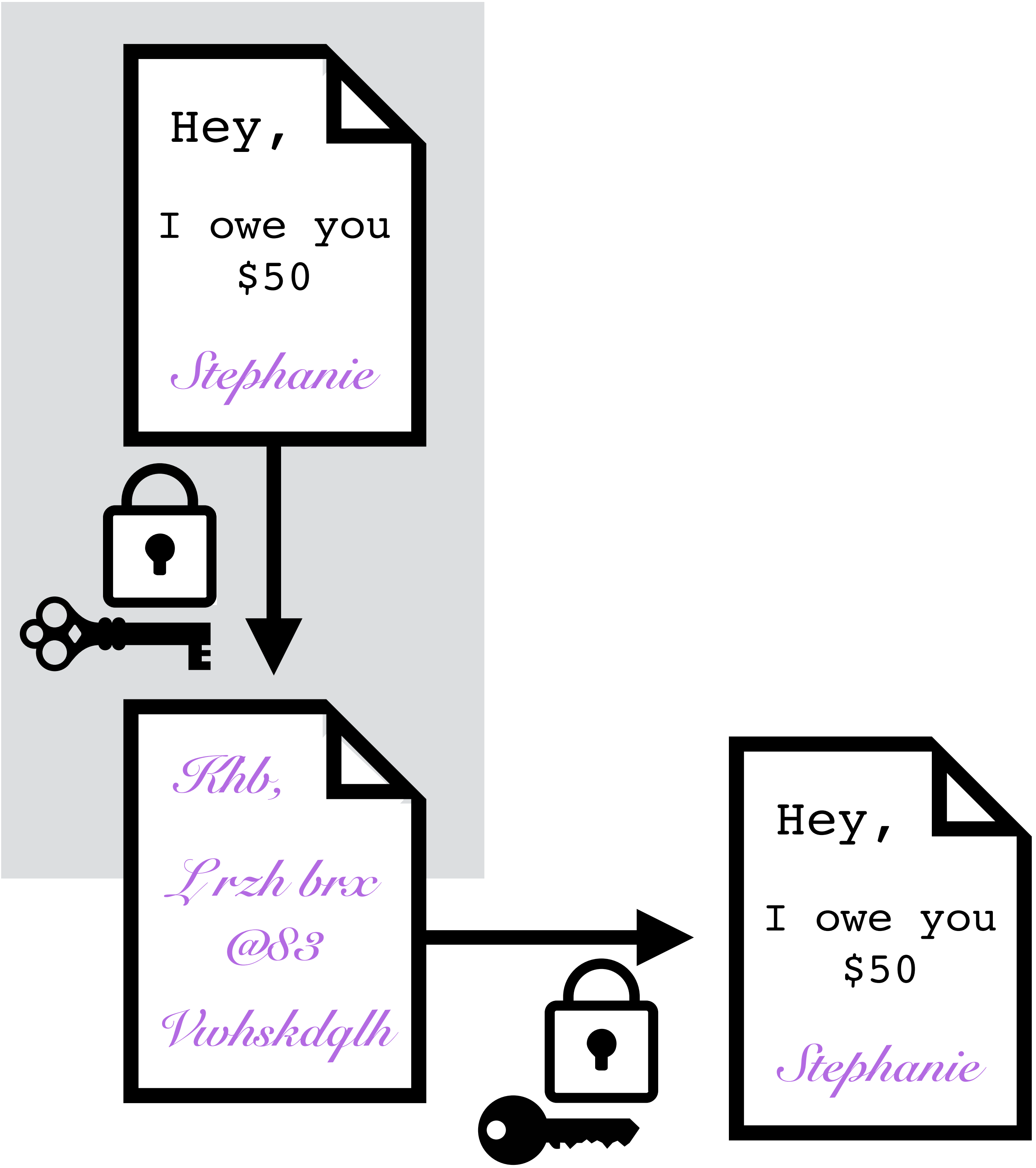
A message encrypted with my private key was encrypted by me.



signing a message

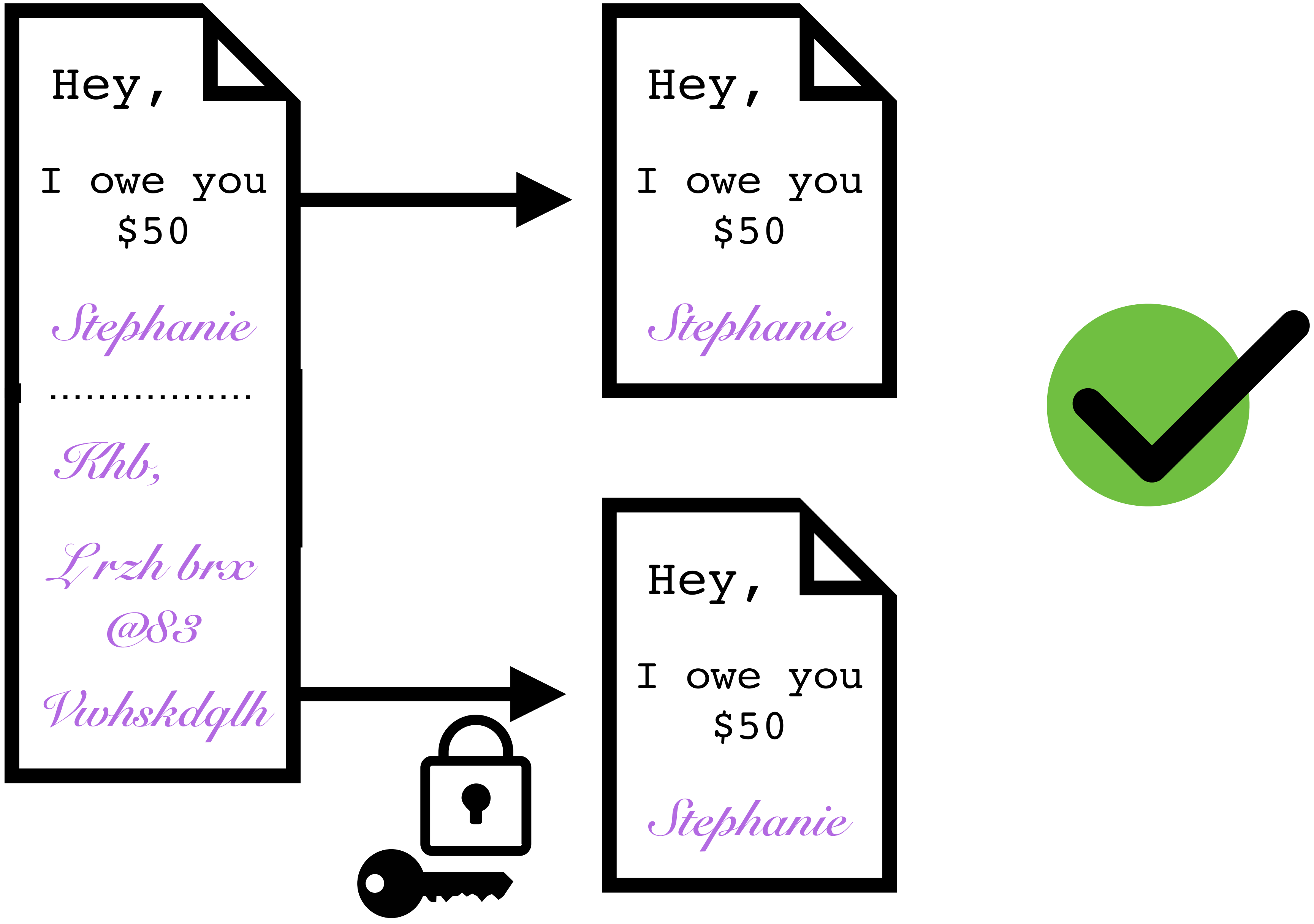
To prove a message was encrypted with my private key…

Decrypt it with my public key!

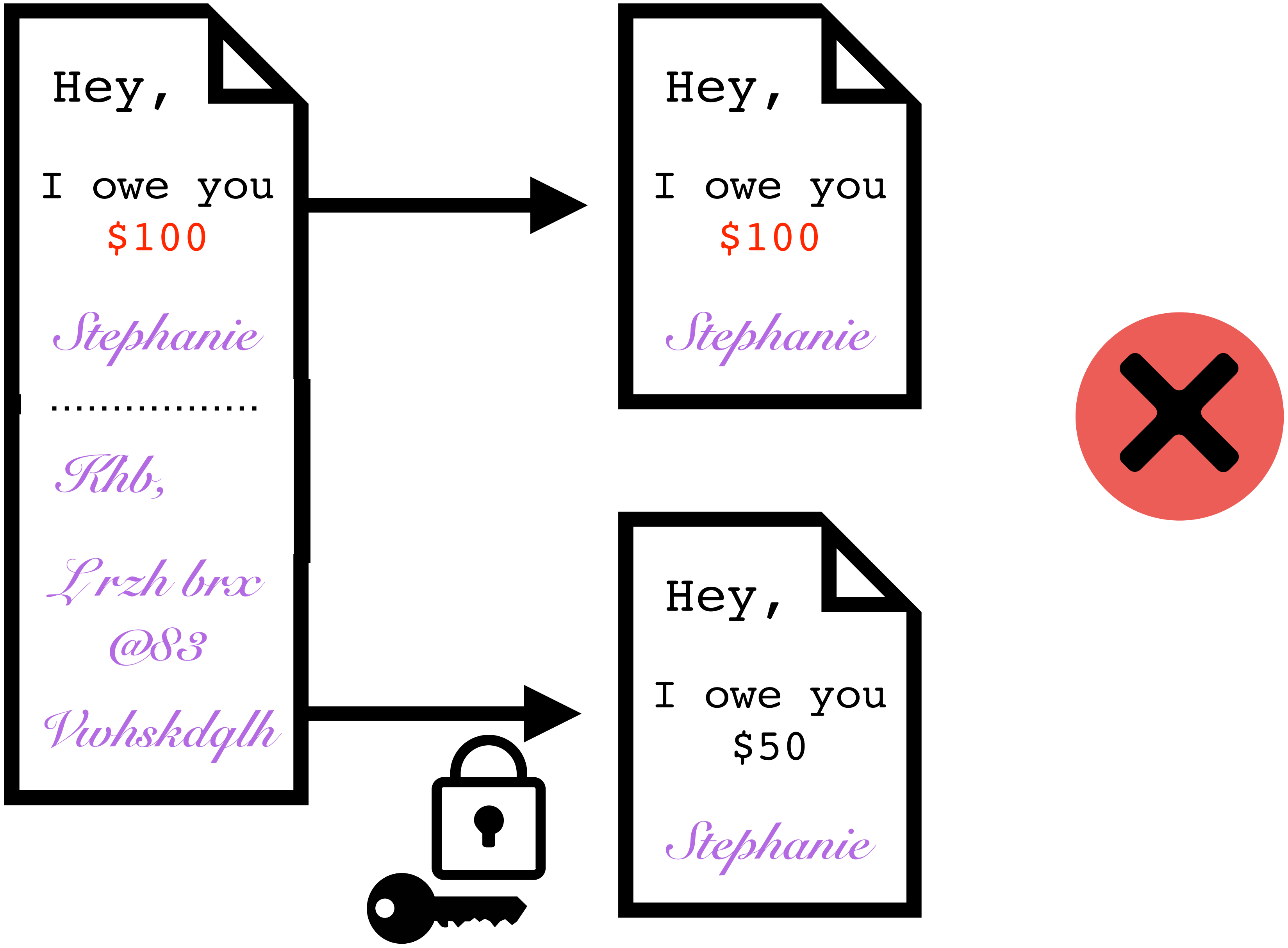


(public key cryptography is cool like that)

checking integrity



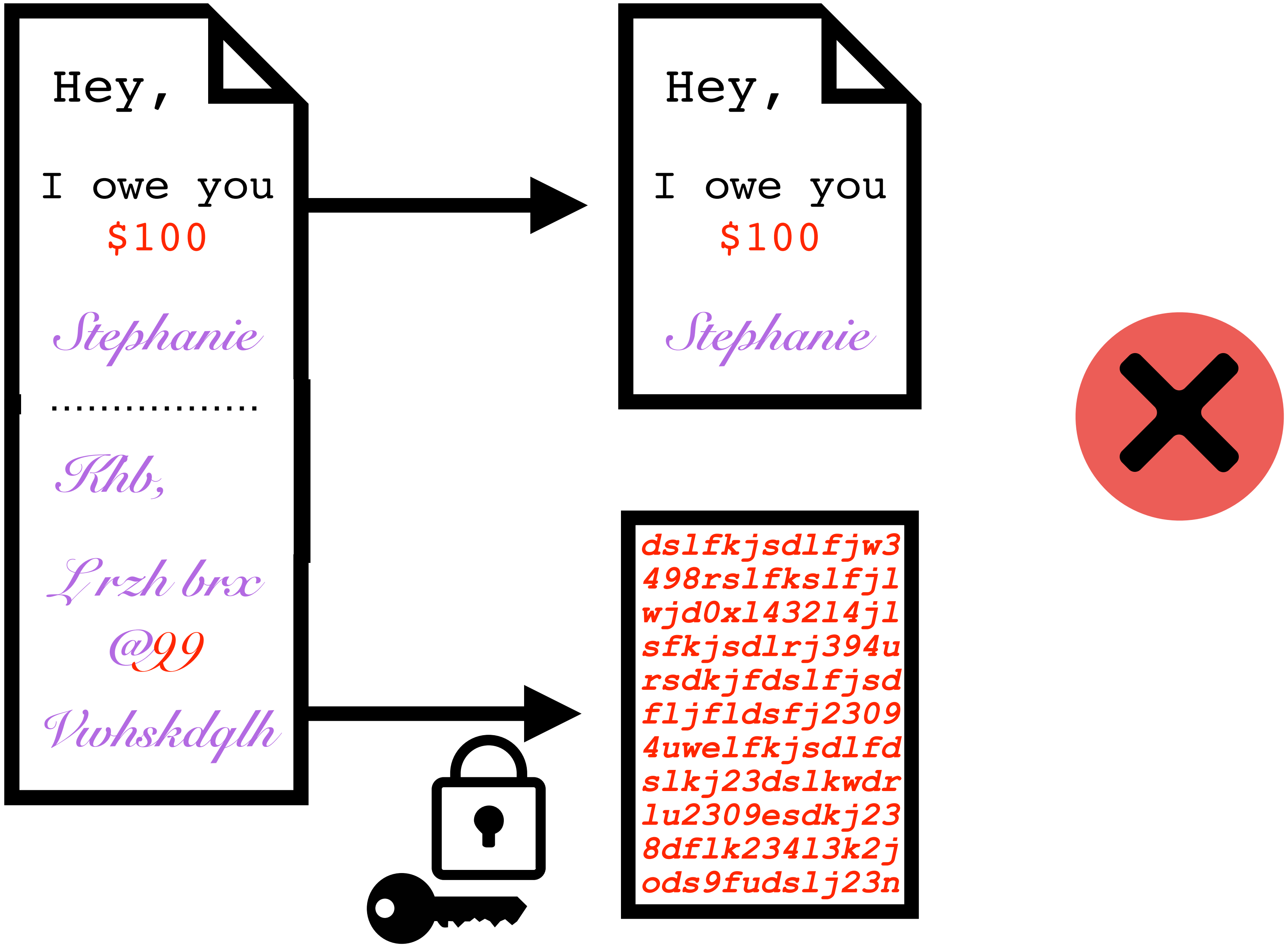
checking integrity



without my private key, this cannot be meaningfully modified

checking integrity

trying to change the ciphertext results in garbage



Hey,

I owe you $100

Stephanie

Khb,

Lrzh brx @99

Vwhskdqlh

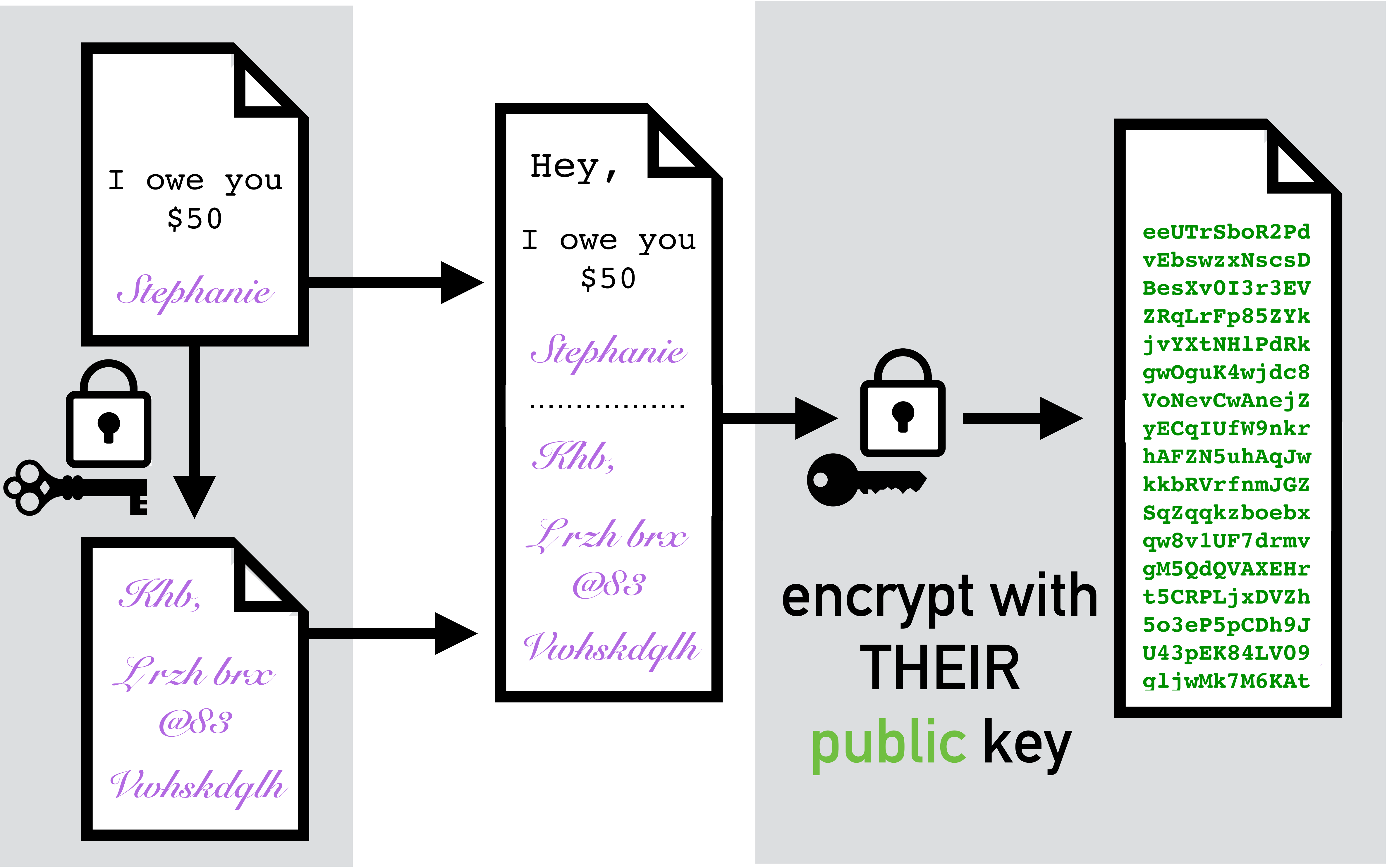
Hey,

I owe you $100

Stephanie

```
dslfkjsdlfjw3
498rslfkslfjl
wjd0xl43214jl
sfkjsdlrj394u
rsdkjfdslfjsd
fljfldsfj2309
4uwelfkjsdlfd
slkj23dslkwdr
lu2309esdkj23
8dflk23413k2j
ods9fudslj23n
```

signing with encryption



encrypt with
THEIR
public key

sign with MY private key

overview of key usage

	private	public
encryption	decrypt a message encrypted with the corresponding public key	encrypt a message that can be decrypted by the corresponding private key
authentication (+ free integrity check)	assert ownership/ authorship of a message	verify ownership of a message signed by the corresponding private key

overview of key usage

	private	public
encryption	I use my private key	I use their public key
authentication (+ free integrity check)	I use my private key	I use their public key

PGP gives us

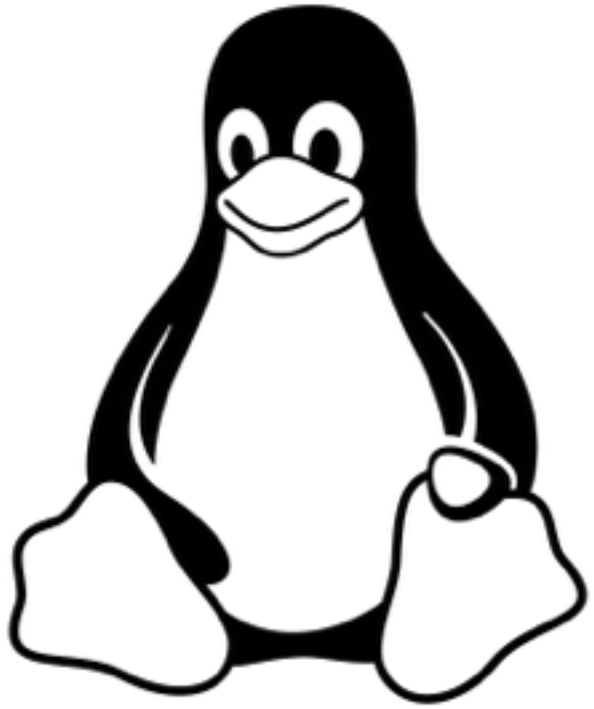
confidentiality & authenticity integrity

by using

encryption & signatures

(now we understand its awesomeness)

getting & using PGP



Mozilla Thunderbird

+ ENIGMAIL

Apple Mail

+

GPGTools

Outlook

+

GPG4WiN

many options :)

(https://en.wikipedia.org/wiki/Comparison_of_email_clients#General_features)

Mozilla
Thunderbird

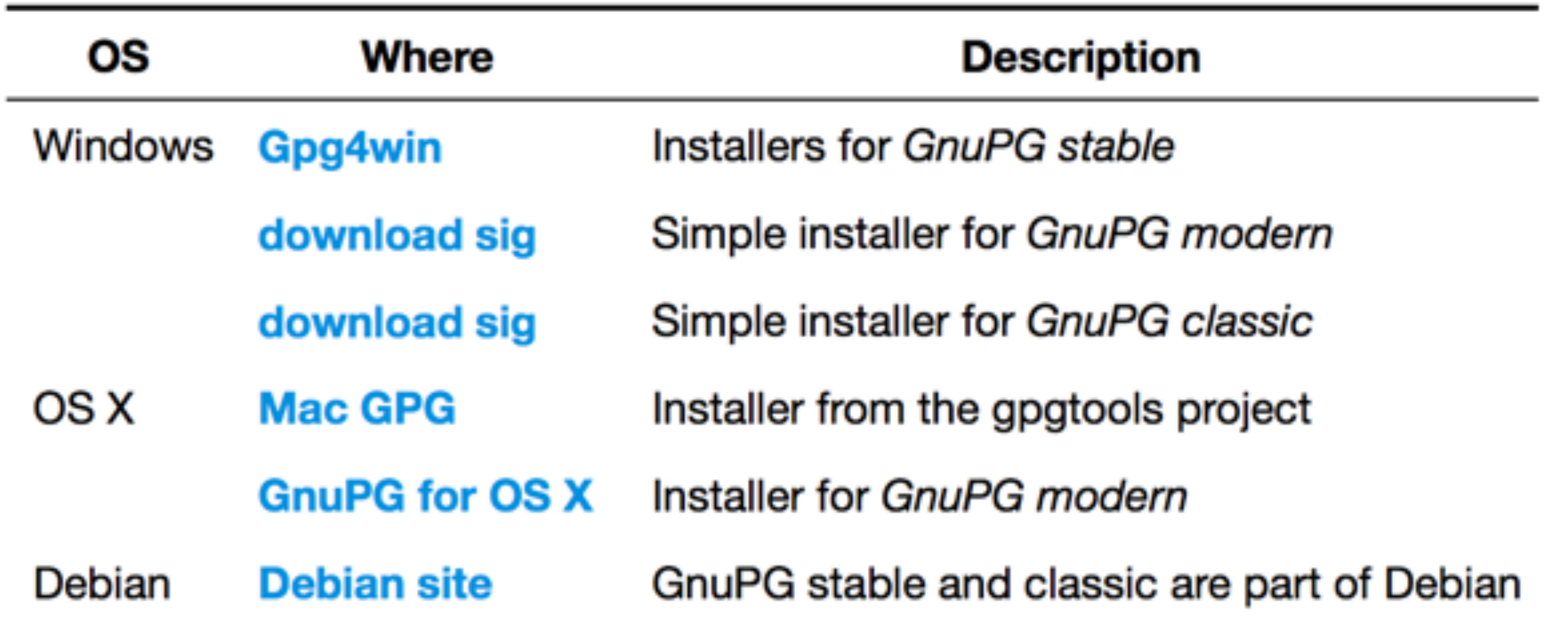
+ ENIGMAIL

Step 0: Get GNU Privacy Guard

(also known as GPG)

GnuPG

This step is platform-specific…

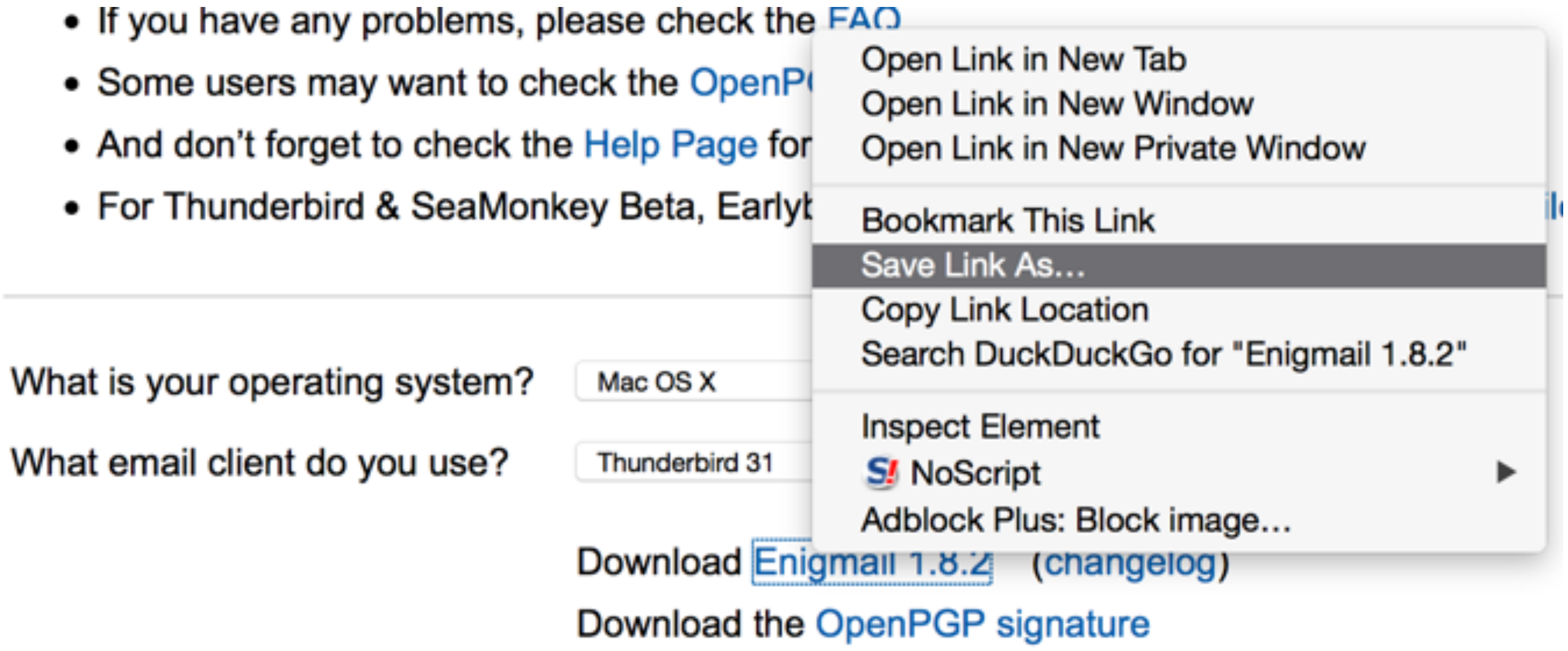


OS	Where	Description
Windows	Gpg4win	Installers for *GnuPG stable*
	download sig	Simple installer for *GnuPG modern*
	download sig	Simple installer for *GnuPG classic*
OS X	Mac GPG	Installer from the gpgtools project
	GnuPG for OS X	Installer for *GnuPG modern*
Debian	Debian site	GnuPG stable and classic are part of Debian

https://www.gnupg.org/download/

Mozilla Thunderbird + ENIGMAIL

Step 1: Download Enigmail



- If you have any problems, please check the FAQ
- Some users may want to check the OpenP
- And don't forget to check the Help Page for
- For Thunderbird & SeaMonkey Beta, Earlyb

What is your operating system? Mac OS X

What email client do you use? Thunderbird 31

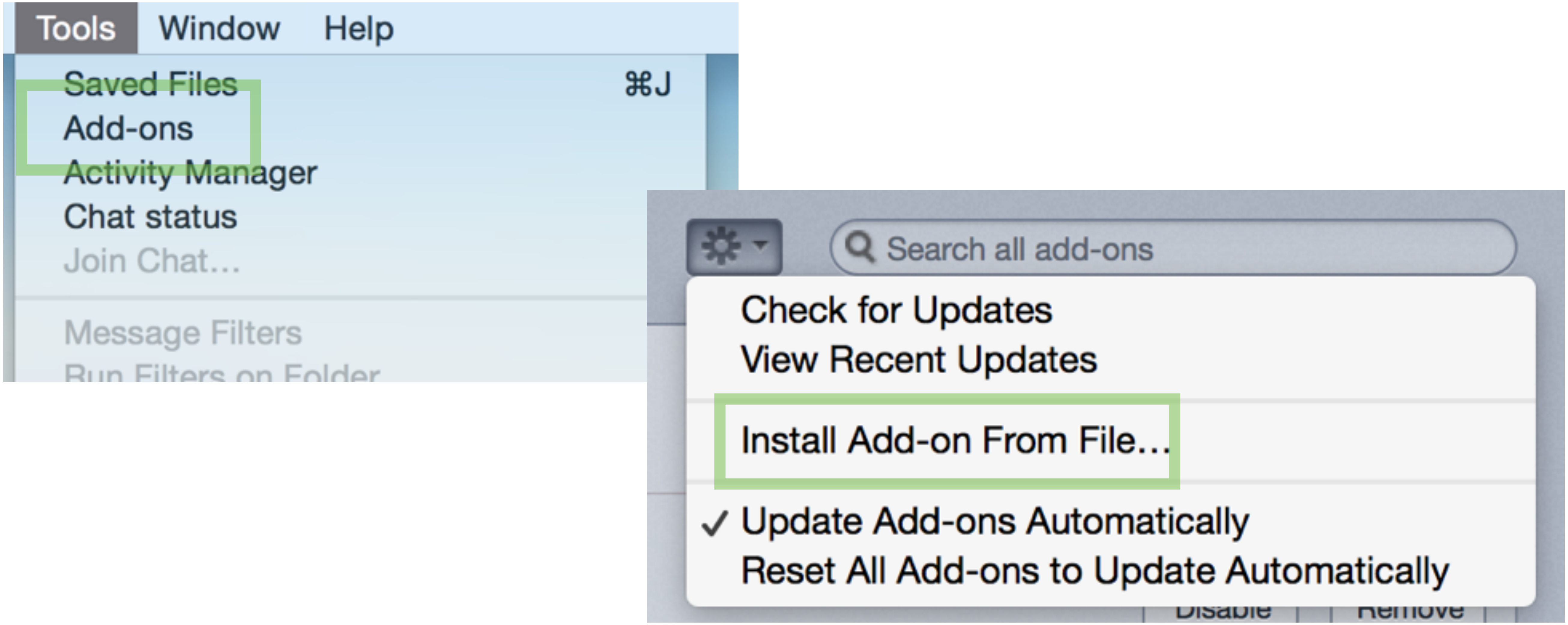
Download Enigmail 1.8.2 (changelog)

Download the OpenPGP signature

https://www.enigmail.net/download/

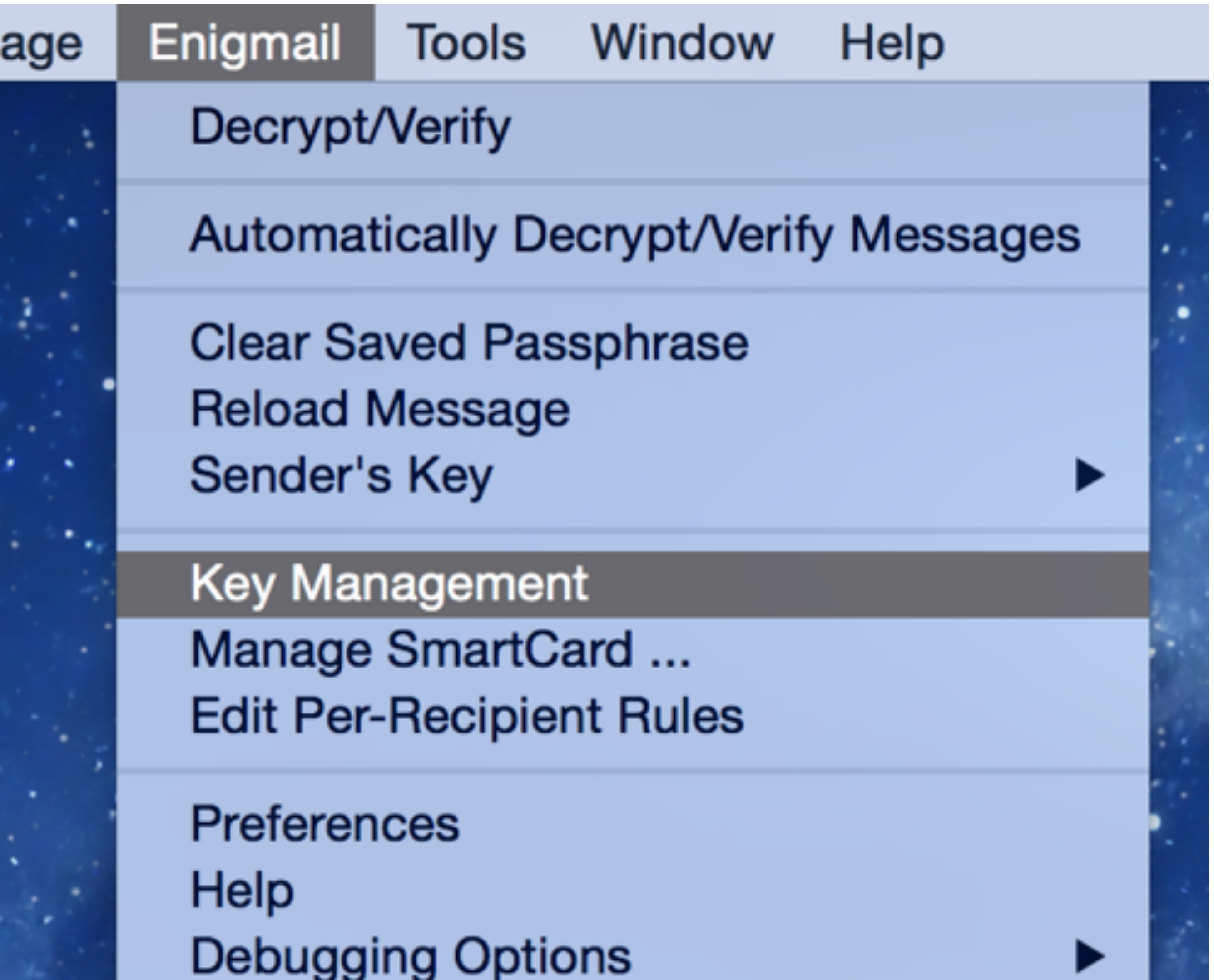
Mozilla Thunderbird + ENIGMAIL

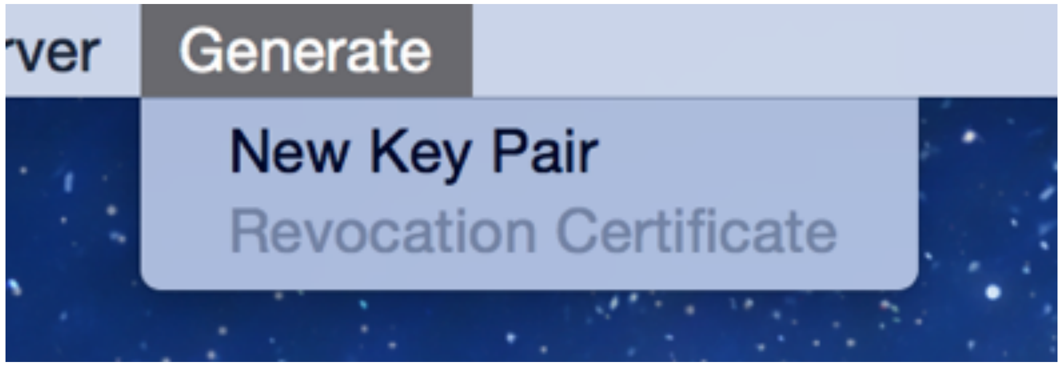
Step 1.5: Add Enigmail to Thunderbird



Mozilla Thunderbird + ENIGMAIL

Step 2: Create a key pair using Enigmail





private key
public key

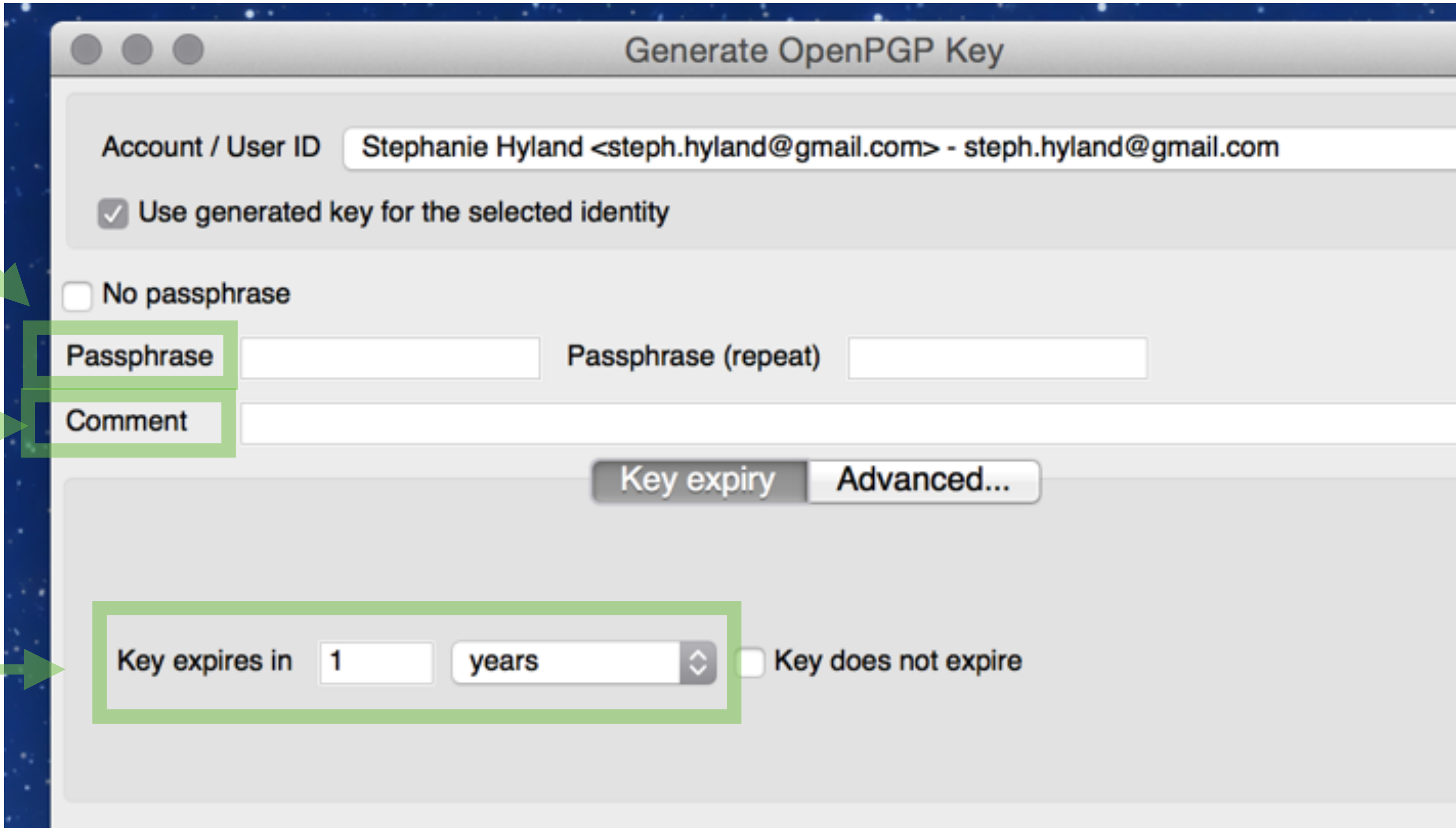
Mozilla Thunderbird + ENIGMAIL

Step 2: Create a key pair using Enigmail

a nonsense sentence is a good passphrase

no comment required

1 year is a good expiration time



Generate OpenPGP Key

Account / User ID: Stephanie Hyland <steph.hyland@gmail.com> - steph.hyland@gmail.com

☑ Use generated key for the selected identity

□ No passphrase

Passphrase:
Passphrase (repeat):

Comment:

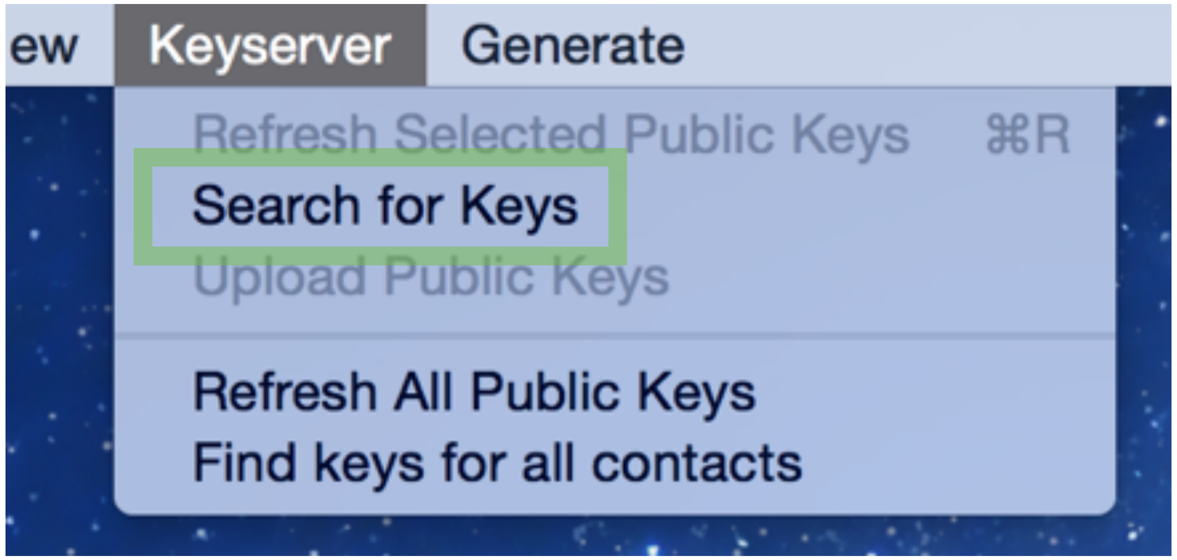
Key expires in: 1 years

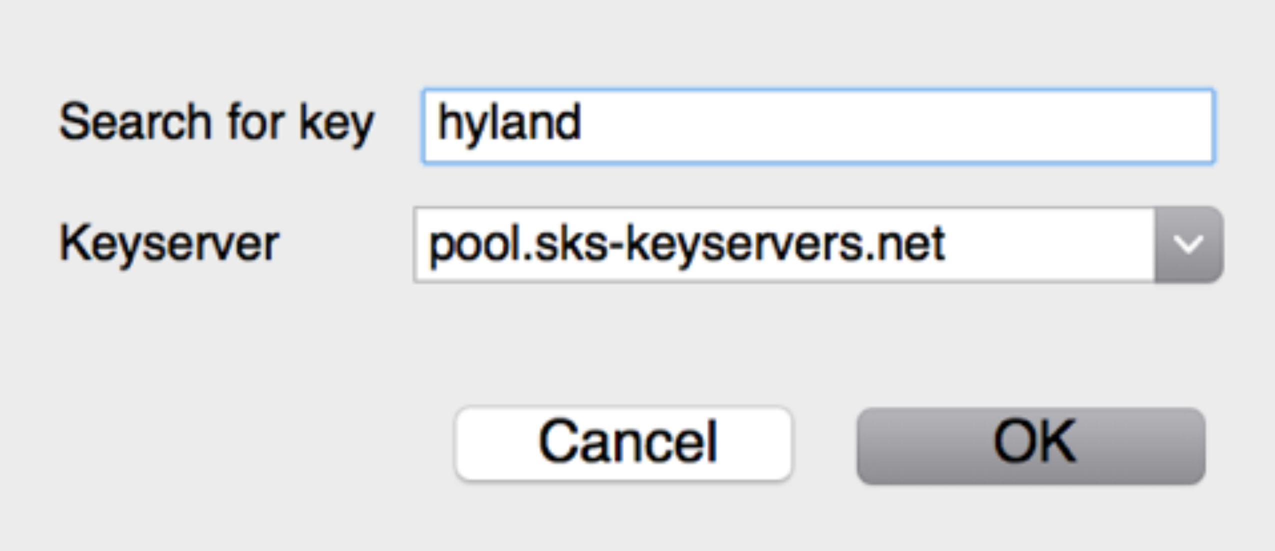
□ Key does not expire

Mozilla Thunderbird + ENIGMAIL

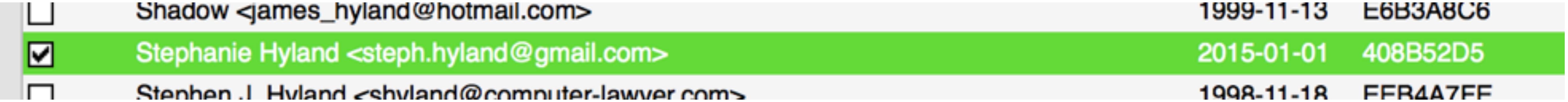
Step 3: Import someone else's public key.

(warning: make sure it's the right key!)




Search for key: hyland

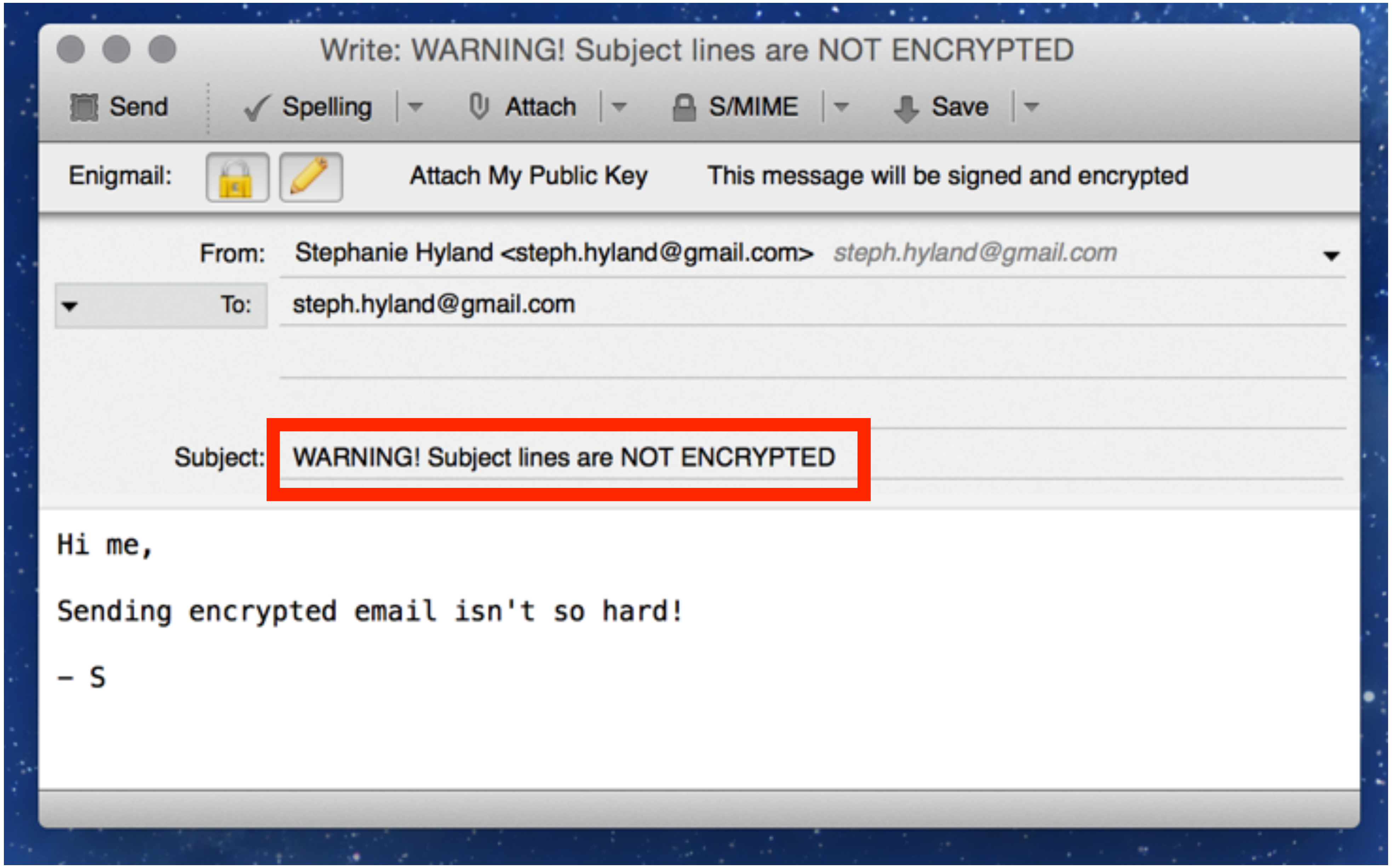
Keyserver: pool.sks-keyservers.net



☐	Shadow <james_hyland@hotmail.com>	1999-11-13	E6B3A8C6
☑	Stephanie Hyland <steph.hyland@gmail.com>	2015-01-01	408B52D5
☐	Stephen J. Hyland <shyland@computer-lawyer.com>	1998-11-18	EEB4A7EE

Mozilla Thunderbird + ENIGMAIL

Step 4: Send an encrypted email.



Write: WARNING! Subject lines are NOT ENCRYPTED

This message will be signed and encrypted

From: Stephanie Hyland <steph.hyland@gmail.com> *steph.hyland@gmail.com*

To: steph.hyland@gmail.com

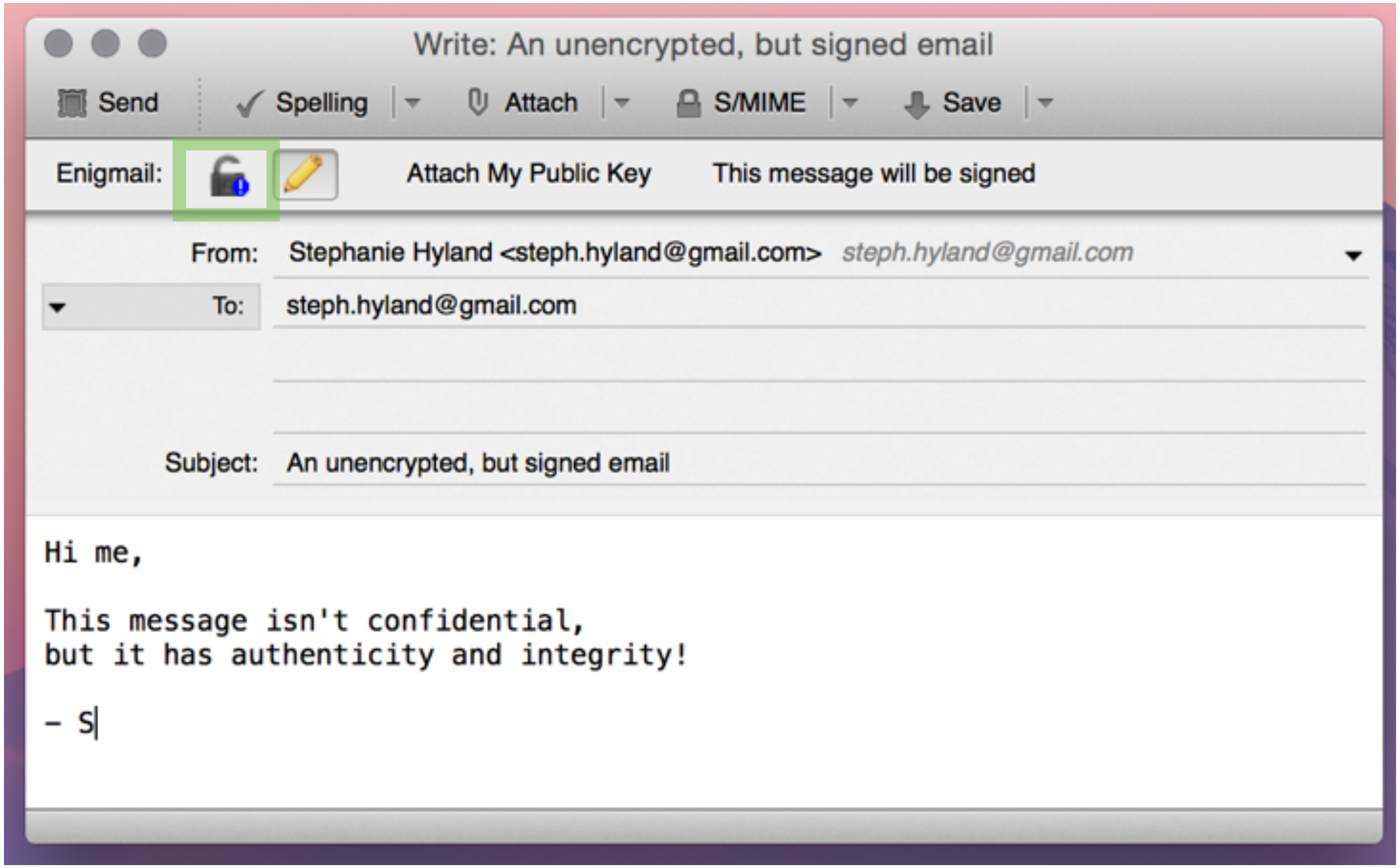
Subject: WARNING! Subject lines are NOT ENCRYPTED

```
Hi me,

Sending encrypted email isn't so hard!

- S
```

encrypted emails
are always
signed

Mozilla Thunderbird + ENIGMAIL

Bonus: Send an unencrypted, signed email.



Write: An unencrypted, but signed email

This message will be signed

From: Stephanie Hyland <steph.hyland@gmail.com> steph.hyland@gmail.com

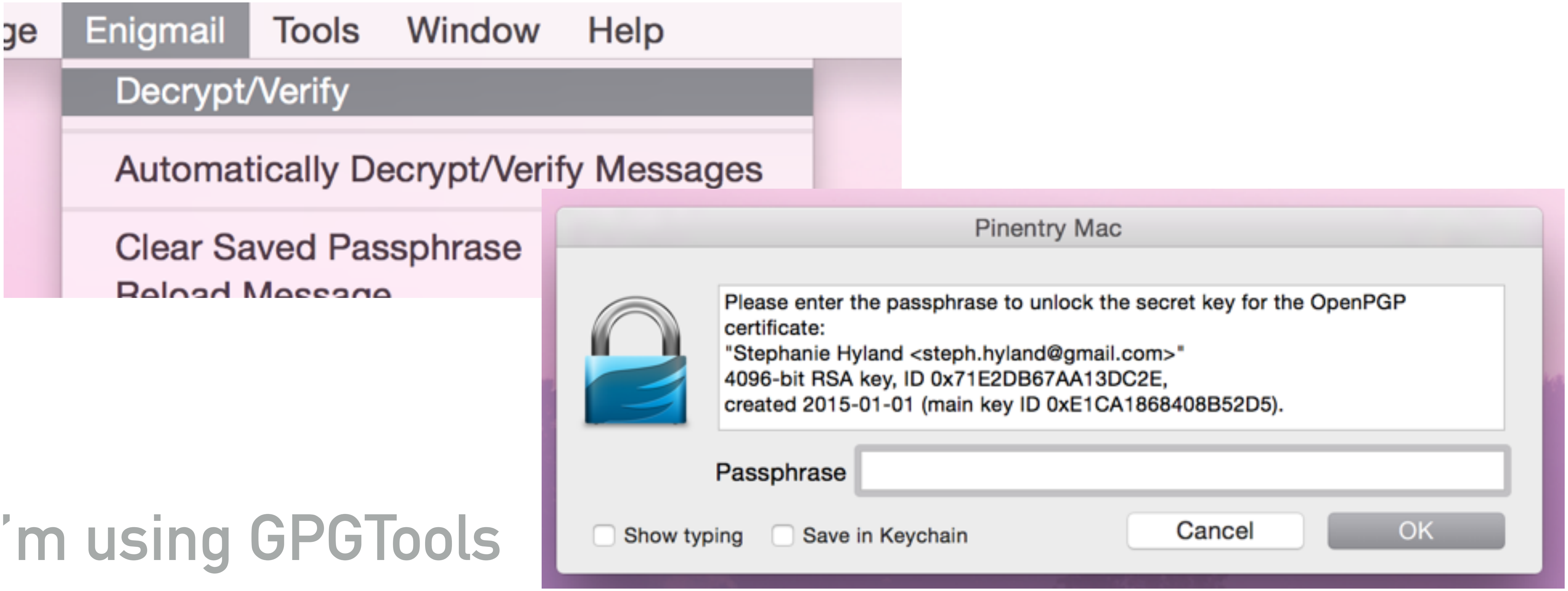
To: steph.hyland@gmail.com

Subject: An unencrypted, but signed email

```
Hi me,

This message isn't confidential,
but it has authenticity and integrity!

- S
```

Mozilla Thunderbird + ENIGMAIL

Step 5: Decrypt an email.



Pinentry Mac

Please enter the passphrase to unlock the secret key for the OpenPGP certificate:
"Stephanie Hyland <steph.hyland@gmail.com>"
4096-bit RSA key, ID 0x71E2DB67AA13DC2E,
created 2015-01-01 (main key ID 0xE1CA1868408B52D5).

Passphrase

□ Show typing □ Save in Keychain

I'm using GPGTools

in summary…

do you PGP?

Yes!

@corcra
Stephanie Hyland
4/27/15, CryptoHarlem