Функция Мёбиуса, алгоритм RSA

Лаборторная работа №6

Осенний семестр, 2024 г.

Функция Мёбиуса.

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } \exists p \in \mathbb{P}\,(p^2 \mid n), \\ (-1)^k, & \text{если } n = p_1 p_2 \cdots p_k \text{ (различные } p_i \in \mathbb{P}). \end{cases}$$

Лемма.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n > 1. \end{cases}$$

Доказательство.

1. Пусть $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, где $p_1, p_2, \ldots, p_k$ — различные простые числа.
2. Сумма по делителям n:

$$\sum_{d|n} \mu(d) = \sum_{d|p_1 p_2 \cdots p_k} \mu(d) = \sum_{i=0}^{k} (-1)^i \binom{k}{i}.$$

3. Заметим, что сумма биномиальных коэффициентов с чередующимися знаками равна:

$$\sum_{i=0}^{k} (-1)^i \binom{k}{i} = (1-1)^k = \begin{cases} 1, & \text{если } k = 0 \text{ (то есть } n = 1), \\ 0, & \text{если } k > 0 \text{ (то есть } n > 1). \end{cases}$$

Таким образом, утверждение леммы доказано.

Взаимно простые числа — целые числа, не имеющие никаких общих делителей, кроме $\pm\, 1$.

Функция Эйлера. $\varphi(n)$ мультипликативная арифметическая функция, значение которой равно количеству натуральных чисел, меньших либо равных n и взаимно простых с ним.

Пусть $n \geq 2$. Значение функции Эйлера числа n можно найти из разложения этого числа на простые множители:

$$n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r},$$

где $p_1, p_2, \ldots, p_r$ — все различные простые делители числа n. Покажем, что

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_r}\right).$$

Если число k взаимно просто с n, то k не делится ни на одно из чисел $p_1, p_2, \ldots, p_r$. Мы найдём величину $\varphi(n)$, вычислив как количество чисел, меньших n и делящихся хотя бы на одно из чисел $p_1, p_2, \ldots, p_r$.

Пусть A_i — множество чисел, меньших n и делящихся на p_i (где $i = 1, 2, \ldots, r$). Имеем:

$$N = n - |A_1 \cup A_2 \cup \cdots \cup A_r| =$$

$$= n - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| - \sum_{i<j<k} |A_i \cap A_j \cap A_k| + \cdots + (-1)^{r-1} |A_1 \cap A_2 \cap \cdots \cap A_r|.$$

Ясно, что

$$|A_i| = \frac{n}{p_i}, \quad |A_i \cap A_j| = \frac{n}{p_i p_j}, \quad |A_i \cap A_j \cap A_k| = \frac{n}{p_i p_j p_k}, \quad \text{и так далее.}$$

Получаем:

$$\varphi(n) = n - \sum_i \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \sum_{i<j<k} \frac{n}{p_i p_j p_k} + \cdots + (-1)^r \frac{n}{p_1 p_2 \ldots p_r}.$$

Вынесем n за скобки:

$$\varphi(n) = n \left(1 - \sum_i \frac{1}{p_i} + \sum_{i<j} \frac{1}{p_i p_j} - \sum_{i<j<k} \frac{1}{p_i p_j p_k} + \cdots + (-1)^r \frac{1}{p_1 p_2 \ldots p_r} \right).$$

Это равно:

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_r}\right),$$

что и требовалось.

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

где p - просыте числа, являющиеся делителями n.

1. Для $n = 30$ найдите сумму $\mu(d)$ по всем делителям n. Найдите сумму знакочередующегося ряда количества подмножеств множества всех простых делителей числа n.

2. Напишите программу, которая для всех чисел от 1 до n выводит таблицу значений $\mu(k)$.

Алгоритм создания RSA

Реализуйте алгоритм RSA (Rivest–Shamir–Adleman), криптографический алгоритм с открытым ключом, основанный на сложности разложения больших чисел на простые множители. Ниже приведён алгоритм создания RSA.

1. **Выбор двух простых чисел.** Сгенерируйте два больших простых числа p и q. Убедитесь, что они различны. Для проверки числа на простоту можно использовать тест Миллера — Рабина.

   Пример (для небольших чисел):

   $$p = 61, \quad q = 53.$$

2. **Вычисление модуля n.** Вычислите произведение $n = p \cdot q$. Это значение будет частью открытого и закрытого ключей.

   Пример:
   $$n = 61 \cdot 53 = 3233.$$

3. **Вычисление функции Эйлера $\varphi(n)$.** Найдите значение функции Эйлера:
   $$\varphi(n) = (p-1)(q-1).$$

   Пример:
   $$\varphi(3233) = (61-1)(53-1) = 60 \cdot 52 = 3120.$$

4. **Выбор открытой экспоненты e.** Выберите число e, такое что:

   (i) $1 < e < \varphi(n)$,

   (ii) НОД$(e, \varphi(n)) = 1$ (взаимно просто с $\varphi(n)$).

   Пример:
   $$e = 17 \quad (\text{НОД}(17, 3120) = 1).$$

5. **Вычисление закрытой экспоненты d.** Найдите d — мультипликативную обратную к e по модулю $\varphi(n)$:
   $$d \cdot e \equiv 1 \,(\mathrm{mod}\, \varphi(n)).$$

   Используйте **расширенный алгоритм Евклида** для нахождения d.

   Пример:
   $$d = 2753 \quad (\text{так как } 17 \cdot 2753 \bmod 3120 = 1).$$

   Мультипликативная обратная к e по модулю $\varphi(n)$.

   Мультипликативная обратная d к числу e по модулю $\varphi(n)$ — это такое число d, которое удовлетворяет сравнению:
   $$d \cdot e \equiv 1 \pmod{\varphi(n)}.$$

   Иначе говоря:

   (a) Произведение $d \cdot e$, разделённое на $\varphi(n)$, даёт остаток 1.

   (b) Это равносильно решению уравнения:
   $$d \cdot e - k \cdot \varphi(n) = 1,$$
   где k — целое число, определяющее, сколько раз мы вычли $\varphi(n)$ из произведения.

   Условия существования. Число d существует тогда и только тогда, когда e и $\varphi(n)$ взаимно просты:
   $$\text{НОД}(e, \varphi(n)) = 1.$$

   Это важно, поскольку взаимная простота гарантирует существование решения.

Как найти d. Для нахождения d используется **расширенный алгоритм Евклида**. Этот алгоритм позволяет найти такие числа d и k, которые удовлетворяют уравнению:

$$d \cdot e + k \cdot \varphi(n) = 1.$$

Здесь d является мультипликативной обратной к e по модулю $\varphi(n)$.

Пример. Пусть:

$$e = 17, \quad \varphi(n) = 3120.$$

Найдем d, такое что:

$$d \cdot 17 \equiv 1 \pmod{3120}.$$

Шаг 1. Применение алгоритма Евклида

Применим расширенный алгоритм Евклида для чисел 17 и 3120:

$$3120 = 183 \cdot 17 + 9,$$

$$17 = 1 \cdot 9 + 8, \quad 9 = 1 \cdot 8 + 1, \quad 8 = 8 \cdot 1 + 0.$$

Так как на последнем шаге НОД равен 1, обратное число существует.

Шаг 2. Обратный ход для нахождения d

Теперь выпишем обратные шаги:

$$1 = 9 - 1 \cdot 8,$$

$$8 = 17 - 1 \cdot 9 \quad \Rightarrow \quad 1 = 9 - 1 \cdot (17 - 1 \cdot 9) = 2 \cdot 9 - 1 \cdot 17,$$

$$9 = 3120 - 183 \cdot 17 \quad \Rightarrow \quad 1 = 2 \cdot (3120 - 183 \cdot 17) - 1 \cdot 17 = 2 \cdot 3120 - 367 \cdot 17.$$

Шаг 3. Устранение кратных 3120

Поскольку d рассматривается по модулю 3120, мы можем убрать кратные 3120:

$$d = -367 \pmod{3120} = 2753.$$

Таким образом, $d = 2753$.

Проверка. Убедимся, что:

$$d \cdot e \equiv 1 \pmod{\varphi(n)}.$$

Подставим значения:

$$2753 \cdot 17 = 46801.$$

Найдём остаток при делении на 3120:

$$46801 \mod 3120 = 1.$$

Значит, $d = 2753$ — действительно мультипликативная обратная к $e = 17$ по модулю 3120.

Итог. Мультипликативная обратная d позволяет "обратить"операцию возведения в степень e по модулю n, что является основой расшифровки в алгоритме RSA.

Формирование ключей. Сформируйте ключи:

- Открытый ключ: (e, n),
- Закрытый ключ: (d, n).

Пример:

$$\text{Открытый ключ: } (17, 3233), \quad \text{Закрытый ключ: } (2753, 3233).$$

Шифрование сообщения

Для сообщения m (где $m < n$), зашифруйте его, используя формулу:

$$c = m^e \pmod{n},$$

где c — зашифрованное сообщение.

Пример:

$$m = 42, \quad c = 42^{17} \pmod{3233} = 2557.$$

Расшифровка сообщения

Расшифруйте зашифрованное сообщение c с помощью формулы:

$$m = c^d \pmod{n}.$$

Пример:

$$c = 2557, \quad m = 2557^{2753} \pmod{3233} = 42.$$

Итог

- Открытый ключ используется для **шифрования**.
- Закрытый ключ используется для **расшифровки**.