# КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

## Разбор заданий: материал 12

## Математические основы криптографии: решение сравнений второй степени

Данный материал демонстрирует разбор задания, посвященного решению сравнений второй степени с одним неизвестным.

В общем случае сравнение второй степени имеет следующий вид: $x^2 \equiv a \pmod{n}$, $n > 1,\ a \in \{1,\ 2,\ \ldots,\ n-1\}$. Очевидно, что решение сравнения представленного вида состоит в извлечении квадратных корней из $a$ по модулю $n$.

Если $n = p$ есть простое число, речь идет о частном случае сравнения второй степени по модулю простого числа. Разрешимость таких сравнений легко установить с помощью символа Лежандра. Задача извлечения квадратных корней по модулю простого числа также не относится к категории вычислительно сложных.

Если модуль является составным и известно его разложение на простые множители, извлечение квадратных корней по данному модулю сводится к решению некоторого количества задач извлечения квадратных корней по простым модулям (делителям составного модуля).

Наконец, если модуль является составным и неизвестно его разложение на простые множители, извлечение квадратных корней по данному модулю становится сложной вычислительной задачей, которая сводится к задаче целочисленной факторизации.

Алгоритм извлечения квадратных корней по модулю простого числа представлен ниже.

**Вход**: целые числа $p > 1$, $a \in \{1,\ 2,\ \ldots,\ p-1\}$.

**Выход**: два квадратных корня из $a$ по модулю $p$.

Шаг 1. Вычислить символ Лежандра $\left(\frac{a}{p}\right)$. Если $\left(\frac{a}{p}\right) = -1$, то квадратных корней нет.

Шаг 2. Выбрать целое $b$, такое, что $\left(\frac{b}{p}\right) = -1$.

Шаг 3. Представить $p - 1 = 2^s \cdot t$, где $t$ — нечетное число.

Шаг 4. Вычислить $a^{-1} \pmod{p}$ по расширенному алгоритму Евклида.

Шаг 5. Вычислить $C_0 = b^t \pmod{p}$, $r = a^{\frac{t+1}{2}} \pmod{p}$.

Шаг 6. Для $i = \overline{1, s-1}$:

Шаг 6.1. Вычислить $d_i = (r^2 \cdot a^{-1})^{2^{s-i-1}} \bmod p$.

Шаг 6.2. Если $d_i \equiv -1 \pmod{p}$, то $r \leftarrow r \cdot C_0 \pmod{p}$.

Шаг 6.3. $C_0 \leftarrow C_0^2 \pmod{p}$.

Шаг 7. Возврат $(r;\ -r)$.

Можно увидеть, что данный алгоритм на первом шаге использует символ Лежандра для проверки существования квадратных корней из данного числа $a$ по модулю $p$. При отрицательном исходе в дальнейших вычислениях нет необходимости.

В основе алгоритма лежит цикл, выполняющийся $s - 1$ раз, где $s$ — это наибольшая степень двойки, являющаяся делителем числа $p - 1$.

Следующий алгоритм осуществляет извлечение квадратных корней по модулю составного числа, представляющего собой произведение двух простых чисел. Этот частный случай решения задачи извлечения квадратных корней по модулю составного числа используется в криптосистеме Рабина.

В данном алгоритме дважды выполняется вычисление квадратных корней из числа $a$ по двум простым модулям–делителям составного модуля $n$. После этого с помощью китайской теоремы об остатках происходит объединение полученных результатов в четыре значения квадратного корня по составному модулю $n$.

**Вход**: целые числа $p > 1$, $q > 1$, $a \in \{1, 2, \ldots, n-1\}$.

**Выход**: четыре квадратных корня из $a$ по модулю $n = pq$.

Шаг 1. Вычислить два квадратных корня $r$ и $-r$ из $a$ по модулю $p$.

Шаг 2. Вычислить два квадратных корня $s$ и $-s$ из $a$ по модулю $q$.

Шаг 3. Вычислить $c_1 p + d_1 q = 1$ по расширенному алгоритму Евклида.

Шаг 4. Вычислить $x = (rd_1 q + sc_1 p) \bmod n$ и $y = (rd_1 q - sc_1 p) \bmod n$.

Шаг 5. Возврат $(\pm x; \pm y)$.

**Пример.**

Решить сравнение $x^2 \equiv 811 \pmod{1457}$, если известно, что $1457 = 31 \cdot 47$.

**Решение.**

Воспользуемся алгоритмом извлечения квадратного корня по модулю составного числа при известной факторизации.

**Шаг I.**

Вычислим два квадратных корня из 283 по модулю 31 с помощью алгоритма извлечения квадратных корней по модулю простого числа. При этом поскольку $283 > 31$, предварительно выполним приведение $283 \pmod{31}$, чтобы входные данные соответствовали требованиям алгоритма.

$811 \pmod{31} = 5$.

Шаг I.1.

Вычислим символ Лежандра $\left(\frac{5}{31}\right)$. В соответствии с квадратичным законом взаимности $\left(\frac{5}{31}\right)\left(\frac{31}{5}\right) = 1$, так как $5 \equiv 1 \pmod 4$. Следовательно, $\left(\frac{5}{31}\right) = \left(\frac{31}{5}\right) = \left(\frac{1}{5}\right) = 1$. Значит, 5 является квадратичным вычетом по модулю 31.

Шаг I.2.

Возьмем $b = -1$. По свойству символа Лежандра $\left(\frac{-1}{31}\right) = -1$, так как $31 \equiv 3 \pmod 4$.

Шаг I.3.

Представим $31 - 1 = 30 = 2^1 \cdot 15$.

Шаг I.4.

Вычислим $5^{-1} \pmod{31}$ с помощью расширенного алгоритма Евклида. Очевидно, что $5^{-1} \pmod{31} = -6 \equiv 25$.

Шаг I.5.

Вычислим $C_0 = (-1)^{15} \pmod{31} = -1$, $r = 5^{\frac{15+1}{2}} \pmod{31} = 25 = -6$.

Шаг I.6.

Данный шаг пропускаем, так как $s = 1$.

Шаг I.7.

Возврат двух квадратных корней из 5 по модулю 31: $r = -6$, $r = 6$.

**Шаг II.**

Вычислим два квадратных корня из 283 по модулю 47 с помощью алгоритма извлечения квадратных корней по модулю простого числа. При этом поскольку $283 > 47$, предварительно выполним приведение $283 \pmod{47}$, чтобы входные данные соответствовали требованиям алгоритма.

$811 \pmod{47} = 12$.

Шаг II.1.

Вычислим символ Лежандра $\left(\frac{12}{47}\right)$. В соответствии со свойствами символа Лежандра $\left(\frac{12}{47}\right) = \left(\frac{2^2}{47}\right)\left(\frac{3}{47}\right) = \left(\frac{3}{47}\right)$. Теперь по квадратичному закону взаимности $\left(\frac{3}{47}\right)\left(\frac{47}{3}\right) = -1$, так как $47 \equiv 3 \pmod{4}$. Следовательно, $\left(\frac{3}{47}\right) = -\left(\frac{47}{3}\right) = -\left(\frac{2}{3}\right) = 1$. Значит, 12 является квадратичным вычетом по модулю 47.

Шаг II.2.

Возьмем $b = -1$. По свойству символа Лежандра $\left(\frac{-1}{47}\right) = -1$, так как $47 \equiv 3 \pmod{4}$.

Шаг II.3.

Представим $47 - 1 = 46 = 2^1 \cdot 23$.

Шаг II.4.

Вычислим $12^{-1} \pmod{47}$ с помощью расширенного алгоритма Евклида. Очевидно, что $12^{-1} \pmod{47} = 4$.

Шаг II.5.

Вычислим $C_0 = (-1)^{23} \pmod{47} = -1$, $r = 12^{\frac{23+1}{2}} \pmod{47} = 24$.

Шаг II.6.

Данный шаг пропускаем, так как $s = 1$.

Шаг II.7.

Возврат двух квадратных корней из 5 по модулю 31: $r = -24$, $r = 24$.

**Шаг III.**

Вычислим $c_1 \cdot 31 + d_1 \cdot 47 = 1$ по расширенному алгоритму Евклида. Получим $c_1 = -3$ и $d_1 = 2$.

**Шаг IV.**

Вычислим

$x = (6 \cdot 2 \cdot 47 + 24 \cdot (-3) \cdot 31) \bmod 1457 = 1246$,

$y = (6 \cdot 2 \cdot 47 - 24 \cdot (-3) \cdot 31) \bmod 1457 = 1339$.

**Шаг V.**

Возврат

$x = 1246$, $-x = -211$, $y = 1339$, $-y = -118$.