Алгоритмы решения задачи дискретного логарифмирования

Задача 1.

Используя алгоритм Силвера-Полига-Хеллмана, найти дискретный логарифм числа 123 по основанию 2 в $\mathbb{F}_{181}^*$ (2 – порождающий элемент в $\mathbb{F}_{181}^*$)

Решение 1. Пусть $q = 181,\ c = 123,\ \alpha = 2$. Надо найти такое m, что $\alpha^m = c$.

Разложим $q - 1$:

$$q - 1 = 180 = 2^2 \cdot 3^2 \cdot 5$$

1. Найдем $m^{(1)} = m \pmod{2^2}$

   Пусть $m^{(1)} = m_0^{(1)} + 2m_1^{(1)}$

   Обозначим $\omega = \alpha^{\frac{q-1}{2}} = 2^{\frac{180}{2}} = 2^{90} = 180$. Тогда множество $\Omega = \{1, \omega\}$ выглядит следущим образом:

   $$\Omega = \{1, 180\}$$

   Найдем $c^{\frac{q-1}{2}}$:

   $$c^{\frac{q-1}{2}} = 123^{\frac{180}{2}} = 123^{90} = 180 = \omega^1$$

   $$\Downarrow$$

   $$m_0^{(1)} = 1$$

   Теперь берём $c_1 = c \cdot \alpha^{q-1-m_0^{(1)}} = 123 \cdot 2^{179} = 152$

   Найдем $c_1^{\frac{q-1}{2^2}}$:

   $$c_1^{\frac{q-1}{2^2}} = 152^{\frac{180}{2^2}} = 152^{45} = 180 = \omega^1$$

   $$\Downarrow$$

   $$m_1^{(1)} = 1$$

   Получили $m^{(1)} = 1 + 2 \cdot 1 = 3$

2. Найдем $m^{(2)} = m \pmod{3^2}$

   Пусть $m^{(2)} = m_0^{(2)} + 3m_1^{(2)}$

   Обозначим $\omega = \alpha^{\frac{q-1}{3}} = 2^{\frac{180}{3}} = 2^{60} = 48,\ w^2 = 48^2 = 132$. Тогда множество $\Omega = \{1, \omega, \omega^2\}$ выглядит следущим образом:

   $$\Omega = \{1, 48, 132\}$$

   Найдем $c^{\frac{q-1}{3}}$:

   $$c^{\frac{q-1}{3}} = 123^{\frac{180}{3}} = 123^{60} = 48 = \omega^1$$

   $$\Downarrow$$

$$m_0^{(2)} = 1$$

Теперь берём $c_1 = c \cdot \alpha^{q-1-m_0^{(2)}} = 123 \cdot 2^{179} = 152$

Найдем $c_1^{\frac{q-1}{3^2}}$:

$$c_1^{\frac{q-1}{3^2}} = 152^{\frac{180}{3^2}} = 152^{20} = 48 = \omega^1$$

$$\Downarrow$$

$$m_1^{(2)} = 1$$

Получили $m^{(2)} = 1 + 3 \cdot 1 = 4$

3. Найдем $m^{(3)} = m \pmod 5$

Обозначим $\omega = \alpha^{\frac{q-1}{5}} = 2^{\frac{180}{5}} = 2^{36} = 59,\ \omega^2 = 59^2 = 42,\ w^3 = 59^3 = 125,\ w^4 = 59^4 = 135$. Тогда множество $\Omega = \{1, \omega, \omega^2, \omega^3, \omega^4\}$ выглядит следующим образом:

$$\Omega = \{1, 59, 42, 125, 135\}$$

Найдем $c^{\frac{q-1}{5}}$:

$$c^{\frac{q-1}{5}} = 123^{\frac{180}{5}} = 123^{36} = 135 = \omega^4$$

$$\Downarrow$$

$$m^{(3)} = 4$$

Получили $m^{(3)} = 4$

Составим систему сравнений:

$$\begin{cases} m = m^{(1)} = 3 \pmod{2^2} \\ m = m^{(2)} = 4 \pmod{3^2} \\ m = m^{(3)} = 4 \pmod 5 \end{cases} \iff \begin{cases} m = 3 \pmod 4 \\ m = 4 \pmod 9 \\ m = 4 \pmod 5 \end{cases} \iff m = 139 \pmod{180}$$

Получили, что $2^{139} = 123 \pmod{181}$.