УДК 512.624

Сорокина Мария Евгеньевна,

кандидат физико-математических наук, преподаватель,

Федеральное государственное бюджетное образовательное учреждение высшего образования «Ярославский государственный университет им. П.Г. Демидова»,

Россия, 150003, г. Ярославль, ул. Советская, д. 14

ИЗУЧЕНИЕ ТЕМЫ «КОНЕЧНЫЕ ПОЛЯ» В КУРСЕ «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Аннотация. В статье приведен вариант методики работы над темой «Конечные поля» при преподавании дисциплины «Криптографические методы защиты информации».

Ключевые слова: конечное поле, мультипликативная группа конечного поля, протокол шифрования Диффи-Хеллмана.

Конечное поле – базовое алгебраическое понятие, необходимое для изучения дисциплины «Криптографические методы защиты информации». Рассмотрим один из вариантов работы с ним.

Первый этап – повторение и обобщение теоретического материала. Подробно конечные поля изучаются в курсе «Алгебра». Цель первого этапа – вспомнить и систематизировать основные факты об этом объекте. Ниже приведена подборка определений и утверждений, знание которых требуется для работы с отдельными протоколами шифрования.

Количество элементов в поле F (*мощность* поля F) обозначается |F|. *Простым* называется поле, не содержащее в себе никакого меньшего подполя. Конечные простые поля – это поля вида $Z_p=Z/(p)$, где p – простое число, и только они. *Характеристикой* конечного поля F называется наименьшее натуральное число n со свойством 1+1+…+1=0 (сумма n единиц), где 0 и 1 – нейтральные эле-

менты по сложению и умножению поля F соответственно. Используется обозначение char F = n. Например, char Z_p = p.

Пусть P – подполе поля F. Тогда F называется *расширением* поля P. В этом случае используется обозначение F/P (говорят «F над P»). Если F – расширение поля P, то F является векторным пространством над P. Размерность F как векторного пространства над P называется *степенью расширения* F над P и обозначается [F:P].

Упражнение 1. Пусть P – поле с числом элементов q и F/P – расширение степени n. Тогда $|F|=q^n$.

Упражнение 2. Любое конечное поле F имеет конечную характеристику p, где p – простое число, и |F| является степенью p.

Теорема 1. *Для каждого конечного поля* P *и для каждого целого натурального числа* n *существует одно и, с точностью до изоморфизма, только одно расширение* F/P *степени* n. (Без доказательства.)

Следствие. *Для каждого простого числа* p *и для каждого натурального числа* n *существует одно и, с точностью до изоморфизма, только одно поле с числом элементов* p^n.

Доказательство заключается в применении теоремы 1 к случаю |P|=p.

Конечное поле с числом элементов $q=p^n$ принято обозначать $\mathbf{F}_q$ или, в честь Э. Галуа, $GF(p^n)$. Приведем без доказательства ряд свойств конечных полей.

Теорема 2. *Справедливы следующие утверждения.*

1) *Мультипликативная группа* $\mathbf{F}_q^*$ *конечного поля* $\mathbf{F}_q$ *является циклической группой порядка* q-1.

2) *Группа автоморфизмов* $\mathrm{Aut}\mathbf{F}_q$ *конечного поля* $\mathbf{F}_q$ *с числом элементов* $q=p^n$ *иклическая порядка* n, *причём* $\mathrm{Aut}\mathbf{F}_q=\langle \Phi \mid \Phi(t)=t^p$ *для всех* t *в* $\mathbf{F}_q \rangle$.

3) *Если* $\mathbf{F}_{p^d}$ *– подполе поля* $\mathbf{F}_{p^n}$, **то** d|n. *Обратно: каждому натуральному делителю* d *числа* n *отвечает ровно одно подполе* $\{t \in \mathbf{F}_{p^n} \mid \Phi^d(t)=t\} = \mathbf{F}_{p^d}$.

4) *Если* $q=p^n$ *и* $\mathbf{F}_q^*=\langle g\rangle$, *то* g – *примитивный элемент поля с минимальным многочленом* f(x) *степени* n *и* $\mathbf{F}_q$ – *поле разложения над* $\mathbf{F}_p$ *многочлена* f(x).

5) *Для любого натурального числа* m *существует хотя бы один неприводимый многочлен степени* m *над* $\mathbf{F}_q$.

Пояснения к Теореме 2:

1. Группа G называется *циклической*, если все ее элементы являются степенями (в мультипликативной терминологии) одного ее элемента *a*. Элемент *a* называется *порождающим (образующим) элементом* группы G; для обозначения этого факта используется запись $G=\langle a\rangle$.

2. *Автоморфизм* поля – это изоморфизм поля на себя. Все автоморфизмы поля P образуют группу относительно операции композиции, она называется *группой автоморфизмов поля* P и обозначается AutP.

3. Если поле F получено из поля P присоединением единственного элемента g, то F называется *простым расширением* поля P, обозначается F=P(g), а g называется *примитивным элементом* расширения. Неприводимый над P многочлен с коэффициентами из P, корнем которого в F является элемент g, называется *минимальным многочленом* элемента g.

Также нам потребуются следующие утверждения о конечных группах.

Теорема 3 (Лагранж). *Порядок конечной группы делится на порядок каждой своей подгруппы.*

Следствие. *Порядок любого элемента делит порядок группы.*

Теорема 4. *Пусть* $G=\langle a\rangle$ *– циклическая группа конечного порядка* n. *Элемент* $g=a^k$ *также является образующей группы* G *тогда и только тогда, когда* (n,k)=1. *Таким образом, у циклической группы порядка* n *существует ровно* φ(n) *образующих элементов, где* φ *– функция Эйлера.*

Напомним, что *функция Эйлера* φ(n) – это мультипликативная арифметическая функция, равная количеству натуральных чисел, меньших n и взаимно про-

стых с ним. Ее значения вычисляются по формуле $\varphi(n) = n(1-1/p_1) \ldots (1-1/p_k)$, где $p_1, .., p_k$ – все простые сомножители, входящие в разложение числа n.

Применим теперь полученную информацию для построения конечных полей.

1) Конечные поля простого порядка p – это в точности кольца вычетов Z_p.

2) Поле $\mathbf{F}_p^n$ при $n > 1$ можно построить как факторкольцо $K=Z_p[x]/(f(x))$, где f(x) – неприводимый многочлен степени n над полем Z_p. Таким образом, для построения поля из p^n элементов достаточно отыскать многочлен степени n, неприводимый над полем Z_p (такой многочлен всегда существует). Элементами поля K являются классы вычетов многочленов степени меньшей n с коэффициентами из $Z_p[x]$ по модулю главного идеала, порождённого многочленом f(x).

Элемент $a=x+(f(x)) \in Z_p[x]/(f(x))$ является корнем многочлена f(x) в K, и поле $K=Z_p[x]/(f(x))$ порождается этим элементом над полем Z_p, поэтому переход от поля Z_p к полю K называется *присоединением к полю* Z_p *корня неприводимого многочлена* f(x).

Для работы с данными необходимо оцифровать элементы поля. Оцифровка производится следующим образом. Пусть $t \in \mathbf{F}_p^n$, тогда $t=b_{n-1}a^{n-1}+ b_{n-2}a^{n-2}+\ldots+ b_1a+b_0$, где $b_0, .., b_{n-1} \in Z_p$. Элементу t при стандартной оцифровке сопоставляется число $(b_{n-1}b_{n-2}\ldots b_1b_0)_p = b_{n-1}p^{n-1}+ b_{n-2}p^{n-2}+\ldots+ b_1p+b_0$ в p-ичном исчислении.

Второй этап – отработка теоретического материала. Проводится с помощью следующей **системы упражнений**.

1) Привести пример многочлена f(x) четвертой степени из кольца $Z_2[x]$, неприводимого над Z_2.

2) Построить поле $\mathbf{F}_{16}$ как факторкольцо $Z_2[x]$ по идеалу, порожденному многочленом f(x) из задания 2).

3) Пусть $a=x+(f(x))$ – образ элемента x кольца $Z_2[x]$ в $Z_2[x]/(f(x))$. Вычислить $(a+1)^5 +a^4 – (a-1)^3$.

4) Найти элемент, обратный a^3-a-1 в $\mathbf{F}_{16}$.

5) Найти какую-либо образующую мультипликативной группы $\mathbf{F}_{16}^*$. Для ограничения количества вычислений использовать следствие теоремы 3.

6) Сколько всего образующих элементов у группы $\mathbf{F}_{16}^*$? Используя результат упражнения 5) и теорему 4, найти их все.

7) Построить поле $\mathbf{F}_{25}$ и найти образующие его мультипликативной группы.

На третьем этапе применим полученные знания и умения к конкретной практической задаче. В качестве такой задачи рассмотрим *протокол шифрования Диффи-Хеллмана*, который заключается в следующем. Выбирается достаточно большое конечное поле F и образующая g мультипликативной группы F*. Элементы F оцифрованы стандартным способом. Эти данные открыты. Двое абонентов A и B общаются по открытому каналу связи. Целью дальнейших действий является получение указанными абонентами секретного ключа. Абонент A выбирает случайным образом натуральное число x и вычисляет $u=g^x$, затем передает значение u абоненту B по открытому каналу. Абонент B случайным образом выбирает натуральное число y и вычисляет $v=g^y$, затем передает значение v абоненту A. Далее A вычисляет значение $z=v^x=(g^y)^x= g^{xy}$, а B вычисляет $z=u^y=(g^x)^y= g^{xy}$. Тем самым, A и B получили один и тот же секретный ключ q=номер я при стандартной нумерации. В силу того, что задача нахождения дискретного логарифма является вычислимо трудной, несанкционированный пользователь, перехватив данные переговоров (значения u, v или оба), не сможет за реальное время вычислить секретный ключ.

Задание. В качестве поля F взять поле $\mathbf{F}_{25}$, в качестве образующего элемента группы $\mathbf{F}_{25}^*$ выбрать один из элементов, найденных в упражнении 7. Продемонстрировать работу протокола Диффи-Хеллмана при x=110, y=82.

Список литературы

1. Кострикин, А. И. Введение в алгебру. Часть III. Основные структуры / А. И. Кострикин. – М. : ФИЗМАТЛИТ, 2004. – 272 с. – Текст: непосредственный.

2. Романьков, В. А. Введение в криптографию / В. А. Романьков. – М. : ФОРУМ, 2012. – 240 с. – Текст: непосредственный.