Малая теорема Ферма и ее применение в криптосистемах

И.А.Баукин

Научный руководитель: **Ильин М.Е,**
к.ф.-м.н., доцент.

Рассматриваются вычисления в поле целых чисел, приводящие к вычислению вычетов по некоторому основанию. Такая арифметика позволяет исследовать свойства натуральных чисел, используемых в криптографии.

Теорема Ферма. Пусть p — положительное простое число и a — целое, тогда :

$a^p \equiv a \pmod p$.

Одно из применений теоремы Ферма — вычисление степеней по модулю p.

Лемма Ферма. Пусть p — простое число и a — целое, не делящееся на p, тогда :

$a^{p-1} \equiv 1 \pmod p$.

Более интересное применение — система шифрования, или криптосистема с открытым ключом —RSA

Система шифрования RSA

Условия реализации:

1) Необходимо выбрать простые числа p и q.

2) Вычислить их произведение $n = p \cdot q$, число (Эйлера) $\varphi(n) = (p-1) \cdot (q-1)$ и некоторое число e , обратимое по модулю числа $\varphi(n)$. Пусть d — обратный элемент к e по модулю $\varphi(n)$: $e \cdot d \equiv 1 \bmod \varphi(n)$.

Пару n и e называют открытым или кодирующим ключом, который доступен всем. Если b — блок сообщения, тогда E(b) — блок зашифрованного сообщения:

$E(b) \equiv b^e \pmod n$.

Для декодировки нужно знать n и d — секретный, декодирующий ключ, сохраняющийся в тайне. Если a — блок зашифрованного сообщения (последовательность чисел), то исходное сообщение однозначно восстанавливается с помощью следующего выражения :

$D(a) = a^d \pmod n$.

Для нахождения обратного элемента d используется расширенный алгоритм Евклида. Криптостойкость системы RSA основывается на том, что при удачном выборе чисел p и q, определение обратного элемента достаточно трудоемкий и затратный процесс.

Рассмотрим следующий простой пример. Попробую зашифровать букву «В», ее численное представление — 12. Возьму p =3 и q = 7, тогда $\varphi(n) = 12$, тогда e = 5, n = 21.

$E(«В») \equiv 12^5 \pmod{21}$ искомый вычет равен 3.

Не трудно убедиться, что обратный к 5 по модулю 12 элемент — 5.

Поскольку a=3, тогда $D(a)=3^5 \pmod{21} \rightarrow D(a)=12$. То есть буква «В».

Литература

1. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. — М.: Постмаркет, 2001. — 328 с.