КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Разбор заданий: материал 11

Математические основы криптографии: нахождение квадратичных вычетов

Данный материал демонстрирует разбор задания, посвященного проверке разрешимости квадратичных сравнений с одним неизвестным с использованием свойств символа Лежандра.

Символ Лежандра $\left(\frac{a}{p}\right)$ — это функция, указывающая на то, является $a \in \{1,\ 2,\ \dots,\ p-1\}$ квадратичным вычетом или невычетом по модулю $p > 2$:

- $\left(\frac{a}{p}\right) = +1$, если a — квадратичный вычет по модулю p;
- $\left(\frac{a}{p}\right) = -1$, если a — квадратичный невычет по модулю p.

Число a называется квадратичным вычетом по модулю p, если квадратичное сравнение $x^2 \equiv a \pmod p$, $p > 1$, $a \in \{1,\ 2,\ \dots,\ p-1\}$ разрешимо (имеет два решения).

Число a называется квадратичным невычетом по модулю p, если данное сравнение не имеет решений.

Для нахождения символа Лежандра может быть использован критерий Эйлера, критерий Гаусса или же квадратичный закон взаимности совместно со свойствами символа Лежандра.

Пример.

Вычислить символ Лежандра $\left(\frac{561}{757}\right)$ с помощью его свойств и с использованием квадратичного закона взаимости.

Решение.

Разложим число 561 на простые множители, что для малых чисел является достаточно простой задачей, и получим $561 = 3 \cdot 11 \cdot 17$. Следовательно, данный символ Лежандра можно представить в виде произведения трех символов Лежандра:

$\left(\frac{561}{757}\right) = \left(\frac{3}{757}\right)\left(\frac{11}{757}\right)\left(\frac{17}{757}\right)$.

Последовательно найдем значения отдельных символов Лежандра, входящих в полученнное произведение.

1) Символ Лежандра $\left(\frac{3}{757}\right)$.

К данному символу Лежандра нельзя применить какое-либо свойство из основного перечня. Поэтому преобразуем его с использованием квадратичного закона взаимности. Для этого необходимо привести значения, образующие данный символ Лежандра, по модулю 4: $3 \pmod 4 \equiv 3$ и $757 \pmod 4 \equiv 1$. Отсюда следует, что $\left(\frac{3}{757}\right)\left(\frac{757}{3}\right) = 1$, поэтому, переворачивая данный символ Лежандра, нужно оставть его знак без изменений:

$\left(\frac{3}{757}\right) = \left(\frac{757}{3}\right) = \left(\frac{1}{3}\right) = 1$.

2) Символ Лежандра $\left(\frac{11}{757}\right)$.

К данному симолу Лежандра также применим квадратичный закон взаимности. Поскольку $757 \pmod 4 \equiv 1$, то $\left(\frac{11}{757}\right)\left(\frac{757}{11}\right) = 1$, следовательно

$$\left(\frac{11}{757}\right) = \left(\frac{757}{11}\right) = \left(\frac{9}{11}\right) = \left(\frac{3^2}{11}\right) = 1.$$

3) Символ Лежандра $\left(\frac{17}{757}\right)$.

К данному симолу Лежандра также применим квадратичный закон взаимности. Поскольку $757 \pmod 4 \equiv 1$, то $\left(\frac{17}{757}\right)\left(\frac{757}{17}\right) = 1$, следовательно

$$\left(\frac{17}{757}\right) = \left(\frac{757}{17}\right) = \left(\frac{9}{17}\right) = \left(\frac{3^2}{11}\right) = 1.$$

Теперь можем вычислить значение исходного символа Лежандра:

$$\left(\frac{561}{757}\right) = \left(\frac{3}{757}\right)\left(\frac{11}{757}\right)\left(\frac{17}{757}\right) = 1 \cdot 1 \cdot 1 = 1.$$

Следовательно, значение 561 является квадратичным вычетом по модулю 757.