МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ МАТЕМАТИКИ, ИНФОРМАЦИОННЫХ
И АВИАЦИОННЫХ ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ТЕОРИИ УПРАВЛЕНИЯ

Рацеев С.М.

Методические указания для самостоятельной работы студентов по дисциплине «Дополнительные главы криптографии»

для студентов специальности
10.05.03 «Информационная безопасность автоматизированных систем»

Ульяновск
2019

Рацеев С.М. Методические указания для самостоятельной работы студентов по дисциплине «Дополнительные главы криптографии» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем». – Ульяновск: УлГУ, 2019.

Методические указания рекомендованы к введению в образовательный процесс решением Ученого Совета ФМИАТ УлГУ (протокол № 2/19 от 19 марта 2019г.).

Тема 1. Группы. Кольца.

Основные вопросы темы:

Алгебраические операции. Группы. Основные свойства группы. Подгруппы. Эквивалентные условия подгруппы. Циклическая группа. Свойства циклических групп. Смежные классы. Индекс подгруппы. Теорема Лагранжа. Нормальная подгруппа. Эквивалентные условия нормальной подгруппы. Фактор-группа. Морфизмы групп. Ядро и образ гомоморфизма. Теорема о гомоморфизме групп. Кольца. Мультипликативная группа кольца. Подкольца. Критерий подкольца. Идеал кольца. Фактор-кольцо. Кольца вычетов. Морфизмы колец. Ядро и образ гомоморфизма. Теорема о гомоморфизме колец. Кольца главных идеалов. Китайская теорема об остатках для идеалов колец. Разложение кольца вычетов в прямую сумму примарных колец.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 2.1-2.4 учебного пособия [3].

Контрольные вопросы:

1. Циклическая группа. Свойства циклических групп. 2. Смежные классы. Индекс подгруппы. Теорема Лагранжа 3. Нормальная подгруппа. Эквивалентные условия нормальной подгруппы. Фактор-группа. 4. Морфизмы групп. Ядро и образ гомоморфизма. Теорема о гомоморфизме групп. 5. Кольца. Мультипликативная группа кольца. Подкольца. Критерий подкольца. 6. Идеал кольца. Фактор-кольцо. Кольца вычетов. 7. Морфизмы колец. Ядро и образ гомоморфизма. Теорема о гомоморфизме колец. Кольца главных идеалов. 8. Китайская теорема об остатках для идеалов колец. Разложение кольца вычетов в прямую сумму примарных колец.

Тема 2. Поля.

Основные вопросы темы:

Поле. Подполе. Простое поле. Характеристика поля. Простые идеалы. Поле частных. Расширение поля. Теорема о башне расширений. Конечные расширения. Алгебраические и трансцендентные элементы. Минимальный многочлен алгебраического элемента, некоторые его свойства. Строение расширения поля, полученное присоединением алгебраического элемента. Поля разложения многочлена. Конечные поля. Теорема о числе элементов конечного поля. Цикличность мультипликативной группы конечного поля. Образующие элементы конечного поля. Неприводимые многочлены над конечными полями. Автоморфизм Фробениуса. Совершенные поля. Трансцендентные расширения полей.

Рекомендации по изучению темы:

Все вопросы изложены в параграфе 2.5 учебного пособия [3].

Контрольные вопросы:

1. Поле: определение и основные свойства. Подполе. Критерий подполя. Критерий конечно-го подполя. 2. Простые поля. Характеристика поля. 3.

Расширение поля. Теорема о башне полей. 4. Алгебраические и трансцендентные элементы поля. Простые расширения полей. Теорема о классификации простых расширений полей. 5. Поле разложения многочлена. 6. Конечные поля. Построение конечного поля. 7. Образующие элементы конечного поля. 8. Неприводимые многочлены над конечными полями.

Задачи для самостоятельной работы:

1. Составить конечное поле $GF(2^d)$ на основе многочлена $p(x)$: а) $d = 3$, $p(x) = x^3 + x + 1$, б) $d = 4$, $p(x) = x^4 + x + 1$.

2. В поле $GF(2^3)$ на основе многочлена $p(x) = x^3 + x + 1$ вычислить (числа — представления двоичного вектора поля): а) $\dfrac{3^2 \cdot 5^5 + 6^3}{7^2}$, б) $\dfrac{5^3 \cdot 3^2 + 6^5}{5^6}$.

3. Для поля из предыдущей задачи с примитивным элементом α вычислить, используя таблицу дискретных логарифмов, значения: $(\alpha + 1)(2\alpha + 1)$, $(\alpha + 2)2\alpha$, $(\alpha + 1)/(\alpha + 2)$, $\dfrac{a^m \cdot b}{c} + d^n$, где $a = \alpha + 2$, $b = 2\alpha + 1$, $c = \alpha + 1$, $d = 2\alpha + 2$, $m = 6$, $n = 7$.

Тема 3. Применение конечных полей в криптографии.

Основные вопросы темы:

Блочный шифр «Кузнечик» из ГОСТ Р 34.12-2015. Рюкзачная криптосистема Шора-Ривеста на основе конечных полей. Построение ортогональных таблиц над конечными полями. Совершенные шифры на основе ортогональных таблиц.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 6.11, 8.8, 9.7 учебного пособия [3].

Контрольные вопросы:

1. Блочный шифр «Кузнечик» из ГОСТ Р 34.12-2015. 2. Рюкзачная криптосистема Шора-Ривеста на основе конечных полей. 3. Совершенные шифры на основе ортогональных таблиц.

Тема 4. Криптография, основанная на хэш-функциях.

Основные вопросы темы:

Электронная подпись на основе схем одноразовой подписи; представление подписи как пути в дереве связанных хэш-значений. Стойкость схемы сводится к предположению о стойкости используемой хэш-функции относительно задач поиска коллизий и/или прообразов. Древовидная подпись Меркля.

Рекомендации по изучению темы:

Рассматриваемые темы можно найти в литературе [3, 5, 6].

Тема 5. Криптография, основанная на кодах исправления ошибок.

Основные вопросы темы:

Обобщенные коды Рида-Соломона. Альтернативные коды. Коды Гоппы.

Построение проверочной матрицы года Гоппы. Двоичные коды Гоппы. Примеры двоичных кодов Гоппы. Схемы шифрования McEliece и Niederreiter на основе кодов Гоппы.

Рекомендации по изучению темы:

Рассматриваемые темы можно найти в литературе [3, 4, 5, 6].

Задачи для самостоятельной работы:

1. Декодер Питерсона-Горенстейна-Цирлера (двоичный случай). Пусть поле $GF(2^4)$ порождается примитивным многочленом $p(x) = x^4 + x + 1$, циклический код длины 15 порождается многочленом

$$g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}.$$

На приемном конце получен вектор v, в котором не более трех ошибок. Найти соответствующий кодовый вектор u и информационный вектор i:

$$\text{а) } v = \left(\begin{array}{cccccccccccccccc} 1, & 0, & 1, & 1, & 1, & 0, & 0, & 0, & 0, & 1, & 0, & 1, & 1, & 1, & 0 \end{array} \right),$$

$$\text{б) } v = \left(\begin{array}{cccccccccccccccc} 1, & 1, & 1, & 0, & 0, & 0, & 1, & 1, & 0, & 0, & 1, & 0, & 0, & 1, & 0 \end{array} \right),$$

$$\text{в) } v = \left(\begin{array}{cccccccccccccccc} 1, & 0, & 0, & 1, & 0, & 1, & 0, & 0, & 0, & 1, & 1, & 1, & 1, & 0, & 1 \end{array} \right).$$

2. Декодер Питерсона-Горенстейна-Цирлера (общий случай). Поле $GF(3^2)$ строится с помощью примитивного многочлена x^2+2x+2, α — примитивный элемент. Код БЧХ над $GF(3)$ с параметрами $n = 8$, $k = 3$ порождается многочленом $g(x) = 2 + x + 2x^2 + 2x^3 + x^5$, $\alpha, \alpha^2, \alpha^3, \alpha^4$ — его подряд идущие корни. На приемном конце получен вектор v, в котором не более двух ошибок. Найти соответствующий кодовый вектор u и информационный вектор i:

$$\text{а) } v = \left(\begin{array}{cccccccc} 1, & 1, & 1, & 2, & 0, & 2, & 2, & 0 \end{array} \right),$$

$$\text{б) } v = \left(\begin{array}{cccccccc} 0, & 0, & 1, & 0, & 1, & 1, & 0, & 2 \end{array} \right).$$

3. Поле $GF(2^3)$ строится с помощью примитивного многочлена $x^3 + x + 1$, α — примитивный элемент. Код Рида-Соломона с параметрами $n = 7$, $k = 3$, $d = 5$ исправляет до двух ошибок. На приемном конце получен вектор v, в котором не более двух ошибок. Найти соответствующий кодовый вектор u с помощью алгоритма Питерсона-Горенстейна-Цирлера и информационный вектор i. Получить вектор i с помощью дискретного преобразования Фурье, если:

$$\text{а) } v = \left(\begin{array}{cccccccc} \alpha^2, & 1, & \alpha, & \alpha^4, & \alpha^2, & \alpha^6, & 1 \end{array} \right),$$

$$\text{б) } v = \left(\begin{array}{cccccccc} \alpha^6, & \alpha^4, & \alpha^6, & 1, & \alpha^5, & \alpha^4, & \alpha \end{array} \right).$$

4. Поле $GF(2^3)$ строится с помощью примитивного многочлена $x^3 + x + 1$, α — примитивный элемент. Код Рида-Соломона с параметрами $n = 7$, $k = 3$, $d = 5$ исправляет до двух ошибок. На приемном конце получен вектор v, в котором не более двух ошибок. Найти соответствующий кодовый вектор u (с

помощью алгоритма Сугиямы и метода Форни) и информационный вектор i, если:

$$\text{а) } v = \left(1,\ \alpha^4,\ \alpha^5,\ \alpha,\ 1,\ \alpha^4,\ \alpha^3 \right),$$

$$\text{б) } v = \left(\alpha^6,\ \alpha^2,\ \alpha,\ \alpha^3,\ \alpha^4,\ \alpha^3,\ \alpha^6 \right).$$

Тема 6. Криптография, основанная на решётках.

Основные вопросы темы: Задача поиска кратчайшего вектора (SVP); SVP 2 NP. Задача поиска ближайшего вектора (CVP); CVP 2 NP. Обучение с ошибками (LWE; RLWE). Наименьшее целочисленное ре-шение СЛАУ (SIS). Система Ring-Learning with Errors.

Рекомендации по изучению темы:

Рассматриваемые темы можно найти в литературе [3, 5, 6].

Тема 7. Выбор точки и размещение данных.

Основные вопросы темы:

Выбор точки эллиптической кривой. Размещение данных на эллиптической кривой. Определение порядка точки эллиптической кривой и нахождение образующего элемента группы точек эллиптической кривой.

Рекомендации по изучению темы:

Все вопросы изложены в параграфе 2.1 учебного пособия [2].

Контрольные вопросы:

1. Определение порядка точки эллиптической кривой. 2. Нахождение образующего элемента группы точек эллиптической кривой.

Тема 8. Криптосистемы на эллиптических кривых.

Основные вопросы темы:

Модификация системы Диффи-Хеллмана на эллиптических кривых. Вероятностное шифрование на основе эллиптических кривых, модификация шифра Эль-Гаамаля. Модификация протокола Месси-Омуры на эллиптических кривых. Модификация протокола Шнорра на эллиптических кривых. Модификация трехпроходного протокола Шнорра на эллиптических кривых. Модификация протокола Окамото на эллиптических кривых. Модификация семейства протоколов MTI на эллиптических кривых. Модификация протокола аутентификации с нулевым разглашением на основе системы Диффи-Хеллмана с использованием эллиптических кривых. Протокол привязки к биту на основе протокола Шнорра с использованием эллиптических кривых. Протокол типа “подбрасывание монеты по телефону” с использованием эллиптических кривых. Модификация протокола голосования на эллиптических кривых. Пятипроходный протокол идентификации на основе изоморфизма графов с использованием эллиптических кривых. Модификация схемы Фельдмана-Шамира на эллиптических кривых. Модификация схемы

Педерсона-Шамира на эллиптических кривых. Электронная подпись ГОСТ Р 34.10-2012. Электронная подпись ECDSA.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 9.2-9.4, 12.6, 13.1, 14.3, 15.3 учебного пособия [3].

Контрольные вопросы:

1. Модификация системы Диффи-Хеллмана на эллиптических кривых. 2. Вероятностное шифрование на основе эллиптических кривых, модификация шифра Эль-Гаамаля. 3. Модификация протокола Месси-Омуры на эллиптических кривых. 4. Модификация схемы разделения секрета Фельдмана-Шамира на эллиптических кривых. 5. Модификация схемы разделения секрета Педерсона-Шамира на эллиптических кривых. 6. Модификация протокола аутентификации Шнорра на эллиптических кривых. 7. Модификация трехпроходного протокола аутентификации Шнорра на эллиптических кривых. 8. Модификация протокола аутентифкации Окамото на эллиптических кривых. 9. Модификация протокола аутентификации с нулевым разглашением на основе системы Диффи-Хеллмана с использованием эллиптических кривых. 10. Модификация протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамаля с использованием эллиптических кривых. 11. Модификация семейства протоколов MTI на эллиптических кривых. 12. Протокол привязки к биту на основе протокола Шнорра с использованием эллиптических кривых. 13. Протокол типа "подбрасывание монеты по телефону" с использованием эллиптических кривых. 14. Электронная подпись ГОСТ Р 34.10-2012. 15. Электронная подпись ECDSA.

Задачи для самостоятельной работы:

1. Модифицированный протокол Шнорра. Пусть $\mathrm{E}_p(u, v)$ — эллиптическая кривая (задается уравнением $y^2 = x^3 + ux + v \pmod p$), известная участникам информационного процесса, G — предварительно согласованная и опубликованная точка порядка n этой кривой, x, Y — соответственно секретный и открытый ключ абонента A ($Y = [-x]G$), k — случайное число из первого шага протокола, a — запрос из второго шага протокола. Известно, что $p = 11$, $u = 10$, $v = 8$, $G = (7, 5)$, $x = 4$, $a = 2$, $k = 3$. Найти n, Y и привести все вычисления на всех шагах протокола (найти R, s, проверить соответствующее равенство).

2. Модифицированный протокол Окамото. Пусть $\mathrm{E}_p(u, v)$ — эллиптическая кривая, известная участникам информационного процесса, G_1, G_2 — предварительно согласованные и опубликованные точки порядка n этой кривой, x_1, x_2 — пара секретных ключей абонента A, Y — открытый ключ абонента A ($Y = [-x_1]G_1 + [-x_2]G_2$), k_1, k_2 — случайные числа из первого шага протокола, a — запрос из второго шага протокола. Известно, что $p = 11$, $u = 10$, $v = 8$, $G_1 = (2, 5)$, $G_2 = (6, 3)$, $x_1 = 3$, $x_2 = 5$, $a = 5$, $k_1 = 2$, $k_2 = 3$. Найти

n, Y и привести все вычисления на всех шагах протокола (найти R, s_1, s_2, проверить соответствующее равенство).

Тема 9. Дискретное логарифмирование на эллиптической кривой.

Основные вопросы темы:

Критерий простоты, использующий эллиптические кривые. Разложение на множители при помощи эллиптических кривых. Универсальные методы логарифмирования. Гельфонда-Шенкса. Метод Полларда. Метод встречи на случайном дереве. Логарифмирование с использованием функции Вейля. Требования к эллиптической кривой.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 1.6, 3.2 учебного пособия [2].

Контрольные вопросы:

1. Критерий простоты, использующий эллиптические кривые. 2. Разложение на множители при помощи эллиптических кривых. 3. Универсальные методы логарифмирования. Метод Гельфонда-Шенкса. 4. Метод Полларда. 5. Метод встречи на случайном дереве. 6. Логарифмирование с использованием функции Вейля.

Литература

[1] Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. М.: КомКнига, 2006. 328 с.

[2] Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006. 280 с.

[3] Рацеев С.М. Математические методы защиты информации [Электронный ресурс]: Электронное учеб. пособие. – Ульяновск: УлГУ, 2018. 1 CD-R. № гос. регистрации – 0321901084.

[4] Сагалович Ю.Л. Введение в алгебраические коды. Учебное пособие. – 2-е изд., перераб. и доп. – М.: ИППИ РАН, 2010. – 302 с.

[5] Тилборг ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. – М.: Мир, 2006. – 471 с.

[6] Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. М.: Академия, 2009. 272 с.