КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Разбор заданий

Математические основы криптографии: исследование групп подстановок

Данный материал демонстрирует разбор задания, посвященного проведению вычислений над подстановками.

Группы подстановок представляют собой пример класса групп, широко используемого в криптографии. Такие элементарные операции, часто реализуемые в составе симметричных шифров и алгоритмов хеширования, как замена и перестановка, основываются на подстановках. Кроме того, существует класс исторических шифров, называемых подстановочными, для анализа которых также полезно уметь работать с подстановками.

Подстановкой на отрезке натурального ряда чисел $\mathbb{N}_k = \{1,\ 2,\ \dots,\ k\}$ называется любая биекция на $\mathbb{N}_k$.

Множество подстановок на $\mathbb{N}_k$ относительно операции композиции подстановок образует группу, которая называется симметрической группой k-ой степени S_k.

Для группы подстановок, как и для любой другой группы, имеет смысл понятие целочисленных степеней элементов группы.

Для подстановок, определенных на достаточно длинном отрезке $\mathbb{N}_k$, может быть затруднительно вычисление порядка посредством последовательного возведения в степень до получения единицы группы. Однако для симметрических групп существует более простой способ вычисления порядка элементов, основанный на понятии цикла.

Порядок подстановки $\varphi \in S_k$ равен наименьшему общему кратному длин независимых циклов, входящих в разложение φ.

Пример.

Вычислить $a(b)^{114}$, где

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 9 & 3 & 6 & 1 & 7 & 4 & 8 & 10 & 2 \end{pmatrix},$$

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 9 & 1 & 2 & 3 & 7 & 4 & 10 & 6 & 8 \end{pmatrix}.$$

Решение.

В данном случае мнимая сложность заключается в том, чтобы возвести подстановку b в степень 114. Делать это «в лоб» было бы действительно достаточно долго. Однако если узнать, каков порядок подстановки b, можно уменьшить показатель степень и, как следствие, снизить сложность вычислений.

Чтобы вычислить порядок подстановки b, необходимо разложить ее в произведение независимых циклов:

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 9 & 1 & 2 & 3 & 7 & 4 & 10 & 6 & 8 \end{pmatrix} = (1\ 5\ 3)(2\ 9\ 6\ 7\ 4)(8\ 10).$$

Можно увидеть, что таковых циклов три: один имеет длину, равную трем, второй — длину, равную пяти, и, наконец, третий — длину, равную двум.

Следовательно, подстановка b имеет порядок, равный $\text{НОК}(3,5,2) = 30$. Поэтому выражение b^{114} можно упростить следующим образом: $b^{114} = b^{3\cdot 30+24} = (b^{30})^3 b^{24} = b^{24}$.

Очевидно, что расчеты должны стать проще, но все же 24-кратная композиция подстановок также является не самой удобной для «ручных» расчетов.

Поэтому здесь лучше использовать другой способ, также основанный на разложении подстановки на независимые циклы.

Заметим, что возведение подстановки в некоторую степень приводит к возведению в эту степень всех циклов, составляющих данную подстановку. Однако каждый цикл фактически представляет собой отдельную подстановку, имеющую свой порядок, равный длине цикла. Причем порядок независимых циклов всегда будет меньше порядка подстановки, составленной из этих циклов.

Ранее было показано, что подстановка b представляет собой произведение трех независимых циклов. Запишем это следующим образом:

$b = \varphi_1\varphi_2\varphi_3$.

Тогда $O(\varphi_1) = 3$, $O(\varphi_2) = 5$, $O(\varphi_3) = 2$. Отсюда следует, что $(\varphi_1)^{114} = (\varphi_1)^{3\cdot 38} = e$, $(\varphi_2)^{114} = (\varphi_2)^{5\cdot 22+4} = (\varphi_2)^4$, $(\varphi_3)^{114} = (\varphi_3)^{2\cdot 57} = e$.

В результате подстановка b^{114} примет следующий вид:

$b^{114} = (\varphi_1)^{114}(\varphi_2)^{114}(\varphi_3)^{114} = e(\varphi_2)^4 e = (\varphi_2)^4 = (2\ 9\ 6\ 7\ 4)^4 = (2\ 4\ 7\ 6\ 9)$.

Теперь подстановка $a(b)^{114}$ может быть вычислена следующим образом:

$$a(b)^{114} = \begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\5&9&3&6&1&7&4&8&10&2\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\1&4&3&7&5&9&6&8&2&10\end{pmatrix} =$$

$$= \begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\5&6&3&4&1&10&7&8&9&2\end{pmatrix}.$$

Задания

1. Определить степень и циклы подстановок

$$A = \begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&1&4&8&7&6&9&2&5\end{pmatrix}$$

$$B = \begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&1&4&8&5&6&7&2&9\end{pmatrix}$$

$$C = \begin{pmatrix}1&2&3&4&5&6&7&8&9\\1&2&3&4&7&6&9&8&5\end{pmatrix}$$

Понизить степень подстановки

Вычислить $a(b)^{104}$, где

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 9 & 3 & 6 & 1 & 7 & 4 & 8 & 10 & 2 \end{pmatrix},$$

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 9 & 1 & 2 & 3 & 7 & 4 & 10 & 6 & 8 \end{pmatrix}.$$