

Logging into mantis.mathcs.carleton.edu
w/o a password

- ① Create a public private key pair
 (n, e) (n, d) `ssh-keygen`
- ② Copy (n, e) to my account on mantis.
public

I wanna login to mantis

ssh jondich@mantis. _____

SSH client
(my laptop)

ssh server
(sshd running on mantis)

TCP handshake
← encrypt R for me →

"random"

→ $E((n,d), R)$

server decrypts
this w/ (n,e)
to see if I
actually had d

RSA
Need agreements on file formats
& key structure

RSA corporation created
specs ~ document series
called "PKC"

