Week 9
Digital Signatures

28 November 2018

CS 35L Lab 4

Jeremy Rotman

Announcements

- Assignment #8 is due Saturday by 11:55pm
- Assignment #10 Presentations
  - **Email me to tell me what story you are choosing**
  - Here is the link to see what stories people have signed up for already
- Quick reminder for the upcoming assignments (9 and 10)
  - No late submissions
- Potentially changing presentation dates
  - If people feel like they need more time in lab today for the assignment

Outline

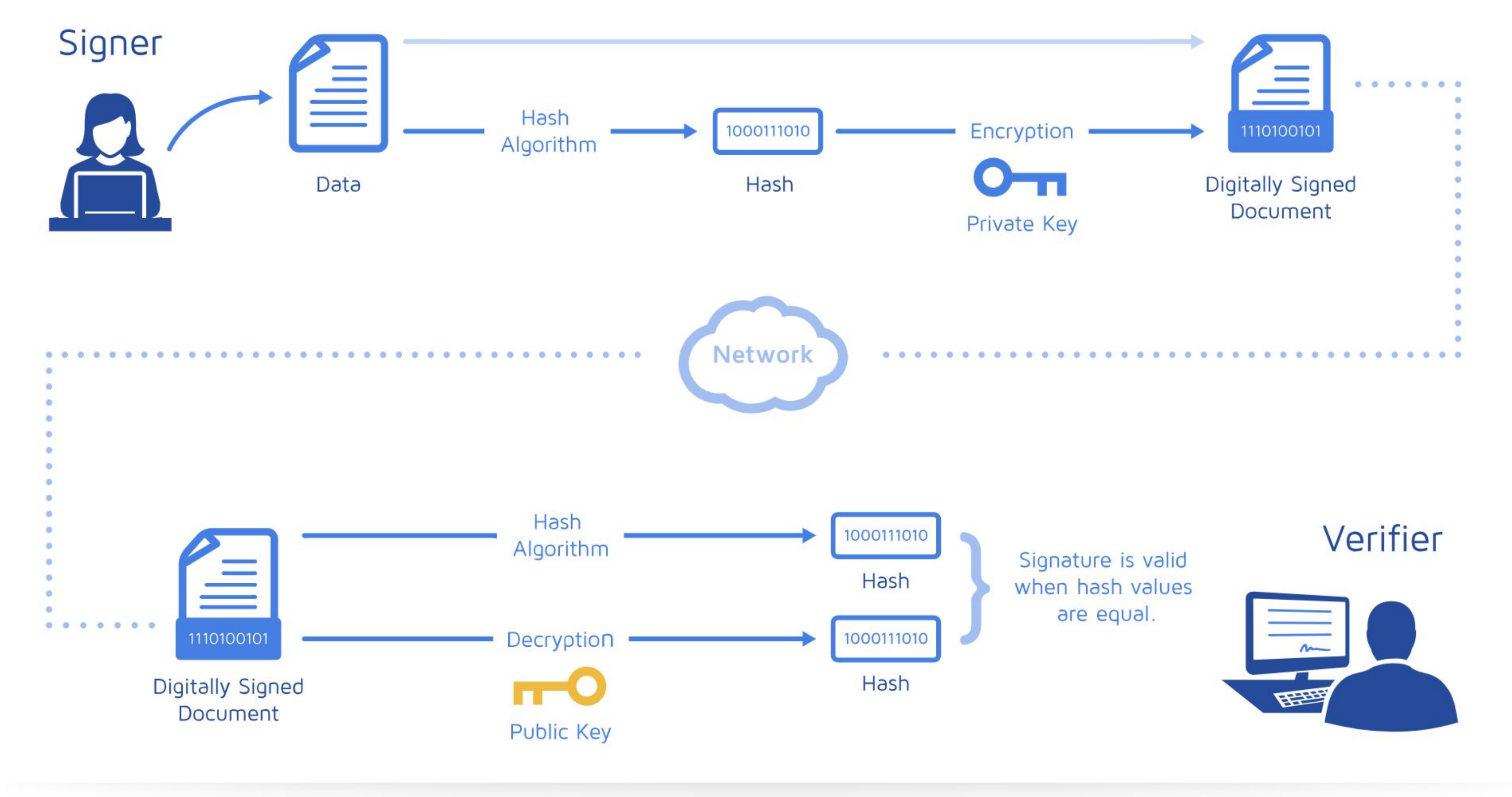
- ➔ Digital Signatures
- ➔ Assignment 8

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

Lab 8

- Debugging for the lab portion
  - If you are using a used BeagleBone
    - You must reset the device
    - I have a microSD that should have the latest software image for the reset
  - For MacOS
    - Make sure to download the drivers from the alternate page, and follow the troubleshooting step in the Piazza setup post
      - If you are getting driver installation issues for newer MAC OS X versions and could not turn the second step green, download the driver located on HERE.
      - Afterwards, run "sudo rm -rf /System/Library/Extensions/HoRNDIS.kext" and restart your computer.

Lab 8

- ➔ Debugging for the lab portion
  - ◆ If you are on Windows and are having errors installing the drivers
    - You are likely encountering issues with verification of the driver signatures
    - Following these steps have fixed it for some students
- ➔ For help on things related to gpg
  - ◆ Generating keypairs, and creating signatures
  - ◆ This manual might help

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)

Questions?