Kryptografia - RSA

Tomáš Lapšanský (xlapsa00)

Máj 2020

1 Úvod

Projekt je zameraný na šifrovací algoritmus RSA. V prvej fáze je vytvorený naprogramovaný algoritmus RSA v jazyku C++. Program ďalej rieši šifrovanie a dešifrovanie správ a následne prelomenie RSA šifry na základe slabého verejného modulu. Pre prácu s veľkými číslami bola použitá knižnica GMP.

2 Generovanie RSA kľúčov

Pri generovaní kľúčov sa udáva dĺžka verejného modulu. Jeho dĺžka by mala byť minimálne 6 bitov. Najprv dôjde k nastaveniu exponentu *e*, teda sa zvolí podľa dĺžky verejného modulu. V prípade že je jeho zvolená dĺžka maximálne 2048 bitov, exponent je nastavený na hodnotu 3. V opačnom prípade na hodnotu 65537.

V ďalšom kroku volíme 2 veľké náhodné prvočísla *p* a *q* a počítame im prislúchajúcu hodnotu *phi*, ktorá je daná ako *(p - 1) * (q - 1)*. Rozhodujúcim faktorom je najväčší spoločný deliteľ pre *e* a *phi*. Ak je ich najväčší spoločný deliteľ číslo 1, použijeme vygenerované prvočísla, v opačnom prípade proces opakujeme. V štandardnom algoritme pre generovanie RSA kľúčov by sme mali zvoliť prvočísla a hľadať vhodné *e*, no pre urýchlenie algoritmu sme sa rozhodli použiť reverzný postup.

V ďalšom kroku program spočíta verejný modulus *n = p * q*. Poslednou časťou algoritmu je výpočet súkromného exponentu *d* pomocou nájdenia inverzného prvku *inv(e, phi)*, ktorý využíva rozšírený euklidov algoritmus.

Po ukončení generovania dostaneme dvojice pre verejný *(e, n)* a súkromný *(d, n)* kľúč. Overiť tieto vygenerované kľúče môžeme jednoducho pomocou prepínačov *-e* alebo *-d* ktoré slúžia na zašifrovanie a dešifrovanie správy.

2.1 Generovanie prvočísel

Pri generovaní je vybraná náhodná hodnota. Následne je testovaná pomocou algoritmu *Solovay-Strassen*. Algoritmus je založený na princípe modulárnej ekvivalencie alebo inak povedané číselnej kongruencie podľa modulo n. Algoritmus skúma *k* čísel, kde ak pre prvočíslo nebude táto kongruencia platiť, je toto

prvočíslo označené ako eulerov svedok. Nie je však zaručené že ak kongruencia platí, je číslo skutočne prvočíslom. Je teda potrebné otestovať viacero čísel, kde pri väčšom počte čísel rastie pravdepodobnosť toho, že dané číslo je prvočíslom. Kongruenciu dokážeme vyjadriť nasledovne.

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$$

Na pravej strane kongurencie sa nachádza tzv. Jacobiho symbol, ktorého výsledkom je prvok množiny {-1, 0, 1}.

3 Šifrovanie a dešifrovanie

Šifrovanie a dešifrovanie je riešené rovnakým algoritmom. Algoritmus využíva funkciu *mpz_powm* z knižnice GMP. Správa je vynásobená daným kľúčom, dostaneme teda zašifrovanú alebo naopak dešifrovanú správu. Výsledok tohto algoritmu sa spočíta ako $message^{exponent} mod modulus$.