The important stuff

The quiz. Take it now

Today we have 2 deliverables in addition to the quiz:

- a gpg public key signed by 3 class members
- an export of ***MY*** public key, signed by you

These deliverables are tied to a project (and projects are 25% of your grade)...

Quiz results

- Doesn't matter, I didn't prepare a lecture
- We're having a Key Signing Party!
- if you are showing up late *take the quiz!*

Get ready to read an write a bunch of files...

It's going to be a lame party isn't it...

```
gpg --full-generate-key
```

- Use your real name and campus email!
- Use all the bits (4096)!
- Feel free to set an expiration of 16w (weeks) if you plan on throwing this away ***AT THE END OF THIS SEMESTER***
- Use a password that you will not forget!
- We will use this key again so make sure you save it!
- if you are showing up late *take the quiz!*

I have a key, now what?

```
mkijowski@pop-os: ~
mkijowski@pop-os:~$ gpg --list-keys
/home/mkijowski/.gnupg/pubring.kbx
---------------------------------
pub   rsa4096 2021-09-08 [SC]
      E47763416159625F60ACE88A7E5CF54E1BBA3984
uid           [ultimate] Matthew Kijowski (Wright State University) <matthew.kijowski@wright.edu>
uid           [ultimate] Matthew Kijowski <matthewkijowski@gmail.com>
sub   rsa4096 2021-09-08 [E]

pub   rsa4096 2021-09-08 [SC]
      FED9EA871214324B1610DE1830905307FD53CB8F
uid           [  full  ] Kayleigh Duncan <kayleigh.duncan@wright.edu>
sub   rsa4096 2021-09-08 [E]

mkijowski@pop-os:~$ gpg --armor --export matthew.kijowski@wright.edu
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGE5KPwBEADT7K1SzLMsDsHV9stUM2TzhBwTPNM5PU/NxsZd3tfw2tRbCi3R
wGmGf/Z/NIpneziUdhB6ovVaTrPDaPYjqJUYQ/J0vq+8hDmPj46m8gKaR4+8jQKR
XjmlEjilMeH7tL98QciLy5guTBlLxV7oZo0OBOECeA6K+chgXWpd+02j9gZFnS/T
/BhQLIGvR2lVc0f3i3M6v0jf2vKif4S4FehYmroeAB36VIoWfBX/RMdfGheBApUL
e3JCOFxkdRD78lT3AzM1wXXI55XoOjXr3rI8V3CX98PnQW8uZ4IisesWMfQIgVid
Xc14GaxtJHUH+sgZ5ngeN0C55Jt4QYmx7Xk1NWrZ1nq6WE5tmMQMKNgFO18macm2
U1OUJ0C684bMaL1fVy3TioxxHXgbY/EOO3kSay26OA6LwDJt7SbZ6IyzVilCoPeU
gn98WDGsQcWFbUN/rGWgfbi/szLK3HY2e3if2E2cCggyp2gn3vMXrxEGlciLDH4B
sSOgPbwGYVC8vGknO4JNZigt/DNOiIwcSEkJDttSpW/aki3FNDampzJRdFmq1inf
```

Use your campus email and your name/initials for the above!

- if you are showing up late *take the quiz!*

Import my public key

I sent it out this morning over email. Copy and paste the contents into a file in linux and import it with:

- `gpg --import kijowski.gpg`
- OR: `gpg --import kijowski.gpg.pub.txt`

Check to make sure the fingerprint matches:

```
E477 6341 6159 625F 60AC  E88A 7E5C F54E 1BBA 3984
                                7E5C F54E 1BBA 3984
```

- `gpg --edit-key matthew.kijowski@wright.edu`
- `sign`
- `save`
- `gpg --armor --export matthew.kijowski@wright.edu`

Return this key to me via pilot dropbox!

Lets party!

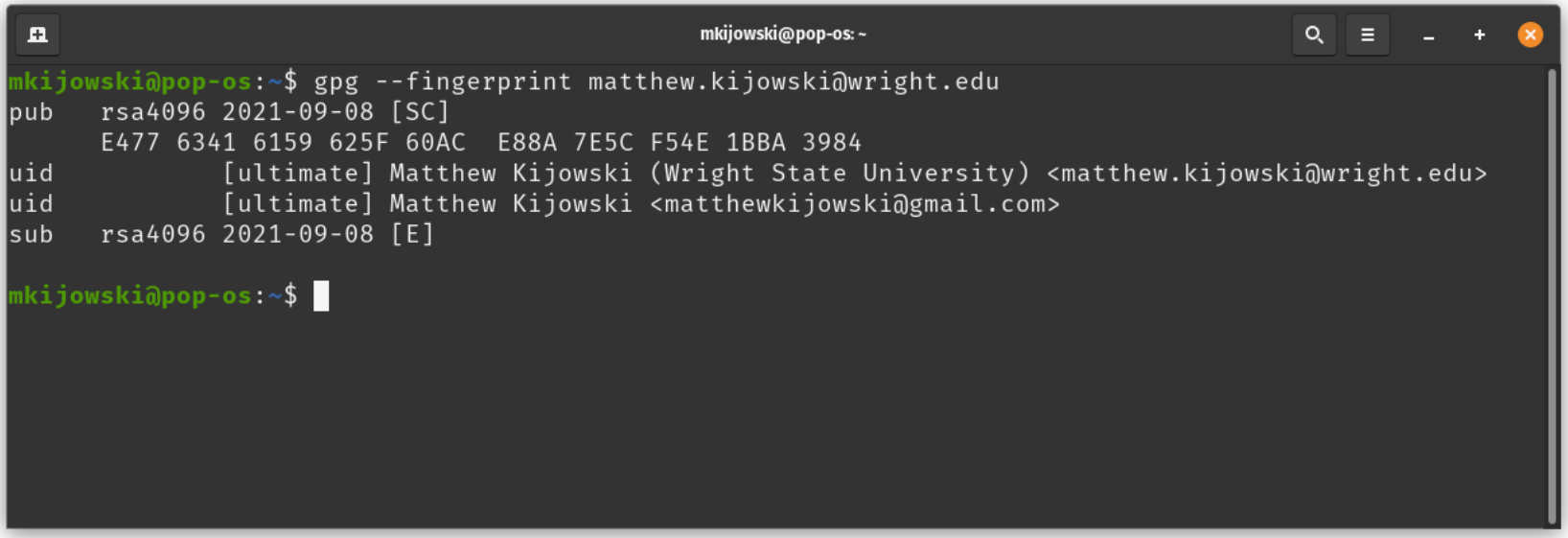

Figure 1: kijowski-fingerprint

- Convince your table mates that you are the person with the given email and share your fingerprint!
- Exchange public keys

Sign each other's keys

- For each public key
  - `gpg --edit-key their.email@wright.edu`
  - check that the fingerprint matches
  - if it does `sign` then `save`
- To help build a trust network you can provide them proof of your signature
  - `gpg --armor --export their.email@wright.edu`
- They can then import this file to add your signature to their key
  - `gpg --import filename`
- Re-export your key after you import a new signature!
  - `gpg --armor --export name@wright.edu`
- Do this for at least a couple students at your table

Among your table (and Discord)

- Download/copy/paste each person's public key from discord
- Make a file in your home directory for each key
- Files should start with `-----BEGIN PGP PUBLIC KEY BLOCK-----`
- Import with the following

```
gpg import <filename>
```

What to do with your public key

- Upload it to Discord (use back-tics to make it a code block)
- Upload to pilot dropbox!

```
gpg --fingerprint matthew.kijowski@wright.edu
```

Signed sealed delivered

Lets sign a message!

- Create a `sample.txt` file with a public message (Hello World or some such thing).
- `gpg --sign sample.txt`
- share the output sample.gpg with someone you exchanged keys with
- `cat` the output file, can you read the contents?
- `gpg --verify sample.gpg`

Now for some fun

Lets send a secret message!

- Create a text file `secret-message.txt`
- Choose someone you have exchanged keys with
- Encrypt the file: `gpg --output secret-message.gpg --encrypt --recipient their.email@wright.edu`
- Send them `secret-message.txt` via email or discord
- The recipient can decrypt with:
  - `gpg --output secret.txt --decrypt secret-message.gpg`

Back up your gpg keys!!!

```
tar -cpzf gnupg.tar.gz ~/.gnupg/
```

if you are using a Wright State laptop

```
cp gnupg.tar.gz /mnt/c/Users/student/Desktop/
```

Save this file!!!

You can also backup your private key and any public keys with:

- `gpg --armor --export-secret-key your.email@wright.edu`
- `gpg --armor --export your.email@wright.edu`
- `gpg --armor --export friends@wright.edu`