Математические основы защиты информации и информационной безопасности

Отчет по лабораторной работе № 6 : Раложение чисел на множители.

Кейела Патачона, группа НПМмд-02-21

Содержание

List of Figures

1 Цель работы

Построить алгоритм, реализующий разложение чисел на множетели.

2 Выполнение работы

Задача разложения на множители - одна из первых задач, использованных для построения криптосистем с открытым ключом. *Задача разложения составного числа на множители* формулируется следующим образом: для данного положительного целого числа n найти его каноническое разложение $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}...{p_s}^{\alpha_s}$, где p_i — попарно различные простые числа, $\alpha_i \geq 1$. На практике не обязательно находить каноническое разложение числа n. Достаточно найти его разложение на *два нетривиальных сомложителя*: $n = pq, 1 \leq p \leq q < n$. Далее будем понимать задачу разложения именно в этом смысле.

2.1 p—Метод Полларда

Пусть n — нечетное составное число, $S = \{0, 1, ..., n–1\}$ и $f : S \to S$— случайное отображение, обладающее сжимающими свойствами, например $f(x) = x^2 + 1(mod \quad n)$. Основная идея метода состоит в следующем. Выбираем случайный элемент $x_0 \in S$ и строим последовательность $x_0, x_1, x_2, ...,$ определяемую рекуррентным соотношением

$$x_{i+1} = f(x_i)$$

где $i > 0$, до тех пор, пока не найдем такие числа i, j, что $i < j$ и $x_i = x_j$. Поскольку множество S конечно, такие индексы i, j существуют (последовательность «зацикливается»). Последовательность x_i будет состоять из «хвоста» $x_0, x_1, ..., x_{i-1}$ длины $O\left(\sqrt{\frac{\pi n}{8}}\right)$ и цикла $x_i = x_j, x_{i+1}, ..., x_{j-1}$ той же длины.

2.2 Алгоритм, реализующий p—метод Полларда.

Вход. Число n, начальное значение c, функция f, обладающая сжимающими свойствами.

Выход. Нетривиальный делитель числа n.

1. Положить $a \leftarrow c, b \leftarrow c$.
2. Вычислить $a \leftarrow f(a)(mod \quad n), b \leftarrow f(f(b))(mod \quad n)$
3. Найти $d \leftarrow$ НОД $(a - b, n)$.
4. Если $1 < d < n$, то положить $p \leftarrow d$ и результат p. При $d = n$ результат: “Делитель не найден”; при $d = 1$ ввернуться на шаг 2.

lab06 > task.py > decompose

```python
def f(x,n):
    return (x**2 + 5) % n

def gcd(a,b):
    r = [a, b]
    while True:
        if r[-2] % r[-1] == 0:
            d = r[-1]
            break
        else:
            r.append(r[-2] % r[-1])
    return d

def pollard_p_method(n,c=1,f=f):
    a, b = c, c
    d = 1

    while d==1:
        a = f(a,n) % n
        b = f(f(b,n),n)%n

        d = gcd(a-b,n)

        print(f"a = {a} b = {b} d = {d}")

    if d != n:
        print(f"Нетривиальный делитель {n} : {d}")
        return d
    else:
        print("Нетривиальный делитель не найден")
        return d

```

Figure 2.1: p—метод Полларда

Пример Найти p—метод Полларда нетривиальный делитель числа $n = 1359331$. Положим $c = 1$ и $f(x) = x^2 + 5(mod \quad n)$. Работа алгоритма иллюстрируется следующей таблицей:

i	a	b	d=НОД(a-b,n)
	1	1	
2	6	41	1
2	41	123939	1
3	1686	391594	1
4	123939	438157	1
5	435426	582738	1
6	391594	1144026	1
7	1090062	885749	1181

Figure 2.2: Пример работы алгоритма p—метода Полларда

Таким образом, 1181 является нетривиальным делителем числа 1359331.

2.3 Метод квадратов. (Теорема Ферма о разложении)

Для любого положительного нечетного числа n, существует взаимно однозначное соответствие между множеством делителей числа n, не меньших, чем $\sqrt{n}$, и множеством пар s, t таких неотрицательных целых чисел, что $n = s^2 - t^2$.

Пример. У числа 15 два делителя, не меньших, чем $\sqrt{15}$, - это числа 5 и 15. Тогда получаем два представления: 1. $15 = pq = 3 * 5$, откуда $s = 4, t = 1, 15 = 4^2 - 1^2$; 2. $15 = pq = 1 * 5$, откуда $s = 8, t = 7, 15 = 8^2 - 7^2$.

```
32
33  def decompose(N):
34      div1 = pollard_p_method(N)
35      div2 = N // div1
36      div1,div2 = max(div1,div2), min(div1,div2)
37      print(f"\nDecomposition of {N} :")
38      print(f"{N} = {int((div1 + div2)//2)}^2 - {int((div1 - div2)/2)}^2\n")
39
40  if __name__ == "__main__":
41      N = int(input("Enter the number to decompose: "))
42      decompose(N)
```

Figure 2.3: Код программа 1

2.4 Результаты работы

```
Enter the number to decompose: 1359331
a = 6 b = 41 d = 1
a = 41 b = 123939 d = 1
a = 1686 b = 391594 d = 1
a = 123939 b = 438157 d = 1
a = 435426 b = 582738 d = 1
a = 391594 b = 1144026 d = 1
a = 1090062 b = 885749 d = 1181
Нетривиальный делитель 1359331 : 1181

Decomposition of 1359331 :
1359331 = 1166^2 - 15^2

PS C:\Users\patat\Desktop\Master Rudn\Git_work\2021-2022\Cybersecurity\laboratory>
```

Figure 2.4: Разложение чисел 1

```
Enter the number to decompose: 15
a = 6 b = 11 d = 5
Нетривиальный делитель 15 : 5

Decomposition of 15 :
15 = 4^2 - 1^2

PS C:\Users\patat\Desktop\Master Rudn\Git_work\2021-2022\Cybersecurity\laboratory> & C:
rs/patat/Desktop/Master Rudn/Git_work/2021-2022/Cybersecurity/laboratory/lab06/task.py"
Enter the number to decompose: 31
a = 6 b = 10 d = 1
a = 10 b = 25 d = 1
a = 12 b = 12 d = 31
Нетривиальный делитель не найден

Decomposition of 31 :
31 = 16^2 - 15^2

PS C:\Users\patat\Desktop\Master Rudn\Git_work\2021-2022\Cybersecurity\laboratory>
```

Figure 2.5: Разложение чисел 2

3 Выводы

В ходе этой лабораторной работы, я изучил и построил алгоритм p— метода Полларда и научился разложение чисел на множетели и в виде разности квадратов.

Список литературы

1. Инструкция к лабораторной работе №6