Problém faktorizácie v asymetrickej kryptografií
(esej na tému „Motivácia k výberu témy“)

Téma kryptografie je v súčasnosti často skloňovaná v kontexte bezpečnosti informačných systémoch, pričom asymetrická kryptografia patrí medzi jej základné stavebné časti. Častokrát slúži práve asymetrická kryptografia na získanie alebo výmenu kľúča medzi dvoma komunikujúcimi stranami, čo kladie asymetrickú kryptografiu medzi základné stavebné prvky kryptografie.

Počas celého môjho doterajšieho pôsobenia na vysokej škole sa zameriavam na štúdium kryptografie a práve aj z tohto dôvodu som si vyberal tému, ktorá je z tejto oblasti. Kryptografia je pre mňa oblasť, v ktorej vidím budúcnosť a svoje ďalšie pôsobenie. Aktuálnosť bezpečnosti kryptografických systémov je stále dôležitá otázka a problém faktorizácie, na základe ktorého existuje asymetrická kryptografia je s rastúcim výpočtovým výkonom a novými metódami výpočtu čoraz jednoduchší. Aj z tohto dôvodu je odporúčaná dĺžka kľúča navýšená z pôvodných 1024 bitov na 2048 bitov.

Ďalším aspektom, prečo som si vybral danú tému sú aj jej možnosti a široké spektrum poznatkov, ktoré sa využívajú na riešenie problému faktorizácie, ktoré by som si chcel počas svojho štúdia osvojiť, upevniť a zdokonaliť sa v nich. Pre príklad uvediem, že problém faktorizácie je riešený počnúc programovaním v asemblery (vzhľadom na efektivitu) cez využitie grafických technológií (programovanie na GPU) až po náročné algebraické algoritmy ktoré predstavujú moderný pohľad na problém faktorizácie z hľadiska efektivity výpočtu a časovej zložitosti, čím sa dostávame k ďalšiemu predmetu bakalárskej práca, a to je komparácie jednotlivých algoritmoch a ich časová zložitosť.

Práve časová zložitosť, ako je popísaná funkciami v závislosti od vstupných parametroch (poz. alebo aj inač) nie je vo všeobecnosti veľmi presná. Práve to je ďalší z dôvodov, prečo som si danú tému vybral. Pohľad a pochopenie správania asymptotickej časovej zložitosti a následná komparácia týchto dvoch hodnôt my prinesie nové poznatky v štúdiu efektívnosti jednotlivých algoritmov. Koniec koncov, priznám sa, že sa nepovažujem za veľkého odborníka na odhadovanie časových zložitostí jednotlivých algoritmov a aj to je jeden z dôvodov, prečo som si danú tému vybral.

Na záver by som chcel ešte spomenúť, že mojím osobným cieľom okrem vyššie napísaného je aj naučenie a zdokonalenie sa v programovacom jazyku C/C++.Všetky tieto faktory, ktoré som popísal, vidím ako veľký prínos pre moje budúce štúdium, spojil som príjemne s užitočným a to v kontexte toho, že v rámci bakalárskej práce sa naučím veci, ktoré budem potrebovať nielen pre prax a moje ďalšie profesionálne uplatnenie, ale aj poznatky, ktoré získam mi uľahčia ďalšie štúdium.