Гавриленко Арсений *777*

Домашняя работа 5

Задача 1.

1. $a = 12^{14^{18^3}} \mod 19 = 12^{14^{18}} \cdot 12^{14^{18}} \cdot 12^{14^{18}} \mod 19$

$$\phi(19) = 18$$

$$a^{\phi(19)} = 1 \mod 19 => a^{18} = 1 \mod 19$$

$$a = 12^{14^{18}} \mod 19 = 1$$

$$a * b * c \mod x = a \mod x * b \mod x * c \mod x$$

$$a = 12^{14^{18^3}} = 1 \cdot 1 \cdot 1 \mod 19 = 1 \mod 19$$

3.

$$7^2 = 1 \mod 24$$

Тгда

$$7^{14^{20^9}} = 1 \mod 24$$

Задача 2.

Задача 3.

$$\Sigma_1^m(i) = \frac{1+m}{2} \cdot m \mod m?$$

$m = 2k; \dfrac{1+2k}{2} \cdot 2k \mod 2k = k + 2k^2 \mod 2k = k \mod 2k = m/2 \mod m$

$m = 2k+1; \dfrac{1+2k+1}{2} \cdot (2k+1) \mod 2k+1 = (k+1)(2k+1) \mod 2k+1$

$$= (k+1) \mod 2k+1 = (m-1)/2 \mod m$$

Задача 4. Пусть на вход подали N пар, разобьем их по две штуки. Рассмотрим первые две(без органичения общности):

$$\begin{cases} a_{1n} = d_1 * x_0 + a_1 \\ a_{2n} = d_2 * y_0 + a_2 \end{cases} \tag{1}$$

Эквивалентно(найдем общие элементы если такие есть):

$$d_1 \cdot x_0 + d_2 \cdot y_0 = a_2 - a_1 =$$

Видим что это уравнение решается с помощью расширенного алгоритма Евлклида за O(log(n)) от входа(величины чисел). Решив мы найдем общие члены двух последовательностей в общем виде, то есть их пересечение. Так устроим турнир между всеми парами рекурсивно. Всего будет O(n) операция нахождения решения системы из двух уравнений, поэтому асимптотика O(nlogn). Корректность следует из корректности алгоритма Евклида а также алгоритма поиска решений(мы решим систему из всех, только последовательно по 2 уравнения).

Задача 5.

$$\begin{cases} x \mod 36 = 24 \\ x \mod 54 = 45 \\ x \mod 107 = 53 \end{cases} \tag{2}$$

$$\begin{cases} x = 36k + 24 \\ x = 54l + 45 \\ x = 107j + 53 \end{cases} \tag{3}$$

Подставим x из второго в первое:

$$54l + 45 = 36k + 24$$

Слева нечетное, справа четное => решений нет

Задача 6.

$$M^{ed} = M^{k \cdot \phi(n)+1} \mod n = M^{k \cdot \phi(n)} * M \mod n$$

Если M и n не взаимнопросты, то:

$$M^{\phi(n)}! = 1 \mod n => M^{k \cdot \phi(n)} * M \mod n! = M \mod n$$

То есть мы не сможем восстановить исходное сообщение

Задача 7.

1. По сути мы зная публичны ключ, хотим сделать вот что - пусть мы знаем w- сможем ли мы восстановить x?(дальше все по модулю n)

$$w = l^d = r^{ed} \cdot x^d = r^{\phi(n)+1} x^d = r \cdot x^d$$

Все наши действия - в кольце вычетов, то тут есть единчиный по умножению элемент , тогда существует элеенмет $r^{-1} : r^{-1} \cdot r = 1$. ТОгда"

$$x = r^{-1} \cdot w$$

2. Вопрос - для всех ли ключей и пареметром справедливо, что сущесвтует r :

$$r^e \cdot x = l \mod n$$

Это уравнение в целых коэфицентах:

$$r^e \cdot x = nj + l$$

У него есть решения, тогда и только тогда когда(x,e,n известные константы), когда l делится на gcd(x, n).

3.

- Прогон от 1 до n - O(n)
- gcd(r^e, n) - O(log n)
- уже этого нам хватит, чтобы показать асимптотику(большую). Если у нас компуткер - то длина входа = имено записаь числа. Пусть длина входа 100 бит, тогда всевозможных чисел 2^100 уже довольно много - 30ая стпень 10ки. I7 считается $27 * 10^10$ операция в секнду., что заметно меньше нашего алгоритма.

<u>Задача 8.</u>