Cry – Project 2 (Software Requirements Specification): Presentation

2017-02-13

Daniel Dunning, Michael Degraw, Vu Phan

1 Introduction
- Scope
- Definitions, Acronyms, and Abbreviations
- References

2 Overall Description
- Product Perspective
- Product Functions
- User characteristics
- Constraints
- Assumptions and Dependencies

3 Specific Requirements
- Interface
- Performance
  - Key Generation
  - Encryption
  - Decryption
  - Cryptanalysis
- Classes

4 Conclusion

Section 1

Introduction

Subsection 1

Scope

Scope

- Cry will allow cryptographers to quickly develop new cryptosystems
    - 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

The only assumption of `Cry` is that it has applicable administrative permissions at the command line

Section 3

Specific Requirements

Subsection 1

Interface

- `Alice` wants to send a confidential message to `Bob`.
- `Eve` wants to eavesdrop that message.

Subsection 2

Performance

Minimum hardware

RAM	4 GB
CPU	1.5 GHz

Bob

Input:

```
$ cry generatekeys -cryptosystem=<cryptosystem>
```

Output:

```
The public & private keys are <public key> & <private key>
(took <key-generation time>).
```

Alice

Input:

```
$ cry encrypt -cryptosystem=<cryptosystem> \
> -publickey=<public key> -plaintext=<plaintext>
```

Output:

```
The ciphertext is <ciphertext> (took <encryption time>).
```

Requirements:

- `<plaintext>` is an obviously meaningful string, such as `‘‘Eve is just a crybaby.’’`
- `<ciphertext>` is an apparently meaningless string, such as `‘‘sdofAOVI29347asdjkADB234’’`

Bob

Input:

```
$ cry decrypt -cryptosystem=<cryptosystem> \
> -privatekey=<private key> -ciphertext=<ciphertext>
```

Output:

```
The plaintext is <plaintext> (took <decryption time>).
```

Eve

Input:

```
$ cry cryptanalyze -cryptosystem=<cryptosystem> \
> -publickey=<public key> -ciphertext=<ciphertext>
```

Output:

```
The plaintext is <plaintext> (took <cryptanalysis time>).
```

Subsection 3

Classes

cryptosystem.h

```
using IntPtr = mpz_t; // GNU Multiple Precision Integer Type
using Key = IntPtr;
using Text = IntPtr;
```

```
class Cryptosystem {
public:
  virtual void generateKeys(Key publicKey, Key privateKey);
    // set these

  virtual void encrypt(Text ciphertext, // set this
    const Text plaintext, const Key publicKey);

  virtual void decrypt(Text plaintext, // set this
    const Text ciphertext, const Key privateKey);

  virtual void cryptanalyze(Text plaintext, // set this
    const Text ciphertext, const Key publicKey);
};
```

Section 4

Conclusion

Q & A

https://github.com/vuphan314/cry