CIS5371-Project

AES and RSA Implementation

Christopher Foley
Bijayita Thapa

Overview

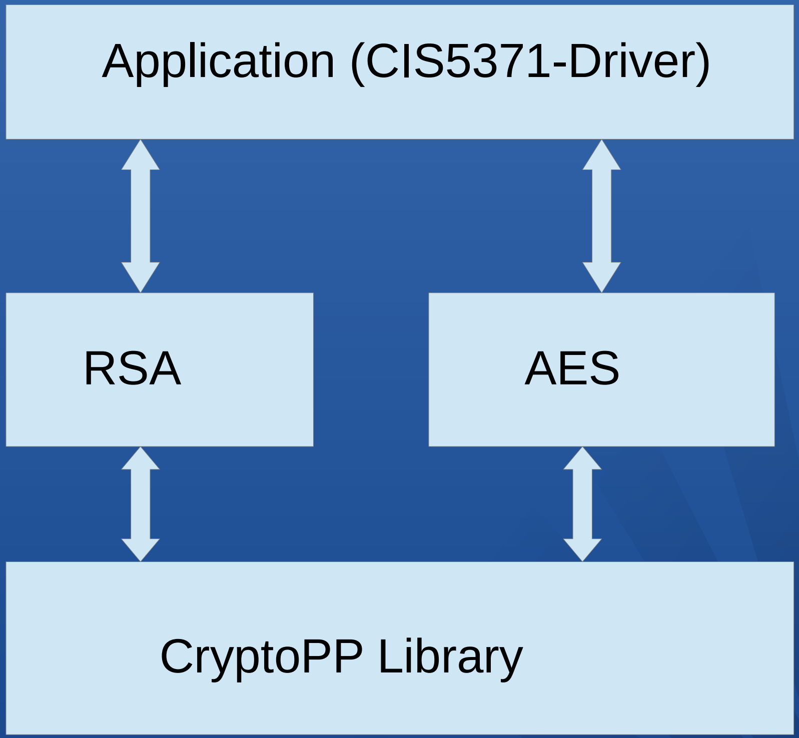
- Description
- Overall Structure
- Lessons Learned
  - GUI
  - Cryptographic packages
  - Implementation

Description

- Command line driven encryption using either RSA or AES encryption
- No modes available yet
- 128 bit keys used
- If key is not specified random numbers will be generated
- RSA or AES selectable
- Future features:
  - CBC modes
  - Adding DES/3DES/ElGamal
  - 192 & 256 byte AES

Overall Structure

- Written in C/C++ to allow for bit manipulations
- CryptoPP used to allow for large integers
- Cryptographic package allows for use of direct linking to packages
- Command line interface provided



Lessons Learned

- GUI
  - Treefrog Framework selected
- Cryptographic Package
  - CryptoPP chosen
- Implementation
  - Issues and concens

Lessons Learned - GUI

- Treefrog Framework Selected
  - C/C++
  - Framework is selectable which means complexity
  - Requires server running
  - Changes to GUI require full rebuildGUI
- OpenSQL/MariaDB or MongoDB available
- Requires screen design first
- After 3 weeks of evenings, I gave up and went to command line.
- Java easier for GUI, but we will continue to investigate/learn

Lessons Learned - CryptoPP

- CryptoPP
- Cryptographic package
  - Numerous algorithms
  - Number Theoretic Package – great for debug and test
- Large integers up to 2^{255}
  - Mathematical functions (including XOR and modulus)
  - Prime/Coprime/Calculate multiplicative invers
- C/C++

Lessons Learned - Implementation

- Although CPU supports 64 bits DES is best implemented as 8 bytes.
- Std::string allows use of streaming, but care must be taken
- When implementing key_expansion in AES parts treated as 32 bit words AND 8 bit bytes.
  - A union was created to allow overlay
  - System was little endian which presented problems accessing bytes and words.
  - Code added to account for endianess of system
  - DEBUG FLAGS critical during compilation
- Lecture Notes AND Handbook of Cryptography essential for development.

Comments

- Christopher Foley <cfoley3@fau.edu> and/or
- Bijayita Thapa <bthapa@my.fau.edu>