

regpg
safely store server secrets

Tony Finch
<fanf2@cam.ac.uk>
<gitmaster@uis.cam.ac.uk>

Network Systems (RNB 1N52)

Tuesday 21st November 2017



UNIVERSITY OF
CAMBRIDGE

University Information Services

agenda

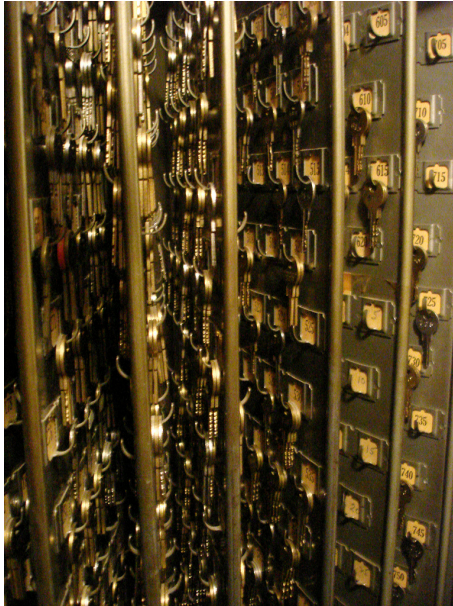
■ Context

- secrets?
- server?
- store?
- safely?
- gpg?
- re?

■ Demo

- keys
- secrets
- recrypt
- X.509 / TLS
- Ansible
- conversion

secrets



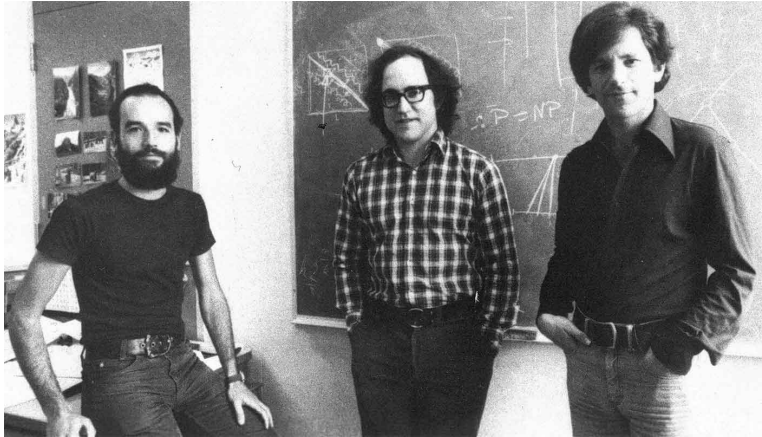
<https://www.flickr.com/photos/fuzzy/3196534149>

secrets – encryption



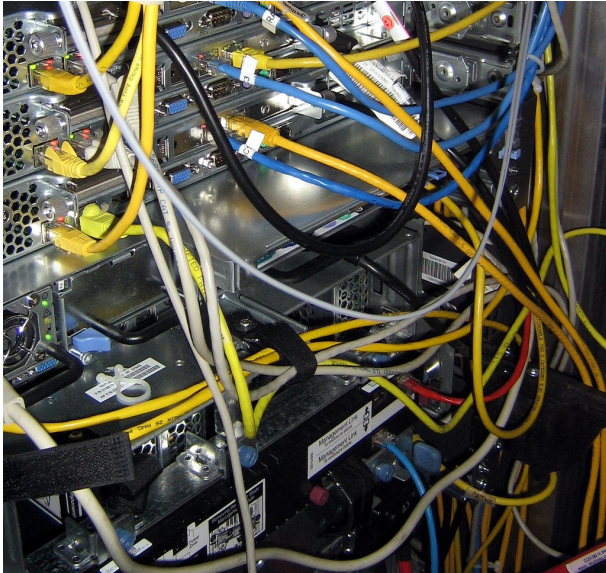
<https://richardskingdom.net/wp-content/uploads/2014/04/encrypt-all-the-things.png>

secrets – Shamir / Rivest / Adleman



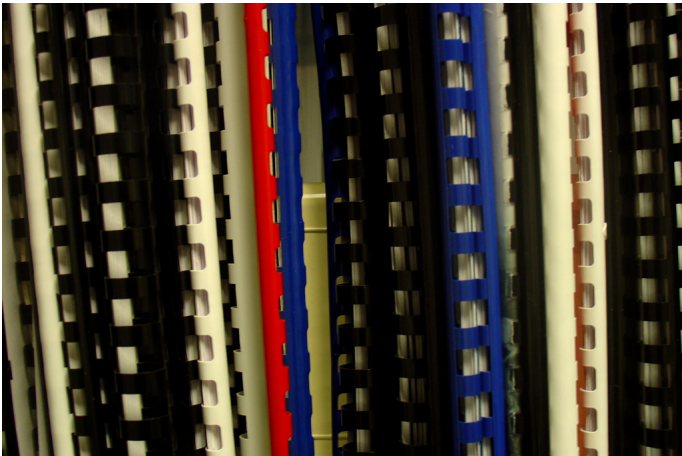
<https://claudiodinardo.com/content/images/2017/08/shamir-rivest-adleman.jpg>

server



<https://www.flickr.com/photos/evilnick/183967344>

server – files



<https://www.flickr.com/photos/lnx/7297731>

store – not share



<https://www.flickr.com/photos/23605686@N05/6921691127>

safely – hazmat containment



<https://www.flickr.com/photos/mamboman/3698344360>

safely – situational awareness



<https://www.flickr.com/photos/109570752@N02/15118828431>

gpg



https://commons.wikimedia.org/wiki/File:Gnupg_logo.svg

regpg



<https://dotat.at/prog/regpg/>

dependencies

■ prerequisites

- perl
- gnupg
- gnupg-agent
- pinentry-*

■ helpers

- ansible
- git
- openssl
- openssh-client
- xclip

check gpg-agent

- `echo $GPG_AGENT_INFO`
- `eval $(gpg-agent --daemon)`

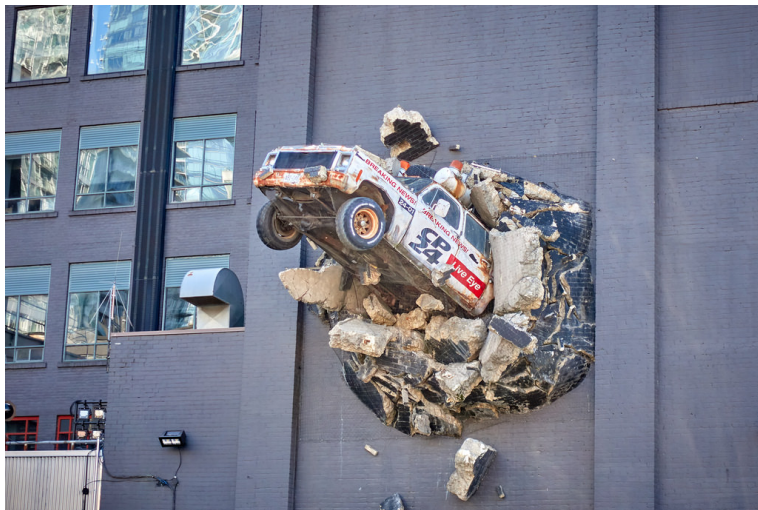
install

- quick
 - `cd ~/bin`
 - `curl -O https://dotat.at/prog/regpg/regpg`
- home page <https://dotat.at/prog/regpg/>
 - supporting documentation
 - distribution tar balls
 - test suite

generate key

- Generate a key just for `regpg`
- Separate from your other `gpg` keys (if any)
- `gpg --gen-key`
- Answer the quiz

generate key – demo



<https://www.flickr.com/photos/eugenuity/34113551603>

manage keys

- addkey
- addself ⇐⇐
- delkey ⇐⇐
- exportkey
- importkey
- lskeys ⇐⇐

manage keys – demo



<https://www.flickr.com/photos/bantam10/3068761016>

secrets

- encrypt 
- decrypt 
- recrypt
- edit 
- pbcopy
- pbpaste
- shred 
- check 

secrets – demo

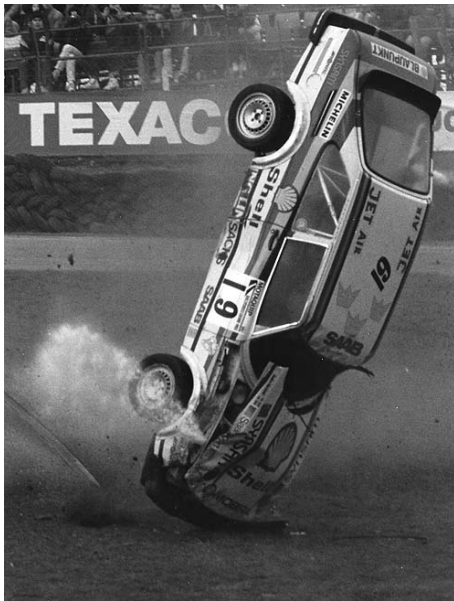


<https://www.flickr.com/photos/zapthedingbat/516726771>

recrypt

- delkey ⇐⇐
- importkey ⇐⇐
- lskeys ⇐⇐
- recrypt ⇐⇐
- check ⇐⇐

recrypt – demo



<https://www.flickr.com/photos/parkstreetparrot/6531496943>

generate TLS / ssh

- gencsrconf 
- gencsr 
- genkey 
- genpwd

generate TLS / ssh – demo



<https://www.flickr.com/photos/zapthedingbat/516726771>

set up hooks

- init 
- init git 
- init ansible 
- init ansible-vault

set up hooks – demo



<https://www.flickr.com/photos/walkingsf/8143196966>

converters

- `conv ansible-gpg` 
- `conv ansible-vault` 
- `conv stgza`

converters – demo



<https://www.flickr.com/photos/eltpics/15367149536>

Questions?



<https://www.flickr.com/photos/debord/4932655275>