Dokumentácia projektu predmetu KRY

RSA

(autor: Matúš Kontra login: xkontr00)

1.Úvod

Zadaním bolo naimplementovať generovanie kľúčov, šifrovanie, dešifrovanie a lámanie asymetrickej šifry RSA. Toto vyžadovalo naštudovanie a naprogramovanie niekoľkých algoritmov z teórie čísel, menovite: netriviálny test primality (Miller-Rabin), rozšírený Euklidov algoritmus, modulárne umocňovanie (right to left binary method). Na faktorizáciu bola využitá knižnica.

2.Generovanie Kľúčov

Implementácia sa nachádza v metóde „genkeys“, parametrizovanej bitovou šírkou. Hľadanie p a q prebieha nasledovným spôsobom. Vygeneruje sa náhodné číslo polovičnej bitovej šírky a najnižší a dva najvyššie bity sa nastavia na 1. Toto zaručuje že číslo je nepárne a že súčin získaný p a q bude spĺňať požiadavok na bitovú šírku. Overí sa či je toto číslo prvočíslo – metóda „Miller-Rabin-test“. Ak nie, číslo sa navýši o 2 a overuje sa jeho primalita. Proces opakujeme dokiaľ sme nenašli prvočíslo. Číslo q sa generuje obdobným spôsobom. Z p a q sa vypočíta n a phi. Verejný exponent sa hľadá následovne – skúsia sa hodnoty 3,17 a 65537 ak ani jedna nevyhovuje generujú sa náhodné čísla z rozsahu 1..phi-1 dokým nespĺňajú podmienku gcd(e, phi) = 1. Privátny exponent využíva rožšírený euklidov algoritmus na nájdenie inverzného modulo prvku.

3.Šifrovanie a Dešifrovanie

Tu sa jednoducho využije naimplementované modulárne umocňovanie na vstupné parametre.

4.Lámanie

Prelomenie RSA spočíva v odvodení čísel p a q z čísla n. Po zistení p a q, sme schopný vypočítať phi a na jeho základe odvodiť privátny kľúč z verejného. V princípe sa jedná o probĺem faktorizácie celého čísla – nájdenie prvočíselných súčiniteľov. Na faktorizáciu bola použitá knžnica „msieve“ vo verzii 1.50. Táto využíva množinu metód – Pollardovo Rho, ECM, QS(Quadratic sive) , NFS(Number field sieve). V prvom kroku knižnica hľadá jednoduchšími metódami malé faktory, zložitejšie komponenty posúva do QS a nakoniec do NFS.

5.Záver

Pri riešení projektu sme sa oboznámili s problematikou asymetrických šifier a matematickými nástrojmi potrebnými k ich aplikácii. Aplikácia úspešne generuje, kóduje a dekóduje. Ďalej sme sa zoznámili teoretickými slabinami šifry RSA. Tieto spočívajú v možnosti odvodiť privátny kľúč z verejného pomocu faktorizácie verejného modulu. Toto je však časovo náročné vzhľadom k dĺžke kľúča.