Cry – Project 2 (Software Requirements Specification): Presentation

2017-02-13

Daniel Dunning, Michael Degraw, Vu Phan

Section 1

Introduction

Subsection 1

Scope

Scope

- `Cry` will allow cryptographers to quickly develop new cryptosystem s
  - It will do so by making testing and benchmarking easier
- `Cry` will also allow the encryption/decryption of data

Subsection 2

Definitions, acronyms, and abbreviations

Definitions

- `Cry`: The cryptographic benchmarking system under development
- `Team Crybabies`: The team responsible for the development of `Cry`
- **cryptographer:** The target audience for `Cry`

Subsection 3

References

References

- **GNU Multiple Precision Arithmetic Library:** https://gmplib.org/
- **Msieve:** https://github.com/radii/msieve

Section 2

Overall description

Subsection 1

Product perspective

Product Perspective

- `Cry` will be implemented as a stand-alone framework, with built in libraries updated as needed.
- User interface will start as command line-based, possibility of implementing with GUI

Subsection 2

Product functions

Product Functions

Testing

- Develop new cryptosystems
- Test cryptosystems against cracking techniques and generate helpful output

Reporting

- Users will receive feedback from output of their test
- Reports will be shown to suggest the security of the cryptosystem and to give helpful feedback in the area of weaknesses in the cryptosystem.

Subsection 3

User characteristics

User Characteristics

Users will most likely have a medium to high level of experience cryptosystems.

Subsection 4

Constraints

Constraints

- Basic memory and CPU availability
- Further library implementations or updates may require parallel operation or interfacing with other applications

Subsection 5

Assumptions and dependencies

Assumptions and dependencies

Only assumption of the system (`Cry`) is that it has applicable adminstrative permissions at the command line

Section 3

Specific requirements

Section 4

Conclusion

Q & A

https://github.com/vuphan314/cry