Защита лаб 5

Часть 2.

С помощью заданного LFSR-генератора получить 12 членов последовательности.

Начальное состояние S0 = (111101)2, .

Конфигурация LFSR.

S5

 S4

 S2

 S3

 S0

 S1

|  |  |  |  |
| --- | --- | --- | --- |
| Номер шага | Состояние регистра | Генерируемый бит | Следующий смещающий бит |
| 0 | 111101 | 1 | 0 |
| 1 | 011110 | 0 | 0 |
| 2 | 001111 | 1 | 1 |
| 3 | 100111 | 1 | 0 |
| 4 | 010011 | 1 | 0 |
| 5 | 001001 | 1 | 0 |
| 6 | 000100 | 0 | 1 |
| 7 | 100010 | 0 | 0 |
| 8 | 010001 | 1 | 0 |
| 9 | 001000 | 0 | 1 |
| 10 | 100100 | 0 | 1 |
| 11 | 110010 | 0 |  |

Полученная последовательность S = {1, 0, 1, 1, 1 ,1, 0, 0, 1, 0, 0, 0}.

Защита лаб 6

Часть 2.

Решить сравнение первой степени алгоритмом Евклида, расширенным алгоритмом Евклида или методом Эйлера:

.

НОД(35, 11) = 1, значит у сравнения одно решение.

35x ≡ 11 (mod 12)

35x ≡ 11 + 12 (mod 12)

35x ≡ 23 (mod 12), НОД(35, 23) = 1, значит продолжаем сложение по следующей схеме:

ax ≡ b + m (mod m)

35x ≡ 35 (mod 12)

35x ≡ 47 (mod 12)

35x ≡ 59 (mod 12)

35x ≡ 71 (mod 12)

35x ≡ 83 (mod 12)

35x ≡ 95 (mod 12) НОД(35, 95) = 5, НОД(5, 12) = 1, значит делим на 5 сравнение

7x ≡ 19 (mod 12)

7x ≡ 31 (mod 12)

7x ≡ 42 (mod 12) НОД(7, 42) = 7, НОД(7, 12) = 1

x ≡ 6 (mod 12)