`Cry` – Project 2
(Software Requirements Specification): Interview

Daniel Dunning, Michael Degraw, Vu Phan

2017-02-13

Contents

1 Questionnaire

1.1 Introduction

- We are `Team Crybabies` (Daniel Dunning, Michael Degraw, Vu Phan).
- We would like know what you think about our `Cry` cryptographic framework.
- This interview is part of the 2017 Spring Texas Tech University Computer Science Capstone class instruced by Dr. Sunho Lim.
- The log and summary of this interview would be accessible only by members of the class (no object-oriented pun intended).
- Your participation is entirely voluntary.
- We appreciate your help.

Question 1. Would you participate in this interview?

Question 2. May we record the audio of this interview? (The recorded interview would be accessible only by `Team Crybabies`.)

1.2 Planned Functionality

Question 3. The `Cry` cryptographic framework will briefly describe whether your created cryptographic algorithm is breakable within a given time frame. Would it be helpful to have a more detailed report? If so, what other infomation should be on that report?

Question 4. `Cry` will have some built-in cryptographic algorithms, including *RSA* and *ElGamal*. What other cryptographic algorithms (such as hashing algorithms and network stream ciphers) should be included and why?

1.3 Requested Functionality

Question 5. If `Team Crybabies` were to add additional functionality to `Cry`, what one feature would be most beneficial to you and why?

Question 6. If you could change one thing about the current state of `Cry`, what would it be and why?

1.4 Conclusion

Thank you so much.

2 Log

2.1 Interviewer: Daniel Dunning

Answer 1. Put their answer here.

Answer 2. Put their answer here.

Answer 3. Put their answer here.

Answer 4. Put their answer here.

Answer 5. Put their answer here.

Answer 6. Put their answer here.

2.2 Interviewer: Michael Degraw

Answer 1. Put their answer here.

Answer 2. Put their answer here.

Answer 3. Put their answer here.

Answer 4. Put their answer here.

Answer 5. Put their answer here.

Answer 6. Put their answer here.

2.3 Interviewer: Vu Phan

Answer 1. Yes. You may personally identify me.

Answer 2. Yes.

Answer 3. Yes:

- probability of sucessful cryptanalysis
- RAM usage
- number and utilization of CPUs

Answer 4.

- symmetric *AES*
- hash function and digital signature

Answer 5. random number generator with good seed and entropy

Answer 6.

- use GMP (GNU Multiple Precision Arithmetic Library)
- start coding...

3 Summary

One summary for all interviews here.