КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Разбор заданий: материал 6

Математические основы криптографии: построение и исследование полей Галуа

Данный материал демонстрирует разбор задания, посвященного построению и исследованию полей Галуа.

Полем Галуа называется поле F_{p^n}, полученное расширением простого конечного поля F_p посредством неприводимого многочлена $f \in F_p[X]$ степени n. Мощность поля Галуа составляет p^n. Элементами поля Галуа являются многочлены, принадлежащие кольцу многочленов над полем F_p, степень которых строго меньше n. Принадлежность многочлена кольцу многочленов $F_p[X]$ означает, что коэффициенты при степенях данного многочлена являются элементами поля F_p. Таким образом, поле Галуа F_{p^n} состоит из всевозможных остатков от деления многочленов, заданных над полем F_p, на неприводимый многочлен $f \in F_p[X]$ степени n.

Существует разные способы построения полей Галуа. В рамках настоящего задания при построении поля Галуа F_{p^n} необходимо записать все его элементы в количестве p^n. После этого необходимо задать операции сложения и умножения в данном поле, построив две таблицы, определяющие результат сложения и умножения для каждой пары элементов поля. Построение таблицы сложения является тривиальным: достаточно сложить коэффициенты при соответствующих степенях двух многочленов с приведением результата по модулю p. Построение таблицы умножения осуществляется несколько сложнее. Как только при перемножении двух элементов поля Галуа, степень которых меньше n, появляется многочлен степени n и более, его необходимо привести по модулю f. Сделать это можно поделив данный многочлен на f, и взяв остаток от деления.

Исследование построенного поля Галуа F_{p^n} сводится к исследованию мультипликативной группы $F_{p^n}^*$ данного поля, которая представляет собой циклическую группу порядка $p^n - 1$. Чтобы исследовать группу $F_{p^n}^*$, необходимо выполнить следующее:

- найти порядок всех элементов группы $F_{p^n}^*$ и выделить все образующие элементы;
- найти все циклические подгруппы группы $F_{p^n}^*$;
- составить диаграмму, описывающую внутреннее устройство группы $F_{p^n}^*$.

При выполнении данного задания необходимо опираться на свойства абстрактных циклических групп и навыки, приобретенные при исследовании подобных групп.

Возведение элементов поля Галуа в различные степени удобно выполнять с помощью построенной таблицы умножения. При этом если в конкретной задаче речь идет лишь об исследовании мультипликативной группы поля Галуа, то строить таблицу сложения нет необходимости.

Пример.

Построить поле Галуа F_{3^2} как расширение поля F_3 посредством неприводимого многочлена $f = 2x^2 - 2x + 1$. Исследовать мультипликативную группу данного поля.

Решение.

Сначала проверим, что данный многочлен действительно является неприводимым. Многочлен второй степени $f \in F_p[\,X]$ является неприводимым только в том случае, если у него нет делителей–многочленов первой степени вида $(x - a)$, $a \in F_p$. Другими словами, ни один из элементов $a \in F_p$ не является корнем многочлена $f \in F_p[\,X]$. В рассматриваемом примере убедиться в том, что многочлен $f \in F_p[\,X]$ не имеет корней, можно с помощью простого перебора всех элементов поля $F_3 = \{0, 1, 2\}$.

Проделаем соответствующие вычисления.

Если $x = 0$, то $2x^2 - 2x + 1 = 1 \neq 0$.

Если $x = 1$, то $2x^2 - 2x + 1 = 1 \neq 0$.

Если $x = 2$, то $2x^2 - 2x + 1 = 5 = 2 \pmod 3 \neq 0$.

Таким образом, многочлен $f = 2x^2 - 2x + 1$ из кольца многочленов $F_3[\,X]$ является неприводимым и может быть использован при построении поля Галуа.

Запишем элементы поля Галуа как всевозможные остатки от деления многочленов из $F_3[\,X]$ на неприводимый многочлен $f = 2x^2 - 2x + 1$:

$F_{3^2} = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}$.

Нужно отметить, что данное множество значений не зависит от выбора неприводимого многочлена, а зависит только от его степени n.

Уточним операции сложения и умножения в поле Галуа, построив для этого две таблицы.

Таблица сложения показывает результат сложения каждой пары элементов поля F_{3^2}.

+	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0								
1	1	2							
2	2	0	1						
x	x	$x+1$	$x+2$	$2x$					
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$				
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$			
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x		
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

Поскольку сложение в поле является коммутативной операций, таблица сложения будет симметрична относительно главной диагонали. Поэтому при заполнении таблицы ограничимся нижним треугольником.

Теперь выделим мультипликативную группу поля $F_{3^2}^*$, исключив из построенного множества нулевой элемент

$F_{3^2}^* = \{1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$.

Данная группа является циклической группой порядка 8. Если обозначить неизвестный пока образующий элемент группы $F_{3^2}^*$ как α, то группу можно представить в виде

$F_{3^2}^* = \langle\alpha\rangle = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$.

Порядок элемента циклической группы достаточно легко определить, если известно, какая степень образующего ему соответствует. Элементы представленной пока еще абстрактной циклической группы порядка 8 имеют следующий порядок: $O(\alpha) = 8$, $O(\alpha^2) = 4$, $O(\alpha^3) = 8$, $O(\alpha^4) = 2$, $O(\alpha^5) = 8$, $O(\alpha^6) = 4$, $O(\alpha^7) = 8$. Каждый из элементов, порядок которого отличен от 8, является образующим циклической подгруппы соответствующего порядка. Таким образом, мультипликативная группа поля F_{3^2} содержит четыре образующих элемента и две циклические подгруппы: циклическую подгруппу порядка 2 с одним образующим и циклическую подгруппу порядка 4 с двумя образующими. Чтобы уточнить устройство группы $F_{3^2}^*$, построим таблицу умножения. Как и операция сложения, операция умножения должна быть определена для всех элементов поля, однако исключим из таблицы умножения нулевой элемент, поскольку он очевидным образом при умножении обращает любой другой элемент в нулевой.

Построение таблицы умножения требует большего количества вычислений по сравнению с построением таблицы умножения. Как только при перемножении двух элементов поля Галуа, степень которых меньше n, появляется многочлен степени n и более, его необходимо привести по модулю неприводимого многочлена f. Сделать это можно поделив данный многочлен на f, и взяв остаток от деления.

Однако, проще воспользоваться другим подходом. Приравняв f к нулю, выразим старшую степень x^n. Данное значение будем подставлять вместо x^n каждый раз, когда при умножении будет появляться многочлен соответствующей степени.

Пусть $f = 2x^2 - 2x + 1 = 0$. Тогда $-2x^2 = -2x + 1$ и $x^2 = x + 1$.

Легко убедиться, что данный подход фактически представляет собой деление с остатком многочлена x^n на неприводимый многочлен f:

$x^2 = -1 \cdot (2x^2 - 2x + 1) + (x + 1)$.

Записанное выражение показывает, что деление многочлена x^2 на неприводимый многочлен $2x^2 - 2x + 1$ дает многочлен нулевой степени -1 в качестве частного и многочлен первой степени $x + 1$ — в качестве остатка.

Теперь продемонстрируем построение таблицы умножения в рассматриваемом примере. Причем также ограничимся треугольным заполнением в силу коммутативности операции умножения.

Заполнение первого столбца, соответствующего умножению элементов группы $F_{3^2}^*$ на единичный элемент, является очевидным.

Заполнение второго столбца также является несложным. Здесь необходимо лишь умножить каждый из элементов группы $F_{3^2}^*$ на многочлен нулевой степени 2 с последующим приведением коэффициентов при степенях полученных многочленов по модулю 3.

$2 \cdot 2 = 4 = 1$;

$2 \cdot x = 2x;$
$2 \cdot (x+1) = 2x + 2;$
$2 \cdot (x+2) = 2x + 4 = 2x + 1;$
$2 \cdot 2x = 4x = x;$
$2 \cdot (2x+1) = 4x + 2 = x + 2;$
$2 \cdot (2x+2) = 4x + 4 = x + 1.$

Для заполнения третьего столбца потребуется использовать описанный выше прием, заменяющий деление с остатком.

$x \cdot x = x^2 = x + 1;$
$x \cdot (x+1) = x^2 + x = 2x + 1;$
$x \cdot (x+2) = x^2 + 2x = 1;$
$x \cdot 2x = 2x^2 = 2x + 2;$
$x \cdot (2x+1) = 2x^2 + x = 2;$
$x \cdot (2x+2) = 2x^2 + 2x = x + 2.$

Все последующие столбцы заполняются аналогичным образом.

$\cdot$	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1							
2	2	1						
x	x	$2x$	$x+1$					
$x+1$	$x+1$	$2x+2$	$2x+1$	2				
$x+2$	$x+2$	$2x+1$	1	x	$2x+2$			
$2x$	$2x$	x	$2x+2$	$x+2$	2	$x+1$		
$2x+1$	$2x+1$	$x+2$	2	$2x$	$x+1$	1	$2x+2$	
$2x+2$	$2x+2$	$x+1$	$x+2$	1	$2x$	$2x+1$	x	2

Имея построенную таблицу умножения для поля Галуа F_{3^2}, легко исследовать мультипликативную группу данного поля $F_{3^2}^*$.

Ранее было установлено, что данная группа содержит четыре образующих элемента. Найдя любой из них, можно определить порядок всех прочих элементов группы и выделить все ее циклические подгруппы.

Возьмем элемент x и последовательно возведем его в различные степени до получения единицы группы. Возведение в степень будем выполнять с помощью таблицы умножения.

При построении таблицы умножения было показано, что $x^2 = x + 1$. В качестве x^3 возьмем значение, находящееся на пересечении строки, соответствующей $(x+1)$, и столбца, соответствующего x. То есть $x^3 = x^2 \cdot x = (x+1) \cdot x = 2x + 1$. Далее будем действовать аналогичным образом.

$x^4 = x^3 \cdot x = (2x+1) \cdot x = 2,$
$x^5 = x^4 \cdot x = 2 \cdot x = 2x,$

$x^6 = x^5 \cdot x = 2x \cdot x = 2x + 2,$

$x^7 = x^6 \cdot x = (2x + 2) \cdot x = x + 2,$

$x^8 = x^7 \cdot x = (x + 2) \cdot x = 1.$

Таким образом, $O(x) = 8$, и данный элемент является образующим мультипликативной группы $F_{3^2}^*$.

Найдем порядок всех оставшихся элементов группы $F_{3^2}^*$.

$O(x^2) = O(x + 1) = 4.$

$O(x^3) = O(2x + 1) = 8.$

$O(x^4) = O(2) = 2.$

$O(x^5) = O(2x) = 8.$

$O(x^6) = O(2x + 2) = 4.$

$O(x^7) = O(x + 2) = 8.$

Следовательно,

$F_{3^2}^* = \langle x \rangle = \langle 2x + 1 \rangle = \langle 2x \rangle = \langle x + 2 \rangle,$

$H_1 = \langle x + 1 \rangle = \langle 2x + 2 \rangle = \{1, 2, x + 1, 2x + 2\}$, $H_1 \leq F_{3^2}^*$,

$H_2 = \langle 2 \rangle = \{1, 2\}$, $H_2 \leq H_1 \leq F_{3^2}^*$.