

Class 36: Public Key Crypto



CS150: Computer Science
University of Virginia
Computer Science

David Evans

<http://www.cs.virginia.edu/evans>

Login Process

Terminal

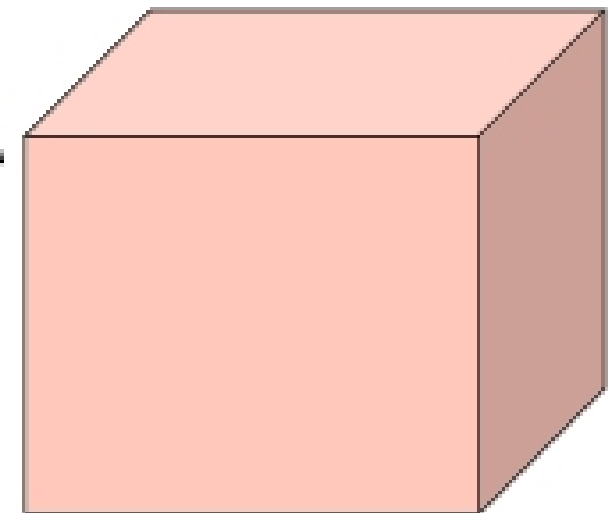
```
Login: alyssa  
Password: fido
```

login sends
<"alyssa", "fido">



Eve

Trusted Subsystem



Password Problems

- Need to store the passwords
 - Dangerous to rely on database being secure
- Need to transmit password from user to host
 - Dangerous to rely on Internet being confidential

Lecture 31, Recap Now

Today

