Домашнее задание 5

Турков Матвей, группа 777

1

Решение:

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

$$14^{18^3} = 14^{6^3 \cdot 3^3} = 2^{6k} \cdot 7^{6k} \mod 18 = 64^k \mod 18 = 10 \mod 18$$

$$12^{14^{18^3}} = 12^{10+18m} = 12^{18m} \cdot 12^{10} \mod 19 = 12^{10} \mod 19 = (12 \cdot 12^4)^2 \mod 19 = 7$$

2.

$$14^{11^{289}} \mod 25$$

$$289 mod \phi(25) = 9$$

$$14^{11^9} \mod 25$$

$$11^9 \mod \phi(25)$$

$$9 = 1 \mod \phi(20)$$

$$11^9 = 11 \mod 20 = 11$$

$$14^{11^9} = 14^{11} \mod 25$$

$$((14^2 \mod 25) \cdot (14^2 \mod 25) \cdot (14^2 \mod 25) \cdot (14^2 \mod 25) \cdot (14^2 \mod 25) \cdot 14) \mod 25$$

$$((21^2 \mod 25) \cdot (21^2 \mod 25) \cdot 21 \cdot 14) \mod 25$$

$$((16^2 \mod 25) \cdot 21 \cdot 14) \mod 25$$

$$(6 \cdot 21 \cdot 14) \mod 25$$

$$(9 \cdot 21) \mod 25$$

$$14^{11^{289}} = 14 \mod 25$$

3.

$$7^2 = 1 \mod 24) \to 7^{14^{20^9}} = 1 \mod 24$$

3

Решение:

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

Четный случай

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

А так же нечетный случай

$$m = 2k+1;\ \frac{1+2k+1}{2} \cdot (2k+1) \mod 2k+1 = (k+1)(2k+1) \mod 2k+1$$
$$= (k+1) \mod 2k+1 = (m-1)/2 \mod m$$

5

Решение:

$$\begin{cases} x \mod 36 = 24 \\ x \mod 54 = 45 \\ x \mod 107 = 53 \end{cases} \quad (1)$$

$$\begin{cases} x = 36k + 24 \\ x = 54l + 45 \\ x = 107m + 53 \end{cases} \quad (2)$$

Подставим x из второго в первое:

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

Слева нечетное, справа четное => решений нет

6

Решение:

Поскольку m и n не взаимопросты и , по определению алгоритма , $n = pq$, то m делимо либо на p, либо на q. Пусть для определенности, $m = ps$, где s некое число, причем необязательно простое.

Рассмотрим процесс шифрования

$$c = E(m) = m^e \mod n = (ps)^e \mod (pq)$$
$$p^e q^e \mod (pq) = p^e \mod (pq) \cdot s^e \mod (pq)$$

Теперь рассмотрим $p^e \mod (pq)$. Ясно, что

$$\forall e : p^e = 0 \mod (pq)$$

А значит, $E(m)$ всегда будет возвращать 0 и мы не сможем ничего зашифровать.