Лабораторная работа № 2

Вариант - 4

Деревянченко
Вязигилов
Поповчик
ВКБ-41

$a = f(a) \mod n$

$b = f(f(b)) \mod n$

$d = НОД(a - b, n)$

$n = 5969$

$a = b = c = 2$

$f = x^2 + 1$

1) $a_1 = f(2) = 2^2 + 1) \mod 5969 = 5$

$b_1 = f(f(2)) = f(5) = (5^2 + 1) \mod 5969 = 26$

$d = НОД(21, 5961) = 1$

2) $a_2 = f(5) = 5^2 + 1 \mod 5969 = 26$

$b_2 = f(f(26)) = f(677^2 + 1) \mod 5969 = 4686$

$НОД(4660, 5961) = 1$

3) $a_3 = f(26) \mod 5969 = 26^2 + 1 \mod 5969 = 677$

$b_3 = f(f(4686)) \mod 5969 = 21958596 + 1 \mod 5969 = 834$ $НОД(\ldots) = 1$

4) $a_4 = f(677) \mod 5969 = 458329 + 1 \mod 5969 = 4686$

$b_4 = f(f(834)) \mod 5969 = 483799540299 \mod 5969 = 3025$ $НОД(\ldots) = 1$

5) $a_5 = f(f(4686)) \mod 5969 = 21958596 + 1 \mod 5969 = 4615$ $НОД(\ldots) = 1$

$b_5 = f(f(3025)) \mod 5969 = \ldots \mod 5969 = 4295$

6) $a_6 = f(4615) \mod 5969 = 21298225 + 1 \mod 5969 = 834$

$b_6 = f(f(4295)) \mod 5969 = \ldots \mod 5969 = 3025$ $НОД(\ldots) = 1$

7) $a_7 = f(834) \mod 5969) = 4635556 \mod 5969 = 3153$ $НОД(\ldots) = 1$

$b_7 = f(f(3025)) \mod 5969 = \ldots \mod 5969 = 4295$

8) $a_8 = f(3153) \mod 5969 = 9941409 + 1 \mod 5969 = 3025$

$b_8 = f(f(4295)) = \ldots = 3025$

$НОД(3025, 3025) = 0.$