Практика №10. Модулярная арифметика. Операции с большими числами.

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ.

Алгоритм генерации простых чисел.

GENPR. Генерации простых чисел (Generate Primes)

Вход: Два целых числа k и m одинарной точности и одномерный массив A длины k; m – нечетное целое число ≥ 3

Выход: Простые числа $p_1 < p_2 < ... < p_r$ одинарной точности, лежащие в замкнутом отрезке $[m, m+2k-2]$

1. [Инициализация] $n := m + 2k - 2$; для $i := 1,2,...,k$ выполнить $A(i) := 1; d := 3$.

2. [Если $d^2 > n$, то получить простые числа и закончить работу] Если $d > [n/d]$, то перейти к шагу 6.

3. [Вычислить наименьшее положительное число j, такое, что $d \mid (m + 2j - 2)$ и $m + 2j - 2 \geq 3$] $r := MOD(m, d)$; $j := 1$; если r>0 и r нечетно, то $j := j + (d - r)/2$; если $m \leq d$, то $j := j + d$.

4. [Вычеркивание составных] Для $i := j, j + d, j + 2d, ...$ пока $j > k$ выполнять $A(j) := 0$.

5. [Изменение d] Если $MOD(d,6) = 1$, то $d := d + 4$, иначе $d := d + 2$; перейти к шагу 2.

6. [Получить простые числа] Для $i := k, k-1, ..., 1$ выполнять {Если $A(i) = 1$, то выдать простое число $m + 2i - 2$}; закончить работу.

Алгоритм возведения в степень. Многие алгоритмы сводятся к выполнению последовательности арифметических операций. Как шифрование, так и расшифрование в RSA предполагают использование операции возведения целого числа в целую степень по модулю N. Если возведение в степень выполнять непосредственно с целыми числами и только потом проводить сравнение по модулю N, то промежуточные значения окажутся огромными. Здесь можно воспользоваться свойствами арифметики в классах вычетов. Таким образом, можно рассмотреть промежуточные результаты по модулю N. Это делает вычисления практически выполнимыми.

E. Возвести в степень (Exponentiate)

Вход: Ненулевые a, k и m, a – элемент Z_m, $k = \sum_{0 \leq i \leq n-1} k_i 2^i$, k совпадает либо с $m - 2$, либо с $\phi(m) - 1$.

Выход: a^{-1}, мультипликативный обратный к a элемент по модулю m, где $a^{-1} = a^k$ в кольце Z_m

1. [Инициализация] $K \coloneqq k; B \coloneqq 1; A \coloneqq a$

2. [Вычисление следующего бита] $q \coloneqq [K / 2]; r \coloneqq K - 2 \cdot q; K \coloneqq q;$ если $r = 0$, то перейти к шагу 5.

3. [Умножить и взять остаток по модулю m] $B \coloneqq A \cdot B (\mathrm{mod}\, m)$

4. [Закончить?] Если $K = 0$, то вернуть $a^{-1} (\mathrm{mod}\, m) \coloneqq B$

5. [Возвести в квадрат и взять остаток по модулю m] $A \coloneqq A^2 (\mathrm{mod}\, m)$; перейти к шагу 2.

ЗАДАНИЕ

Сгенерировать два больших простых числа

Выполнить с числами операции сложения, вычитания, умножения, деления, вычисления остатка от деления одного числа на другое, возведения одного из чисел в степень n по модулю m.