Vysoké učení technické v Brně
Fakulta informačních technologií

Kryptografie – 2. projekt

Dokumentace

06. květen 2018 Ján Jusko (xjusko00)

1 Úvod

Tento dokument popisuje riešenie druhého projektu v predmete Kryptografie (KRY). Jeho cieľom bolo bližšie sa zoznámiť s asymetrickým šifrovacím algoritmom RSA a následne implementovať funkcie k generovaniu kľúčov, (de)šifrovaniu a prelomeniu RSA. K implementácii bol zvolený jazyk C++ spolu s knihovnou pre prácu s veľkými číslami - *gmp.h*.

2 Riešenie

Aplikácia *kry* implementuje štyri funkcie popísané v nasledujúcich podkapitolách. Celková štruktúra programu sa skladá z hlavnej triedy RSA ktorá poskytuje štyri verejné metódy implementujúce príslušné štyri funkcie. Ako jedinú triednu premennú má táto trieda štruktúru RSAKeys obsahujúcu všetky potrebné parametre RSA algoritmu.

2.1 Generování klíčů

Funkcionalitu generovania kľúčov implementuje funkcia *RSA::generate*. Prvým krokom sa snaží nájsť dve prvočísla P, Q. Tie sú počiatočným náhodným číslom sekvenčne vyhľadávané a testované algoritmom *Solovay-Strassen* na primalitu. Následne sú jednoducho vypočítaná hodnoty phi, N verejný modulus a E verejný exponent. Privátny exponent D je získaný pomocou extended Euclid algorithm pre multiplikatívny inverz.

2.2 (De)šifrování

Šifrovanie, tak ako aj dešifrovanie je implementované v jednej metóde s názvom *cipher_or_decipher*. Kedže volaním rovnakej funkcie *moz_powm* vieme získať zašifrovanú resp. otvorenú správu, rozhodol som sa tieto dve prípady spojiť do rovnakej metódy.

2.3 Prolomení RSA

Štvrtú funkciu - prolomení RSA aplikácia neimplementuje.

3 Záver

Cieľ projektu bol čiastočne naplnený. V programe .kry sú implementované tri zo štyroch potrebných funkcií ktoré približujú fungovanie asymetrického šifrovacieho algoritmu RSA. Projekt bol vypracovaný v jazyku C++ a priebežne testovaný na referenčnom stroji *merlin*.