Bezpečnosť informačných a komunikačných systémov

Katedra elektroniky a multimediálnych telekomunikácií

Domáca úloha č.5

Martin Chlebovec **18. Okt. 2020**

Vypracovanie DÚ č. 5:
Numerické zadanie krokov potrebných k výpočtu k*P.
Poradové číslo študenta: 9
Pridelené celočíselné hodnoty: x, y, k: 17, 20, 19.

Realizáciu zadania v rámci domácej úlohy som realizoval s ručnými výpočtami a následným overením medzivýsledkov dostupnými nástrojmi. Cieľom úlohy bolo vypočítať Z = 19P.

1. fáza úlohy - Výpočet 2P, 4P, 8P, 16P
Pre výpočet inverzného prvku som sa rozhodol využiť Euklidov algoritmus s následným spätným chodom s využitím posledného nenulového zvyšku. Na základe dostupných vzorcov v prednáškových materiáloch 8.5 som využil vzťahy pre predpis P=Q na výpočet premenných s (bez menovateľa s násobením inverzným prvkom), xr, yr s následným overením vzájomnej kongruencie medzi xr, yr so zohľadnením modula M = E_23(1,1). Takto bolo možné efektívne odhaliť prípadnú nepresnosť pri výpočte, najmä pri spätnom chode Euklidovho algoritmu (zlé znamienko vo výpočte, nesprávne sčítanie).

Pri realizácii výpočtov som zistil, že sa hodnoty P opakujú (sú vzájomne identické), každý 8-mi násobok:

- P == 8P (17,20)
- 2P ==16P (13,7)

2. fáza úlohy - Výpočet 3P, 19P
Pre určenie parametra pre Euklidov algoritmus som využil rozdiel xq-xp z menovateľa vzťahu pre výpočet s pre predpis P≠Q. Vypočítaním nsd a následným spätným chodom bolo možné určiť inverzný prvok a ním vynásobiť vzťah v menovateli pre výpočet s. Následným výpočtom xr a yr bolo možné určiť súradnice bodu na eliptickej krivke s možnosťou overenia vzájomnej kongruencie oboch parametrov.

Pre 3P som využil vstupné parametre P a 2P. Pre výpočet 19P využité vstupné parametre 3P a 16P. Vzťahy “spájania” zohľadnené podľa predpisu k cvičeniu č.3 v readme.txt súbore, kedy platí zápis premennej k v dvojkovej sústave - násobky v jednotlivých bitových bodoch P, v našom prípade 19, bitovo 10011, teda P, 2P, 16P. Výsledok 19P reprezentuje hľadaný výsledok Z = 19P, t.j. (13,16).

Problémy pri výpočte:

- Pár krát chyba pri výpočte spätného Euklidovho algoritmu. S využitím EC - kongruencie vypočítačných bodov xr a yr bolo možné jednoducho overiť, či sú parametre v poriadku. Ak kongruentné neboli, bolo možné vrátiť sa len o pár krokov späť a výpočet opakovať.
- Použitie nesprávneho parametra pri výpočte yr vo vzťahu pre P≠Q (po prehliadnutí som použil xq namiesto xr), pri detailnejšej kontrole problém odstránený

Nástroje pre kontrolu čiastkových riešení:

- Využil som nástroj MODULO CALCULATOR pre výpočet zvyšku pre zadané modulo M = 23
- Pre kontrolu inverzného prvku modulo M som využil nástroj MODULAR MULTIPLICATIVE INVERSION, čím som mohol rýchlo overiť, či je výsledný inverzný prvok v spätnom chode Euklidovho algoritmu správny