login as: bob

bob@localhost's password:

Last login: Wed Oct 26 07:37:09 2016 from 10.0.2.2

[bob@localhost ~]$ gpg --fingerprint James

pub 2048R/2BA7F626 2016-10-24 [expires: 2016-11-23]

Key fingerprint = CBBA 8578 9B76 2E1B 8275 DE47 587A 47B1 2BA7 F626

uid James (Hello) <Jkratohvil@una.edu>

sub 2048R/83A3F482 2016-10-24 [expires: 2016-11-23]

[bob@localhost ~]$ gpg --list-keys

/home/bob/.gnupg/pubring.gpg

----------------------------

pub 2048R/2BA7F626 2016-10-24 [expires: 2016-11-23]

uid James (Hello) <Jkratohvil@una.edu>

sub 2048R/83A3F482 2016-10-24 [expires: 2016-11-23]

[bob@localhost ~]$ gpg --import todd\_grimes.publickey

gpg: key 9C304E25: public key "Todd Grimes (Generate a key) <jgrimes2@una.edu>" imported

gpg: Total number processed: 1

gpg: imported: 1 (RSA: 1)

[bob@localhost ~]$ gpg --list-keys

/home/bob/.gnupg/pubring.gpg

----------------------------

pub 2048R/2BA7F626 2016-10-24 [expires: 2016-11-23]

uid James (Hello) <Jkratohvil@una.edu>

sub 2048R/83A3F482 2016-10-24 [expires: 2016-11-23]

pub 2048R/9C304E25 2016-10-20 [expires: 2017-10-20]

uid Todd Grimes (Generate a key) <jgrimes2@una.edu>

sub 2048R/1278AA66 2016-10-20 [expires: 2017-10-20]

[bob@localhost ~]$ gpg -d messageforKirk.gpg

You need a passphrase to unlock the secret key for

user: "James (Hello) <Jkratohvil@una.edu>"

2048-bit RSA key, ID 83A3F482, created 2016-10-24 (main key ID 2BA7F626)

gpg: encrypted with 2048-bit RSA key, ID 83A3F482, created 2016-10-24

"James (Hello) <Jkratohvil@una.edu>"

Secret message for Kirk

This is a test message.

[bob@localhost ~]$ gpg -r jgrimes2@una.edu

gpg: Go ahead and type your message ...

Hey Todd, I got your message

^C

gpg: signal Interrupt caught ... exiting

[bob@localhost ~]$ ls

gpghelp listing mykey todd\_grimes.publickey

keyfile messageforKirk.gpg test

[bob@localhost ~]$ nano test

[bob@localhost ~]$ ls

gpghelp listing messageforKirk.gpg test

keyfile message mykey todd\_grimes.publickey

[bob@localhost ~]$ gpg -r jgrimes2@una.edu -e message

gpg: 1278AA66: There is no assurance this key belongs to the named user

pub 2048R/1278AA66 2016-10-20 Todd Grimes (Generate a key) <jgrimes2@una.edu>

Primary key fingerprint: F1E9 2198 0225 5363 2ADC E02D 2F8B EB1D 9C30 4E25

Subkey fingerprint: 755C 095F 8489 F25E 214B 35D1 70D4 25CF 1278 AA66

It is NOT certain that the key belongs to the person named

in the user ID. If you \*really\* know what you are doing,

you may answer the next question with yes.

Use this key anyway? (y/N) y

[bob@localhost ~]$ ls -r

todd\_grimes.publickey mykey messageforKirk.gpg listing gpghelp

test message.gpg message keyfile

[bob@localhost ~]$ mv message.gpg messageToTodd.gpg

[bob@localhost ~]$ ls

gpghelp listing messageforKirk.gpg mykey todd\_grimes.publickey

keyfile message messageToTodd.gpg test

[bob@localhost ~]$ ls

gpghelp listing messageforKirk.gpg mykey todd\_grimes.publickey

keyfile message messageToTodd.gpg test

[bob@localhost ~]$ gpg --sign messageforKirk.gpg

You need a passphrase to unlock the secret key for

user: "James (Hello) <Jkratohvil@una.edu>"

2048-bit RSA key, ID 2BA7F626, created 2016-10-24

[bob@localhost ~]$ nano messageforKirk.gpg

[bob@localhost ~]$ nano message

[bob@localhost ~]$ ls

gpghelp message messageforKirk.gpg.gpg test

keyfile message2 messageToTodd.gpg todd\_grimes.publickey

listing messageforKirk.gpg mykey

[bob@localhost ~]$ gpg --sign message2

You need a passphrase to unlock the secret key for

user: "James (Hello) <Jkratohvil@una.edu>"

2048-bit RSA key, ID 2BA7F626, created 2016-10-24

[bob@localhost ~]$ mv message2 message2.gpg

[bob@localhost ~]$ ls

gpghelp message messageforKirk.gpg.gpg test

keyfile message2.gpg messageToTodd.gpg todd\_grimes.publickey

listing messageforKirk.gpg mykey

[bob@localhost ~]$ gpg --sign message2.gpg

You need a passphrase to unlock the secret key for

user: "James (Hello) <Jkratohvil@una.edu>"

2048-bit RSA key, ID 2BA7F626, created 2016-10-24

[bob@localhost ~]$ mv message2 messageToTodd2.gpg

mv: cannot stat ‘message2’: No such file or directory

[bob@localhost ~]$ mv message2.gpg.gpg messageToTodd2.gpg

[bob@localhost ~]$ gpg -r jgrimes2@una.edu

gpg: Go ahead and type your message ...

^C

gpg: signal Interrupt caught ... exiting

[bob@localhost ~]$ gpg -d signedMessageToKirk.gpg.gpg

▒

▒▒▒P▒9▒▒u▒V▒o!QKyZ▒񀛫▒c▒~▒#l▒▒mY-ٞ▒▒▒%▒▒▒p▒▒=▒▒f▒u1t▒▒$;-ݰ▒?Y▒▒s!g▒3cSU▒▒▒#2}vT▒▒▒&G▒▒ۺ\*▒▒▒▒\▒h▒P▒▒k▒▒▒

▒▒▒▒▒V/R▒▒t@▒▒U▒▒`▒▒o}▒{▒;>X}

▒9R▒▒=▒<Z'5

▒;O%S,'C ▒▒▒q▒U':▒▒f▒▒'▒K▒Jߞ▒

▒▒n▒W\*H▒ľ4):WI2F;u9▒▒V.▒J|ؠ▒ c%R▒>ϦY6▒aY▒A▒cxg▒▒

)Q▒bTKW;<▒▒▒▒▒!▒!o▒m]յ

▒▒▒▒R.wƷO▒H▒▒!di3u▒▒ף▒gpg: Signature made Wed 26 Oct 2016 07:51:31 AM CDT using RSA key ID 9C304E25

gpg: Good signature from "Todd Grimes (Generate a key) <jgrimes2@una.edu>"

gpg: WARNING: This key is not certified with a trusted signature!

gpg: There is no indication that the signature belongs to the owner.

Primary key fingerprint: F1E9 2198 0225 5363 2ADC E02D 2F8B EB1D 9C30 4E25

[bob@localhost ~]$