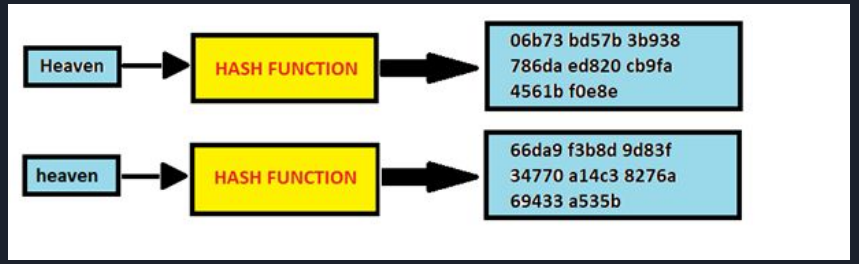
SHA-1 Algorithm

Presenters: Elizabeth Hwang, Derek Mata, Christopher Yamada

SHA-1: A Quick Summary

- What is it
  - Stands for “Secure Hashing Algorithm”
  - A hashing algorithm is useful for shortening input data into a smaller form. This form cannot be understood by bitwise operations, modular additions, and compression functions.
- Why do we need it
  - Prevent hackers from taking valuable information
  - Digital certificates to validate users/sites
- Common applications/examples
  - Apps like SSH need security and protection via SSL/TLS



Reference: *https://www.encryptionconsulting.com/education-center/what-is-sha/*

Experimental Methodology

- Develop hashing algorithm using python3
- Run algorithm on 3 embedded computers using same interpreter
  - Raspberry Pi 3B+ - (1GB)
  - Raspberry Pi 4 - (4GB)
  - Jetson Nano 2GB
- Compile data from all 3 tests
  - Elapsed time of whole program
  - Average CPU usage
  - Average Memory usage
- Determine best computer based on:
  - Performance
  - Cost

Gantt Chart

Link for our project Gantt Chart:

https://docs.google.com/spreadsheets/d/1cZGLI5sTm5Qg32X9O2FckCiZgqcl7iHQV7iH6phKpFE/edit?usp=sharing