Российский университет транспорта (МИИТ)

Институт транспортной техники и систем управления

Кафедра «Управление и защита информации»

Отчет

по практическому заданию

по теме «Возведение в степень по модулю числа»

по дисциплине «Криптографические методы защиты информации»

Выполнил:

Студент группы ТКИ-342

Дроздов А.Д.

Проверил:

Доцент кафедры УиЗи, к.т.н., с.н.с.

Михалевич И.Ф.

Москва 2023

Оглавление

Задание

Номер варианта: 4.

Вычислить:

$$c = a^b \mod 8 \tag{1}$$

$$c = a^b \mod 10 \tag{2}$$

$$c = a^b \mod 13 \tag{3}$$

$$c = a^b \mod 15 \tag{4}$$

$$c = a^b \mod 17 \tag{5}$$

$$c = a^b \mod 19 \tag{6}$$

Исходные данные:

$$a = 15 \tag{7}$$

$$b = 157 \tag{8}$$

Провести анализ сложности выполненных расчетов для каждого из примененных алгоритмов.

1. Теоретическая часть

1.1. Бинарный алгоритм возведения в степень по модулю числа

Бинарный алгоритм – это один из методов, позволяющий возвести число в степень по заданному модулю с помощью разложения степени в двоичное число.

Исходное выражение:

$$c = a^b \ mod \ m \tag{9}$$

Для возведения числа в степень по заданному модулю необходимо степень b из десятичной системы счисления перевести в двоичную и представить исходное выражение c следующим образом, где k – степени разложенного b (степени двойки)

$$c = a^k \ mod \ m \tag{10}$$

Выполняем вышеуказанные преобразования до тех пор, пока результат не будет найден.

ВХОД: Целые числа a, $x = (x_t x_{t-1} \ldots x_0)_2$, p.
ВЫХОД: Число $y = a^x \bmod p$.
1. $y \leftarrow 1$, $s \leftarrow a$.
2. FOR $i = 0, 1, \ldots, t$ DO
3. IF $x_i = 1$ THEN $y \leftarrow y \cdot s \bmod p$;
4. $s \leftarrow s \cdot s \bmod p$.
5. RETURN y.

Рисунок 1 – Псевдокод бинарного алгоритма

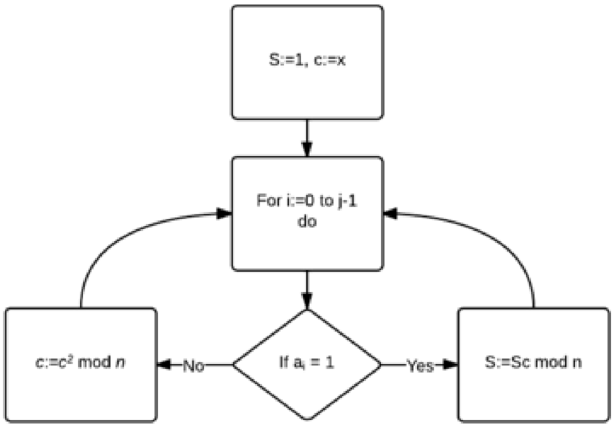

Рисунок 2 – Блок-схема бинарного алгоритма

1.2. Альтернативный алгоритм быстрого возведения в степень по модулю числа – Китайская теорема об остатках

Пусть необходимо возвести число a в степени b по модулю m:

$$c = a^b \; mod \; m \tag{11}$$

Тогда выражение c можно разложить на простые множители $p_1 - p_n$, $p_i < p_j$ при $j > i$ и построить следующую систему:

$$\begin{cases} a^b = r_1 \; mod \; p_1 \\ \vdots \\ a^b = r_n \; mod \; p_n \end{cases} \tag{12}$$

Вычеты $x^a \equiv r_i \; (mod \; p_i)$ с использованием малой теоремы Ферма, где $i = 1,2, \dots j$: m – простое число и $0 < a < p$. Тогда:

$$a^{m-1} \; mod \; m = 1 \tag{13}$$

Теперь a^b можно представить как $r_{1,\dots,n} + kp_{1,\dots,n}$, где k – целое число

$$\begin{cases} a^b = r_1 + kp_1 \\ \vdots \\ a^b = r_n + kp_n \end{cases} \tag{14}$$

Подставляя одно уравнение в другое, получим результат.

1.3. Оценки сложности алгоритмов

n – кол-во бит числа.

Бинарный алгоритм имеет сложность 1.5n умножения двух чисел, 1.5n операций деления числа 2n-битовых чисел на n-битовое число.

Для алгоритма с применением китайской теоремы об остатках сложность $O = \frac{3n}{2}$.

2. Практическая часть

2.1. Вычисление с помощью бинарного алгоритма

Число $a = 15$, степень $b = 157$.

$$c = 15^{157}\ mod\ 8 \tag{15}$$

$$157_{10} = 10011101_2 \tag{16}$$

$$c = 15^{157}\ mod\ 8 = 15^{128} * 15^{16} * 15^{8} * 15^{4} * 15^{1}\ mod\ 8 \tag{17}$$

Выражение 1:

$$c = 15^{157}\ mod\ 8 \tag{18}$$

$$15^{1}\ mod\ 8 = 7 \tag{19}$$

$$15^{4}\ mod\ 8 = 15^{1} * 15^{1} * 15^{1} * 15^{1}\ mod\ 8 = 1 \tag{20}$$

$$15^{8}\ mod\ 8 = 1 \tag{21}$$

$$15^{16}\ mod\ 8 = 1 \tag{22}$$

$$15^{128}\ mod\ 8 = 1 \tag{23}$$

Подставляем полученные значения и получаем результат:

$$c = 15^{157}\ mod\ 8 = 7 * 1\ mod\ 8 = 7 \tag{24}$$

Выражение 2:

$$c = 15^{157}\ mod\ 10 \tag{25}$$

$$15^{1}\ mod\ 10 = 5 \tag{26}$$

$$15^4 \, mod \, 10 = 15^1 * 15^1 * 15^1 * 15^1 \, mod \, 10 = 5 \tag{27}$$

$$15^8 \, mod \, 10 = 5 \tag{28}$$

$$15^{16} \, mod \, 10 = 5 \tag{29}$$

$$15^{128} \, mod \, 10 = 5 \tag{30}$$

Подставляем полученные значения и получаем результат:

$$c = 15^{157} \, mod \, 10 = 5 * 5 * 5 * 5 * 5 \, mod \, 10 = 5 \tag{31}$$

Выражение 3:

$$c = 15^{157} \, mod \, 13 \tag{32}$$

$$15^1 \, mod \, 13 = 2 \tag{33}$$

$$15^4 \, mod \, 13 = 15^1 * 15^1 * 15^1 * 15^1 \, mod \, 13 = 3 \tag{34}$$

$$15^8 \, mod \, 13 = 9 \tag{35}$$

$$15^{16} \, mod \, 13 = 15^8 * 15^8 \, mod \, 13 = 3 \tag{36}$$

$$15^{128} \, mod \, 13 = 9 \tag{37}$$

Подставляем полученные значения и получаем результат:

$$c = 15^{157} \, mod \, 13 = 2 * 3 * 9 * 3 * 9 \, mod \, 13 = 2 \tag{38}$$

Выражение 4:

$$c = 15^{157} \, mod \, 15 \tag{39}$$

$$15^1 \, mod \, 15 = 15 \tag{40}$$

$$15^4 \, mod \, 15 = 15^1 * 15^1 * 15^1 * 15^1 \, mod \, 15 = 0 \tag{41}$$

$$15^8 \, mod \, 15 = 0 \tag{42}$$

$$15^{16} \, mod \, 15 = 15^8 * 15^8 \, mod \, 15 = 0 \tag{43}$$

$$15^{128} \, mod \, 15 = 0 \tag{44}$$

Подставляем полученные значения и получаем результат:

$$c = 15^{157} \, mod \, 15 = 15 * 0 \, mod \, 15 = 0 \tag{45}$$

Выражение 5:

$$c = 15^{157} \, mod \, 17 \tag{46}$$

$$15^1 \, mod \, 17 = 15 \tag{47}$$

$$15^4 \, mod \, 17 = 15^1 * 15^1 * 15^1 * 15^1 \, mod \, 17 = 16 \tag{48}$$

$$15^8 \, mod \, 17 = 1 \tag{49}$$

$$15^{16} \, mod \, 17 = 1 \tag{50}$$

$$15^{128} \, mod \, 17 = 1 \tag{51}$$

Подставляем полученные значения и получаем результат:

$$c = 15^{157} \, mod \, 17 = 15 * 16 * 1 \, mod \, 17 = 2 \tag{52}$$

Выражение 6:

$$c = 15^{157} \, mod \, 19 \tag{53}$$

$$15^1 \, mod \, 19 = 15 \tag{54}$$

$$15^4 \, mod \, 19 = 15^1 * 15^1 * 15^1 * 15^1 \, mod \, 19 = 9 \tag{55}$$

$$15^8 \, mod \, 19 = 5 \tag{56}$$

$$15^{16} \, mod \, 19 = 6 \tag{57}$$

$$15^{128} \, mod \, 19 = 16 \tag{58}$$

Подставляем полученные значения и получаем результат:

$$c = 15^{157} \, mod \, 19 = 15 * 9 * 5 * 6 * 16 \, mod \, 19 = 10 \tag{59}$$

2.2. Вычисление с помощью китайской теореме об остатках

Число $a = 15$, степень $b = 157$.

По китайской теореме об остатках сначала необходимо значение модуля представить, как произведение взаимно простых чисел. Поэтому возьмем выражение 2, в котором $mod \; 10$ представим следующим образом.

Выражение 2:

$$c = 15^{157}\, mod\; 10 \tag{60}$$

$$10 = 2 * 5 \tag{61}$$

Тогда по теореме получим систему:

$$\begin{cases} 15^{157} \equiv r_1\, (mod\; 2) \\ 15^{157} \equiv r_2\, (mod\; 5) \end{cases} \tag{62}$$

$$\begin{cases} 5^{157} * 3^{157} \equiv r_1\, (mod\; 2) \\ 5^{157} * 3^{157} \equiv r_1\, (mod\; 5) \end{cases} \tag{63}$$

$$\begin{cases} 5^{156} + 5^1 * 3^{156} + 3^1 \equiv r_1\, (mod\; 2) \\ 0 * 3^{157} \equiv r_1\, (mod\; 5) \end{cases} \tag{64}$$

$$\begin{cases} 5^{156} + 1 * 3^{156} + 1 = 5^{155} + 2 * 3^{156} + 2 \equiv r_1\, (mod\; 2) \\ 0 \equiv 0\, (mod\; 5) \end{cases} \tag{65}$$

$$\begin{cases} 157 * 157 = 1 * 1 \equiv 1\, (mod\; 2) \\ 5^{157} * 3^{157} \equiv 0\, (mod\; 5) \end{cases} \tag{66}$$

$$\begin{cases} t = 15^{157} \equiv 1 + 2u\, (mod\; 2) \\ t = 15^{157} \equiv 0 + 5v\, (mod\; 5) \end{cases} \tag{67}$$

Подставит t из первого уравнения во второе:

$$1 + 2u\, mod(5) = 5v\, mod(5) \tag{68}$$

$$2u \equiv 4\, mod(5) \tag{69}$$

$$u \equiv 2\, mod(5) \tag{70}$$

$$t = 1 = 15^{157}\, mod\; 2 = 1 + 2 * u = 5 \tag{71}$$

$$c = 15^{157}\, mod\; 10 = 5 \tag{72}$$

Заключение

В результате выполнения практической работы было рассмотрено два алгоритма быстрого возведения числа в степень по модулю. При вычислении заданных выражений вышеуказанными способами можно убедиться в том, что бинарный алгоритм универсален и подходит для выражения любой сложности, а метод с использованием китайской теоремы об остатках применим только в том случае, когда модуль раскладывается на взаимно простые сомножители.