Bezpečnosť informačných a komunikačných systémov

Katedra elektroniky a multimediálnych telekomunikácií

Domáca úloha č.9

Martin Chlebovec **8. Nov. 2020**

Vypracovanie DÚ č. 9:
Číslo študenta: 9
Vstupné vektory: x = 17 y = 20 z = 19 → P[17, 20]

15. Nov. - oprava vzorca ľavej strany pre overenie vzáj. kongruencie (pôvodne 2x pre pravú stranu použitý pre obe strany)
Riešenie DÚ využíva programovú implementáciu v jazyku C s komentovaným zdrojovým kódom.

Funkčnosť programu:
V cykle sú vypočítané hodnoty (mod M, M=23) 2P, 4P, 8P, 16P (výpočet je tvorený určením inverzného prvku, jednotlivých parametrov xr, yr, s s overením vypočítaných hodnôt EC metódou - overením vzájomnej kongruencie). Následne obdobný výpočet pre hodnoty 3P (2P +P), 19P (16P+3P). Hodnota 19P zodpovedá hodnote Z = k*P (k=19).

Všetky medzivýsledky sú vypísané do konzolovej aplikácie a sú prevedené na kladnú hodnotu (mod M). Výsledky zodpovedajú hodnotám dosiahnutím v papierovej verzii DÚ. Program prekladaný bez makefilu a parametrov, priamo v Linux Cent OS stroji príkazom do konzole: **gcc -std=c99 -o main Chlebovec_Martin_DU9_BIKS.c -lm**.

Nakoľko sa mi nepodarilo implementovať Euklidov (GCD) algoritmus so spätným chodom tak ako v papierovej verzii zadania, použil som alternatívu pre výpočet inverzného prvku vo forme multiplikatívnej inverzie zo zdroja:
https://www.geeksforgeeks.org/multiplicative-inverse-under-modulo-m/

Screenshoty vykonaného programu nižšie:

Výstup programu - rozloženie k=19 na mocninové násobky, výpočet 2P a 4P, overenie medzivýsledkov EC metódou

```
Vytvoril: MARTIN CHLEBOVEC - BIKS
DU c.9

Rozklad k=19, na mocninove nasobky cisla 2
2^4 = 16
2^3 = 8
2^2 = 4
2^1 = 2
2^0 = 1

P[17, 20], E_23(1,1)
2*yp=40
Inv. prvok(40, 23) = 19
s = 1
xr = 13
yr = 7
EC kontrola (13, 7), OK, SU KONGRUENTNE, TEST PASSED


2P[13, 7]
2*yp=14
Inv. prvok(14, 23) = 5
s = 10
xr = 5
yr = 4
EC kontrola (5, 4), OK, SU KONGRUENTNE, TEST PASSED
```

Výstup programu - výpočet 8P, 16P a 3P, overenie medzivýsledkov EC metódou

```
4P[5, 4]
2*yp=8
Inv. prvok(8, 23) = 3
s = 21
xr = 17
yr = 20
EC kontrola (17, 20), OK, SU KONGRUENTNE, TEST PASSED


8P[17, 20]
2*yp=40
Inv. prvok(40, 23) = 19
s = 1
xr = 13
yr = 7
EC kontrola (13, 7), OK, SU KONGRUENTNE, TEST PASSED


16P[13, 7]


2P+1P
3P[?, ?]
Inv. prvok(19, 23) = 17
s = 9
xr = 5
yr = 19
EC kontrola (5, 19), OK, SU KONGRUENTNE, TEST PASSED


3P[5, 19]
```

Výpočet 19P (výsledok) Z = k*P (19P), výpis čiastkových výsledkov, EC overenie