Generating SSH Public/Private Keys
(for authentication)
Password-Based Authentication

• Most commonly used method of authentication
  E.g.: You can log in to your CPSC account (via SSH) as follows on the CPSC server(s) available at:

  http://www.cpsc.ucalgary.ca/tech_support/services/remote_access
  
  `ssh username@servername`
  
  `username@servername`’s password:

• But, as demonstrated in the lecture on Friday, some security pitfalls exist over use of passwords

• Public key-based authentication offers better security

• You do not have to throw your PII on the wire...!
Public Key-Based Authentication

- Generate a public/private key pair
- The public key resides on the system you are logging in to
- The private key resides on the system you log in from
- The system you log in from should be a “trusted” system that you own
- The public key can be visible to anyone, while the private key must be kept secret; only known to you
Public Key-Based Authentication – Cont’d

• No need to send login information (e.g., password) out on the wire, when authenticating to a system

• Main advantage of key-based authentication: key values are more difficult to brute-force than plain passwords (especially with good key lengths – 2048 (default); 4096)
Class Activity

Now, let’s generate our RSA key pairs and authenticate to a CPSC server by means of our public/private key pairs