Week 9
Digital Signatures

6 March 2019

CS 35L Lab 4

Jeremy Rotman

Announcements

- Assignment #8 is due Saturday by 11:55pm
- For Assignment #10
  - **Email me to tell me what story you are choosing**
  - Here is the link to see what stories people have signed up for already
    - Choose a story at least one week before you present
- Submission for Assignments #8 and #10 will be done on CCLE, there will be a link specific to our lab
- Reminder for future assignments:
  - Assignments #9 and #10 DO NOT allow late submissions
- Question for Presenters today

Outline

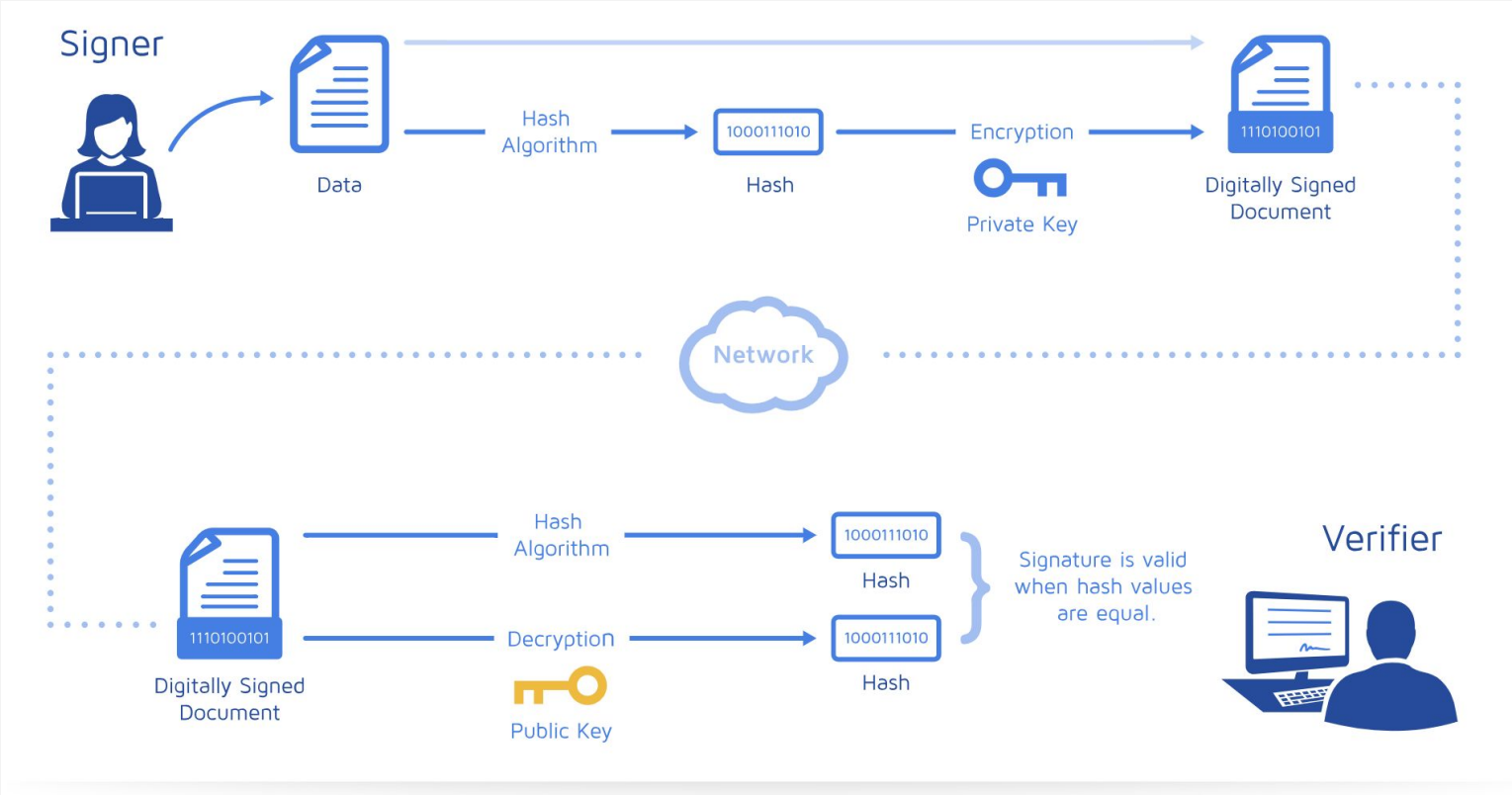
- ➔ Digital Signatures
- ➔ Assignment 8

Questions?

Digital Signatures

- Electronic stamp or seal
  - Certifies and timestamps the document
  - Acts like a handwritten signature, but also adds more
- Digital Signatures are tamper-proof
  - This ensures data integrity
  - If the file is changed after being signed
    - The signature cannot be verified

Digital Signatures



Detached Digital Signatures

- A digital signature must compress the original document
  - This is not always ideal
  - A clearsigned document is an option
    - But the document must still be edited in some way
- What to do if you are signing a tarball?
- A detached digital signature is stored and transmitted in a file that is separate from the original file
  - Both must be used in the verify command to verify the signature

Homework 8

- ➔ Make sure to answer the two questions in the homework
- ➔ You will have to generate a keypair with gpg
  - ◆ You will submit the public key
- ➔ You will then have to copy the file
  - ◆ /sys/bus/i2c/devices/0-0050/eeprom
  - ◆ This is in your beaglebone
    - Electrically Erasable Programmable Read-Only Memory
    - It holds board information
      - Manufacture, revision, and pin-usage
- ➔ Use your private key to generate a detached signature for this file

Homework 8

- You will submit
  - hw-pubkey.asc
    - Your public key generated for the homework
  - hw.txt
    - The answers to the homework questions
  - eeprom
    - The copy of the file from your beaglebone
  - eeprom.sig
    - The detached signature for your eeprom file
  - log.txt
    - Your lab log (from the lab section)

Homework 8

- For help on things related to gpg
  - Generating keypairs, and creating signatures
  - This manual might help

Questions?