Программа магистерского курса «Математические методы защиты информации»

(3 семестр магистратуры ММФ, 2013-2014 учебный год)

Автор программы Лось Антон Васильевич

Отдельные главы теории кодирования

- Скорость кода, пропускная способность, энтропия по Шеннону, ее свойства. Вероятность ошибки декодирования. Математическое ожидание, дисперсия, неравенство Чебышева. Объем шара (через энтропию). Теорема Шеннона для двоичного симметричного канала связи с шумом (с доказательством).
- Код, линейный код, циклический код. Код БЧХ. Декодирование БЧХ-кодов (алгоритм Горенстейна-Питерсона-Цирлера). Декодирование БЧХ-кодов, исправляющих две ошибки. Декодирование двоичных БЧХ-кодов (общий случай).
- Каскадные методы построения кодов. Каскадные методы кодирования Зиновьева (два метода), Соловьевой, Фелпса. Двоичные коды малых длин с кодовым расстоянием 3, с наилучшими на сегодняшний день параметрами. Использование конструкции Плоткина для построения бесконечных классов двоичных кодов с хорошими параметрами.
- Свитчинговые методы построения кодов. Конструкция Васильева как свитчинговая конструкция. Коды Моллара. Вторая и третья теоремы Шапиро и Злотника.
- Коды Рида-Маллера, определение, конструкция, группа автоморфизмов. Код Хэмминга как код Рида-Маллера. Применение на практике.
- Применение теории кодирования на практике (кодирование для жестких магнитных дисков, кодирование для систем передачи по оптоволоконным кабелям, кодирование для систем хранения информации во флэш-памяти, кодирование в системах мобильной связи GSM, система цифровой магнитной записи звука R-DAT).

Введение в криптологию

- Введение в криптологию. Секретность и имитостойкость. Основные идеи. Криптография и криптоанализ.
- Криптографические системы с секретными ключами. Подстановки. Перестановки. Полиалфавитные шифры. Шифр с бегущим ключом. Криптографические системы коды. Стандарты шифрования данных DES, AES, GOST. S-блоки.
- APN-функции, их свойства. Мономиальные APN-функции. Параметры кода, отвечающего APN-функциям – длина кода, кодовое расстояние, размерность, радиус покрытия. Теорема Зиновьева-Додунекова о коде Препараты.

- Определение совершенно секретного шифра. Теорема Шеннона о существовании совершенно секретных шифров.
- Криптографические системы с открытыми ключами. Односторонняя функция с лазейкой. “Шарады” Меркля.
- Криптосистема Диффи и Хэллмана и проблема вычисления дискретного логарифма.
- Криптосистема RSA и проблема разложения числа на простые сомножители.
- Криптосистемы Шамира и ЭльГамаля.
- Кодирующая система МакЭлиса. Криптосистема Нидеррайтера.
- Цифровая подпись, применение различных криптосистем для создания цифровой подписи.
- Определение эллиптической кривой. Криптосистемы на эллиптических кривых, электронная подпись.

Сжатие информации

- Разделимые и префиксные коды. Стоимость кодирования, энтропия и ее свойства, избыточность. Неравенство Крафта-Макмиллана. Теорема Крафта, теорема Макмиллана.
- Оптимальное кодирование. Метод Хаффмена. Теорема Хаффмена. Метод Фано.
- Метод Шеннона для бернуллиевских источников. Теоремы Шеннона.
- Критерий разделимости побуквенного кодирования. Теоремы Маркова. Алгоритм распознавания разделимости, основанный на теоремах Маркова.
- Код “стопка книг”.
- Адаптивные методы сжатия данных. Методы Лемпела-Зива и их модификации.
- Арифметический код.

Основная литература

1. Б. Я. Рябко, А. Н. Фионов, Основы современной криптографии для специалистов в информационных технологиях, Изд-во “Научный Мир”, М. 2004.
2. Б. Я. Рябко, А. Н. Фионов, "Криптографические методы защиты информации", Изд-во «Телеком. Горячая линия, М., 2005.
3. Р. Е. Кричевский, Сжатие и поиск информации. Наука, 1986.
4. В. И. Нечаев, Элементы криптографии. Основы теории защиты информации. – М.: Высшая школа. 1999. – 109 с.
5. Л. А. Шоломов, Основы теории дискретных логических и вычислительных устройств. – М.: Наука. 1980. – 399 с.
6. В. Н. Потапов, Теория информации. Кодирование дискретных вероятностных источников. Новосибирск: Изд. центр НГУ. 1999. 71 с.
7. В. Д. Колесник, Кодирование при передаче и хранении информации (алгебраическая теория блоковых кодов), Москва, Высшая школа. 2009, 550 с.

8. Б. Д. Кудряшов, Теория информации, издательский дом “Питер”, 2009, 213 с., под грифом УМО.
9. Ф. И. Соловьева, Введение в теорию кодирования, учебное пособие для студентов ММФ и ФИТ НГУ., Изд. НГУ, 2011г., 123 с., под грифом УМО.

Дополнительная литература

10. Л. А. Шеннон, Работы по теории информации и кибернетике. М.: ИЛ. 1963.
11. Введение в криптографию. Под ред. В. В. Ященко. Москва, МЦНМО – ЧеРо, 1999.
12. А. Саломаа, Криптография с открытым ключом. Пер. с англ. – М.: Мир. 1996. – 318 с.
13. С. Баричев, Р. Серов, Основы современной криптографии, Москва, 2001. - 121 с.
14. Ж. Земор, Курс криптографии, М.-Ижевск: НИЦ “Регулярная и хаотическая динамика”; Институт компьютерных исследований, 2006. – 256 с.

Интернет-ресурсы

1. Теория кодирования в НГУ, см. http://www.codingtheory.nsu.ru
2. В. Н. Потапов, Введение в теорию информации, 102 с., см. http://math.nsc.ru/~potapov/posobiya.htm