Федеральное государственное автономное образовательное учреждение
высшего образования
«Омский государственный технический университет»

Кафедра «Комплексная защита информации»

Задача 4.1.2
по дисциплине «Криптография и криптографические протоколы»
Вариант №18

Проверил работу:
д.н., профессор
_____ Широков И.В.
подпись

Автор работы:
студент гр. ИВТм-223
_____Трачевский Д.А.
подпись

Омск 2023

4.1.2 Возведение в степень в кольце Z_n

Вычислить выражение $a^k \bmod n = ?$

18) n = 821, a = 470, k = 33;

Решение

33 представим в двоичном виде.

$(33)_2$	$c_0 = 1$
1	$c_1 \equiv 1^2 \cdot 470^1 = 1 \cdot 470 = 470 \bmod 821$
0	$c_2 \equiv 470^2 \cdot 470^0 = 220900 \cdot 1 = 220900 \equiv 51 \bmod 821$
0	$c_3 \equiv 51^2 \cdot 470^0 = 2601 \cdot 1 = 2601 \equiv 138 \bmod 821$
0	$c_4 \equiv 138^2 \cdot 470^0 = 19044 \cdot 1 = 19044 \equiv 161 \bmod 821$
0	$c_5 \equiv 161^2 \cdot 470^0 = 25921 \cdot 1 = 25921 \equiv 470 \bmod 821$
1	$c_6 \equiv 470^2 \cdot 470^1 = 220900 \cdot 470 = 103823000 \equiv 161 \bmod 821$

33 = 100001

Чтобы вычислить значение 470 ^ 33 по модулю 821, мы можем использовать алгоритм модульного возведения в степень.

Начиная с основания 470, мы будем последовательно возводить его в квадрат и уменьшать результат по модулю 821 по мере продвижения справа налево по двоичному представлению показателя степени. Всякий раз, когда есть двоичная цифра 1, мы также умножаем основание на соответствующую степень 2.

Ответ: 161