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 10.05.01 «Компьютерная безопасность»

Ульяновск
2019

Рацеев С.М. Методические указания для самостоятельной работы студентов по дисциплине «Дополнительные главы криптографии» для студентов специальности 10.05.01 «Компьютерная безопасность». – 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. Криптография, основанная на хеш-функциях

Основные вопросы темы:

Хеш-функции. Криптографические хеш-функции. Способы построения криптографических хеш-функций. Понятие имитации и подмены кода аутентификации. Определение вероятностей P_{im}, P_{podm}. Нижние оценки для вероятности имитации и подмены кода аутентификации. Критерий достижимости нижних оценок. Оптимальные коды аутентификации. Достаточные условия оптимального кода аутентификации. Электронная подпись на основе схем одноразовой подписи; представление подписи как пути в дереве связанных хеш-значений. Стойкость схемы сводится к предположению о стойкости используемой хеш-функции относительно задач поиска коллизий и/или прообразов. Древовидная подпись Меркля.

Рекомендации по изучению темы:

Рассматриваемые темы можно найти в литературе [1, 3, 4].

Тема 2. 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 [1, 2, 3, 4].

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:

а) $v = \big(\ 1,\ 0,\ 1,\ 1,\ 1,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 1,\ 1,\ 0\ \big)$,

б) $v = \big(\ 1,\ 1,\ 1,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0\ \big)$,

в) $v = \big(\ 1,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 1,\ 1,\ 1,\ 0,\ 1\ \big)$.

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:

а) $v = \big(\ 1,\ 1,\ 1,\ 2,\ 0,\ 2,\ 2,\ 0\ \big)$,

б) $v = \left(\ 0, \ \ 0, \ \ 1, \ \ 0, \ \ 1, \ \ 1, \ \ 0, \ \ 2 \ \right).$

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:

а) $v = \left(\ \alpha^2, \ \ 1, \ \ \alpha, \ \ \alpha^4, \ \ \alpha^2, \ \ \alpha^6, \ \ 1 \ \right),$

б) $v = \left(\ \alpha^6, \ \ \alpha^4, \ \ \alpha^6, \ \ 1, \ \ \alpha^5, \ \ \alpha^4, \ \ \alpha \ \right).$

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:

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

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

Тема 3. Криптография, основанная на решётках

Основные вопросы темы:

Алгебраическая решётка. Основные свойства решёток. Модулярные и дистрибутивные решетки. 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 [1, 3, 4].

Литература

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

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

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

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