КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Практическая работа 5

Математические основы криптографии: исследование абстрактных циклических групп

Данный материал демонстрирует разбор задания, посвященного исследованию абстрактных циклических групп.

Абстрактной циклической группой будем называть циклическую группу $G = \langle x \rangle$, природа элементов которой не определена и известен лишь ее порядок, $|G| = n$. Такая группа может быть записана как $G = \{1_G, x, x^2, \dots, x^{n-1}\}$. Чтобы исследовать группу G, необходимо выполнить следующее:

- найти порядок всех элементов группы G, представляющих собой различные степени образующего элемента x;
- определить все образующие элементы группы G помимо элемента x;
- найти все циклические подгруппы группы G;
- составить диаграмму, описывающую внутреннее устройство группы G.

Пример.

Исследовать $G = \langle x \rangle$, если $|G| = 18$.

Решение.

Абстрактная циклическая группа G восемнадцатого порядка с образующим x может быть записана следующим образом:

$G = \{1_G, x, x^2, x^3, x^4, x^5, x^6, x^7, x^8, x^9, x^{10}, x^{11}, x^{12}, x^{13}, x^{14}, x^{15}, x^{16}, x^{17}\}$.

Порядком элемента $g \in G$ называется наименьшее натуральное число k, такое, что $g^k = 1_G$. Порядок образующего элемента группы совпадает с порядком группы, поэтому в рассматриваемом случае можем записать:

$O(x) = 18, x^{18} = 1_G$.

Очевидно, что $x^{18} = x^{36} = x^{54} = \dots = x^{18 \cdot m} = 1_G$, где $m \in \mathbb{Z}$.

Чтобы определить порядок всех прочих элементов группы, достаточно знать, каким степеням образующего они соответствуют.

Вернемся к общему случаю циклической группы G, порожденной элементом x и имеющей порядок n, и рассмотрим произвольный элемент $x^l \in G$, $1 < l < n$. Если порядок данного элемента есть k, то $(x^l)^k = x^{lk} = 1_G$. Однако из свойств образующего элемента группы следует, что $x^{nm} = 1_G$, $\forall m \in \mathbb{Z}$. Следовательно, $x^{lk} = x^{nm}$, $lk = nm$ и $k = \frac{nm}{l}$ для некоторого целого m.

Таким образом, порядок элемента группы, представляющего собой l-ю степень образующего элемента группы, можно определить как наименьшее натуральное число k, на которое нужно домножить l, чтобы получить число, кратное порядку группу.

Воспользуемся сформулированным правилом при нахождении порядка элементов рассматриваемой группы восемнадцатого порядка.

$O(x^2) = 9$, так как 9 — это наименьшее натуральное число, на которое нужно домножить число 2, чтобы получить число, кратное 18.

$O(x^3) = 6$, так как $(x^3)^6 = x^{18} = 1_G$.

$O(x^4) = 9$, так как $(x^4)^9 = x^{36} = 1_G$.

$O(x^5) = 18$, так как $(x^5)^{18} = x^{60} = 1_G$.

$O(x^6) = 3$, так как $(x^6)^3 = x^{18} = 1_G$.

$O(x^7) = 18$, так как $(x^7)^{18} = x^{126} = 1_G$.

$O(x^8) = 9$, так как $(x^8)^9 = x^{72} = 1_G$.

$O(x^9) = 2$, так как $(x^9)^2 = x^{18} = 1_G$.

$O(x^{10}) = 9$, так как $(x^{10})^9 = x^{90} = 1_G$.

$O(x^{11}) = 18$, так как $(x^{11})^{18} = x^{198} = 1_G$.

$O(x^{12}) = 3$, так как $(x^{12})^3 = x^{36} = 1_G$.

$O(x^{13}) = 18$, так как $(x^{13})^{18} = x^{234} = 1_G$.

$O(x^{14}) = 9$, так как $(x^{14})^9 = x^{126} = 1_G$.

$O(x^{15}) = 6$, так как $(x^{15})^6 = x^{90} = 1_G$.

$O(x^{16}) = 9$, так как $(x^{16})^9 = x^{144} = 1_G$.

$O(x^{17}) = 18$, так как $(x^{17})^{18} = x^{306} = 1_G$.

Теперь определим все образующие элементы группы G. Очевидно, что это будут те элементы, порядок которых равен 18, то есть совпадает с порядком группы. Следовательно, $G = \langle x \rangle = \langle x^5 \rangle = \langle x^7 \rangle = \langle x^{11} \rangle = \langle x^{13} \rangle = \langle x^{17} \rangle$.

Можно увидеть, что данный список образующих полностью соответствует теореме, говорящей о том, что элемент $g = x^k \in G$, где $G = \langle x \rangle$ есть циклическая группа порядка n, является образующим группы G тогда и только тогда, когда выполняется условие НОД$(k, n) = 1$.

Все прочие элементы, порядок которых меньше 18, являются образующими циклических подгрупп группы G. Причем элементы, имеющие одинаковый порядок, очевидным образом являются образующими одной и той же циклической подгруппы. Перечислим циклические подгруппы группы G.

$H_1 = \langle x^2 \rangle = \langle x^4 \rangle = \langle x^8 \rangle = \langle x^{10} \rangle = \langle x^{14} \rangle = \langle x^{16} \rangle$, $|H_1| = 9$.

$H_2 = \langle x^3 \rangle = \langle x^{15} \rangle$, $|H_2| = 6$.

$H_3 = \langle x^6 \rangle = \langle x^{12} \rangle$, $|H_3| = 3$.

$H_4 = \langle x^9 \rangle$, $|H_4| = 2$.

Нетрудно заметить, что количество циклических подгрупп циклической группы совпадает с количеством нетривиальных делителей порядка циклической группы. В общем случае это следует из теоремы Лагранжа и обратной теоремы Лагранжа.

Чтобы определить состав циклической подгруппы, необходимо взять любой ее образующий и записать все его степени, до тех пор, пока не будет получена единица группы.

$$H_1 = \{(x^2)^0, (x^2)^1, (x^2)^2, (x^2)^3, (x^2)^4, (x^2)^5, (x^2)^6, (x^2)^7, (x^2)^8, (x^2)^9\} =$$
$$= \{1_G, x^2, x^4, x^6, x^8, x^{10}, x^{12}, x^{14}, x^{16}\}.$$

$H_2 = \{(x^3)^0, (x^3)^1, (x^3)^2, (x^3)^3, (x^3)^4, (x^3)^5\} = \{1_G, x^3, x^6, x^9, x^{12}, x^{15}\}$.

$H_3 = \{(x^6)^0, (x^6)^1, (x^6)^2\} = \{1_G, x^6, x^{12}\}$.

$H_4 = \{(x^9)^0, (x^9)^1\} = \{1_G, x^9\}$.

Можно увидеть, что подгруппа H_4 также является подгруппой подгруппы H_2. А подгруппа H_3 одновременно является подгруппой подгруппы H_1 и подгруппы H_2. Более того, если взять абстрактную циклическую группу порядка 9 и исследовать ее, то можно будет убедиться, что устройство подгруппы H_1 полностью совпадает с устройством абстрактной циклической группы порядка 9. В частности, группа порядка 9 должна иметь одну циклическую подгруппу порядка 3, поскольку 3 является единственным нетривиальным делителем числа 9. Аналогичные рассуждения верны и для подгрупп H_3 и H_4.