Tutorial 1

Outline

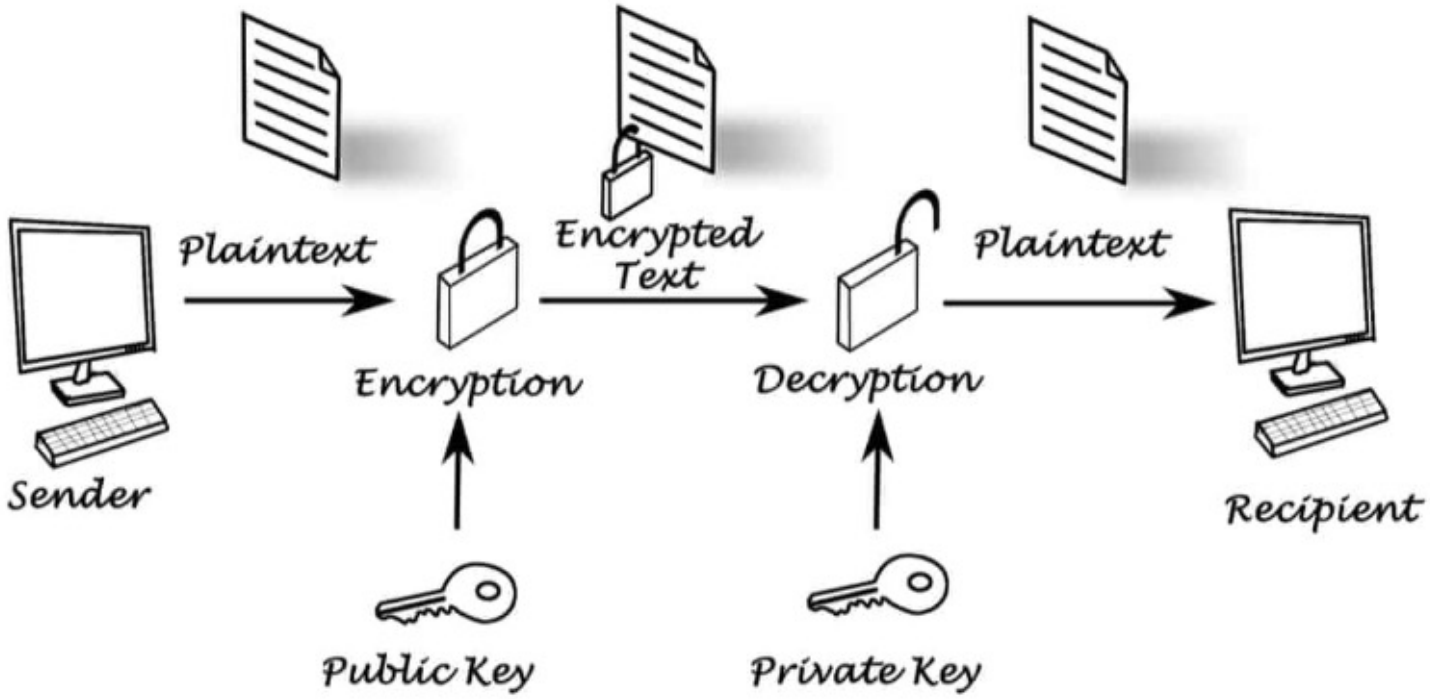
- SSH for authentication
  - Definitions
  - Concepts of Important Components
    - Public key
    - Private key
  - Try it out by yourself!

Definitions

- **Secure Shell Protocol (SSH)** - a common method for remote login to another computer which is secure.
- **server** - a secured machine you are SSHing into. The server sits and waits to be contacted.
- **client** - usually your machine. The client initiates contact with the server.

Important Components of SSH key-based authentication

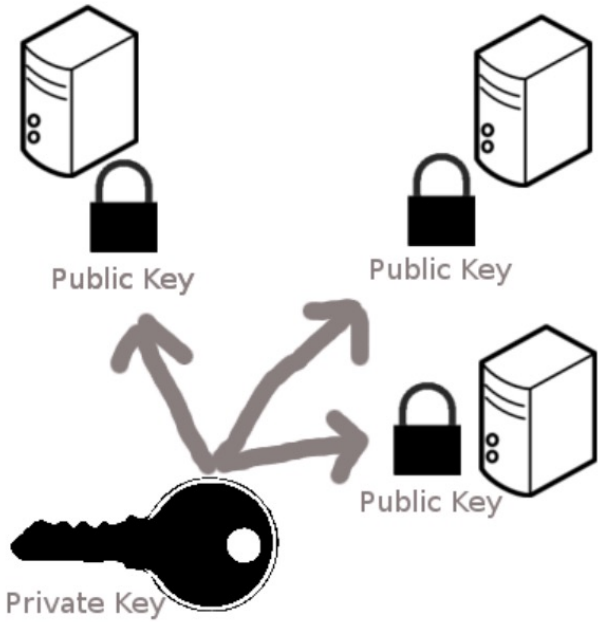
- Public Key:
  - CAN encrypt messages
  - But CANNOT decrypt messages generated by the private key
- Private Key:
  - CAN decrypt messages generated by the public key



- How to generate keys:
  - using ssh-keygen, to make private key (usually called id_ed25519) and a public key (usually called id_ed25519.pub)

- Public key (padlock):
  - Could make copies(id_ed25519.pub) and put anywhere
  - Encrypt the messages

- Private key (key):
  - Decrypt the message



Keep Private Key Safe!

- ssh-keygen allows you to put a passphrase on the private key
- this should be shared with NO ONE!
- if your private key does fall into the wrong hands, the person must still know the passphrase to use the private key

Now, it’s your turn!

Try to set up SSH for authentication on Github by yourself!