Popa Alex Ovidiu
936

06.11.2020

PKC Assignment B
(02)

$n = 7031$ - factorize using the continued fractions method.

Solution

Firstly, a_i, b_i and $b_i^2 \pmod n$ were generated using a C++ program, for $i = \overline{0,4}$. The values are shown below:

i	0	1	2	3	4
a_i	83	1	5	1	2
b_i	83	84	503	587	1677
$b_i^2 (\mathrm{mod}\, n)$	-142	25	-107	50	-71

To choose the factor base B, we need to factorize each $b_i^2 \bmod n$ in its absolute value:

$142 = 2 \cdot 71$

$25 = 5^2$

$107 = 107$

$50 = 2 \cdot 5^2$

$71 = 71$

- choose the primes which appear in more than one element or at an even power in one number

$\Rightarrow B = \{-1, 2, 5, 71\}$

For the B written before, the B-numbers from $b_i^2 \bmod n$ are: $-142 = 2 \cdot 71 \cdot (-1) \rightarrow i=0$

$25 = 5^2 \rightarrow i=1$

$50 = 2 \cdot 5^2 \rightarrow i=3$

$-71 = 71 \cdot (-1) \rightarrow i=4$

And their vectors v_i are:

$v_0 = (1, 1, 0, 1)$

$v_1 = (0, 0, 2, 0)$

$v_3 = (0, 1, 2, 0)$

$v_4 = (1, 0, 0, 1)$

Pick a subset of vectors which sum up to $0 \pmod 2$

$v_0 + v_1 + v_3 + v_4 = 0 \pmod 2$

$\Rightarrow b = b_0 \cdot b_1 \cdot b_3 \cdot b_4 \pmod n$

$= 83 \cdot 84 \cdot 587 \cdot 1677 \pmod{7031}$

$b = 3550 \pmod{7031}$

$C = 2 \cdot 5^2 \cdot 71 = 50 \cdot 71 = 3550 \pmod{7031}$

$b = \pm C = -3481$

$\Rightarrow$ we need to pick another subset of v_i's which sum up to 0. If there aren't any left, we generate more $a_i, b_i, b_i^2 \% n$.

$v_0 + v_3 + v_4 = 0 \pmod 2$

$b = b_0 \cdot b_3 \cdot b_4 \pmod n$

$= 83 \cdot 587 \cdot 1677 \pmod{7031}$

$= 4897 = -2134 \pmod{7031}$

$c = 2 \cdot 5 \cdot 71 = 710 \pmod{7031}$

$b \neq \pm c \Rightarrow$ a factor of $n = 7031$ is

$(-2134 + 710, 7031)$ or $(-2134 - 710, 7031) \Leftrightarrow$

$\Leftrightarrow \underbrace{(-1424, 7031)}_{= 89}$ or $\underbrace{(-2844, 7031)}_{= 79}$

$\Rightarrow \underline{n = 7031 = 79 \cdot 89}$

(3)

Scanned with CamScanner