Sprint #4

Timeframe: April 27 - May 4

April 28
April 29
May 1
May 4

Scrum Board and Charts: Link

- Ana - Scrum Master
- Ivins - Dev Team
- Jacob - Project Owner
- Jonathan - Dev Team
- Mark - Dev Team
- Victor - Dev Team

May 4

- **Ana**
  - Progress: more work on RSA attack - small private key attack (not complete)
  - Blocks: I went home and other classes
  - Future: finish attack and organize RSA
- **Ivins**
  - Progress: finished RSA (looked into OpenSSL)
  - Blocks: Speak with Yin about use of OpenSSL
  - Future: Verifying necessity of OpenSSL
- **Jacob**
  - Progress: started working on stego attack
  - Blocks: already finished by another group member
  - Future: prepare for final submission
- **Jonathan**
  - Progress: finished CSV
  - Blocks: none
  - Future: prepare for final submission
- **Mark**
  - Progress: wrote Chinese Remainder Theorem
  - Blocks: none
  - Future: prepare final submission
- **Victor**
  - Progress: worked on stego attack, tests CSV attacks
  - Blocks: already finished by another group member
  - Future: prepare for final submission

May 1

- **Ana**
  - Progress: started on a small private key attack
  - Blocks: chinese remainder theorem
  - Future: continue working on attack
- **Ivins**
  - Progress: working on decryption, started on OpenSSL
  - Blocks: large numbers are passing back to many blocks
  - Future: work on OpenSSL
- **Jacob**
  - Progress: Research for attacks on text based stego
  - Blocks: picking a new stego implementation
  - Future: plan future attacks
- **Jonathan**
  - Progress: new stego implementation (Excel)
  - Blocks: picking new stego implementation
  - Future: converse with teammates and start new stego implementation
- **Mark**
  - Progress: finished Fermat's attack
  - Blocks: none
  - Future: work on 3rd RSA attack
- **Victor**
  - Progress: researched new stego attack
  - Blocks: other classes
  - Future: work on new stego implementation

April 29

- **Ana**
  - Progress: Nothing
  - Blocks: Linear Algebra
  - Future: Add bounds to Pollard (p-1) attack
- **Ivins**
  - Progress: started decoding and decoding test cases
  - Blocks: google tests yield seg faults
  - Future: fixing seg faults in test cases and speak with Yin about OpenSSL
- **Jacob**
  - Progress: Nothing
  - Blocks: CSCE 313 (MP5)
  - Future: Sudoku stego attack
- **Jonathan**
  - Progress: Started final presentation
  - Blocks: none

    - Future: continue working on presentation
- **Mark**
    - Progress: Nothing
    - Blocks: classes
    - Future: optimize Fermat's, Chinese Remainder Theorem
- **Victor**
    - Progress: Nothing
    - Blocks: other classes
    - Future: combine encoder/decoder with solver for Sudoku stego, find attack method

April 28

- **Ana**
    - Progress: Pollard (p-1) attack implemented
    - Blocks: none
    - Future: input bounds into Pollard's attack
- **Ivins**
    - Progress: Scrapped original RSA, now using base 94 encryption
    - Blocks: Chem Test
    - Future: Start Attack 3
- **Jacob**
    - Progress: Finished Test cases and solver
    - Blocks: CSCE 313 (MP5)
    - Future: start the last attack
- **Jonathan**
    - Progress: Nothing
    - Blocks: none
    - Future: Start on Presentation
- **Mark**
    - Progress: Nothing
    - Blocks: Classes
    - Future: Improve the square root of n attack for RSA
- **Victor**
    - Progress: finished encoding/decoding for stego
    - Blocks: other classes
    - Future: combine encoder/decoder with solver for Sudoku stego, find attack method