

Project 4 Specification Notes

<2015-04-09 Thu>

Contents

| | | |
|----------|--|----------|
| 1 | Dates | 2 |
| 1.1 | TODO Sprint #1 | 2 |
| 1.2 | TODO Sprint #2 | 2 |
| 1.3 | TODO Sprint #3 | 2 |
| 1.4 | TODO Sprint #4 | 2 |
| 1.5 | TODO All Deliverables | 2 |
| 1.6 | TODO Final Presentation | 2 |
| 2 | Design Choices | 3 |
| 2.1 | C++14 | 3 |
| 2.2 | Test Driven Development | 3 |
| 2.3 | Git-Flow | 3 |
| 3 | Requirements | 4 |
| 3.1 | Workflows | 4 |
| 3.2 | Features | 4 |
| 4 | Rubric | 6 |
| 4.1 | RSA Cryptosystem (15 pts) | 6 |
| 4.2 | Attacks on RSA (15 pts) | 6 |
| 4.3 | LSB image stegosystem (15 pts) | 6 |
| 4.4 | Attacks on LSB image stego: (15 pts) | 6 |
| 4.5 | Weekly Sprint progress reports: (20 pts) | 6 |
| 4.6 | Final Presentation (20 pts) | 6 |

1 Dates

1.1 TODO Sprint #1

SCHEDULED: <2015-04-06 Mon>-<2015-04-13 Mon>
DEADLINE: <2015-04-13 Mon 23:59>

1.2 TODO Sprint #2

SCHEDULED: <2015-04-13 Mon>-<2015-04-20 Mon>
DEADLINE: <2015-04-20 Mon 23:59>

1.3 TODO Sprint #3

SCHEDULED: <2015-04-20 Mon>-<2015-04-27 Mon>
DEADLINE: <2015-04-27 Mon 23:59>

1.4 TODO Sprint #4

SCHEDULED: <2015-04-27 Mon>-<2015-05-05 Tue>
DEADLINE: <2015-05-05 Tue 23:59>

1.5 TODO All Deliverables

SCHEDULED: <2015-05-05 Tue 23:59>
DEADLINE: <2015-05-05 Tue 23:59>

1.6 TODO Final Presentation

SCHEDULED: <2015-05-11 Mon 10:30>-<2015-05-11 Mon 12:30>
DEADLINE: <2015-05-11 Mon 10:30>-<2015-05-11 Mon 12:30>

2 Design Choices

2.1 C++14

- Use `build.tamu.edu`
 - `gcc-4.9.2` (add `share/examples/bashrc` to your `~/.bashrc`)
 - `linux x86_64`

2.2 Test Driven Development

- Google Test
- TDD Proof
 - `travis-ci`
 - * Requires committing and **pushing**¹ failing tests (so `travis-ci` builds and runs them)
 - * Gives us time-stamped builds and test runs for **every** commit and pull-request

2.3 Git-Flow

- `git flow`
 - Makes following the git-flow branching model stupidly easy
 - Use `feature/FEATURE_NAME` branches for new additions
 - * keep these specific and small
 - When a feature is done, create a pull request
 - * allows `travis` to test if your branch builds
 - * allows the rest of the group to discuss the feature

¹Shouldn't be a problem except for Chris

3 Requirements

3.1 Workflows

3.1.1 Agile

- 1-week sprints
 - At beginning of each week:
 - * Choose features from product back-log to include in this sprint
 - At end of each week:
 - * Unfinished tasks go back in back-log
 - * Demonstrate sprint's result to TA
 - * Submit to CSNet:
 - Backlogs
 - Burn-down Charts
 - Sprint Status Charts
- 4 scrums/week
 - Ask each group member (and record):
 1. "What have you done since last scrum meeting?"
 2. "What has impeded your work?"
 3. "What do you plan on doing between now and next scrum?"
 - At end of meeting:
 - * Each team-member should update burn-down chart:
 - remaining effort for each task
 - status of tasks
- As soon as product is finished submit to CSNet

3.1.2 TDD

- Provide proof

3.2 Features

3.2.1 Encryption

- Encrypt to cipher-text
- Embed cipher-text in a .bmp image

3.2.2 Decryption

3.2.3 Crack

4 Rubric

- 4.1 RSA Cryptosystem (15 pts)
- 4.2 Attacks on RSA (15 pts)
- 4.3 LSB image stegosystem (15 pts)
- 4.4 Attacks on LSB image stego: (15 pts)
- 4.5 Weekly Sprint progress reports: (20 pts)
- 4.6 Final Presentation (20 pts)