Blum-Blum-Shub

Аметов Имиль, гр. M07-903

4 июня 2020 г.

Дано: $p = 67$, $q = 31$. Требуется вычислить начальную последовательность генератора псевдослучайных чисел Blum-Blum-Shub и указать период.

Решение: генератор псевдослучайных чисел Blum-Blum-Shub вычисляется по формуле

$$x_{N+1} = x_N^2 \mod n,$$

где $n = pq = 67 \cdot 31 = 2077$, а N — номер элемента последовательности. В качестве начального элемента было выбрано $x_0 = 3$. Была вычислена следующая последовательность:

$$x_0 = 3,$$

$$x_1 = 3^2 \mod 2077 = 9 \mod 2077 = 9,$$

$$x_2 = 9^2 \mod 2077 = 81 \mod 2077 = 81,$$

$$x_3 = 81^2 \mod 2077 = 6561 \mod 2077 = 330,$$

$$x_4 = 330^2 \mod 2077 = 108900 \mod 2077 = 896,$$

$$x_5 = 896^2 \mod 2077 = 802816 \mod 2077 = 1094,$$

$$x_6 = 1094^2 \mod 2077 = 1196836 \mod 2077 = 484,$$

$$x_7 = 484^2 \mod 2077 = 234256 \mod 2077 = 1632,$$

$$x_8 = 1632^2 \mod 2077 = 2663424 \mod 2077 = 710,$$

$$x_9 = 710^2 \mod 2077 = 504100 \mod 2077 = 1466,$$

$$x_{10} = 1466^2 \mod 2077 = 2149156 \mod 2077 = 1538,$$

$$x_{11} = 1538^2 \mod 2077 = 2365444 \mod 2077 = 1818,$$

$$x_{12} = 1818^2 \mod 2077 = 3305124 \mod 2077 = 617,$$

$$x_{13} = 617^2 \mod 2077 = 380689 \mod 2077 = 598,$$

$$x_{14} = 598^2 \mod 2077 = 357604 \mod 2077 = 360,$$

$$x_{15} = 360^2 \mod 2077 = 129600 \mod 2077 = 826,$$

$$x_{16} = 826^2 \mod 2077 = 682276 \mod 2077 = 1020,$$

$$x_{17} = 1020^2 \mod 2077 = 1040400 \mod 2077 = 1900,$$
$$x_{18} = 1900^2 \mod 2077 = 3610000 \mod 2077 = 174,$$
$$x_{19} = 174^2 \mod 2077 = 30276 \mod 2077 = 1198,$$
$$x_{20} = 1198^2 \mod 2077 = 1435204 \mod 2077 = 2074,$$
$$x_{21} = 2074^2 \mod 2077 = 4301476 \mod 2077 = 9.$$

Элементы последовательности x_1 и x_{21} совпадают и равны 9. Следовательно, период генератора псевдослучайных чисел Blum-Blum-Shub для $p = 67$, $q = 31$ и $x_0 = 3$ равен 20.