БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ

Председатель Учебно-методического
объединения вузов Республики Беларусь
по естественнонаучному образованию
_____ В.В. Самохвал

«____»_____ 2006 г.

Регистрационный № ТД -_____/тип.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ

Учебная программа
для Белорусского государственного университета по специальности
1- 98 01 01- 01 Компьютерная безопасность

Минск
2006

Составители:
С.В. Агиевич – заведующий НИЛ проблем безопасности информационных технологий Национального научно–исследовательского центра прикладных проблем математики и информатики Белгосуниверситета, кандидат физ.–мат. наук

Рецензенты:

Кафедра информатики Белорусского государственного университета информатики и радиоэлектроники;

В.И. Берник – главный научный сотрудник отдела комбинаторных моделей и алгоритмов Института Математика НАН Беларуси, доктор физ.-мат. наук, профессор

Рекомендована к утверждению в качестве базовой для БГУ:

Кафедрой математического моделирования и анализа данных Белорусского государственного университета
(протокол №15 от «04» апреля 2006 г.).

Научно-методической комиссией факультета прикладной математики и информатики Белорусского государственного университета
(протокол №___ от «____»_____2006г.).

Ученым Советом факультета прикладной математики и информатики
(протокол №5 от «25» апреля 2006 г.).

Научно-методическим Советом Белорусского государственного университета
(протокол №___ от «____»_____2006г.).

Согласована
Научно-методическим Советом по компьютерной безопасности УМО вузов Республики Беларусь по естественнонаучному образованию
(протокол №___ от «____»_____2006г.).

Ответственный за редакцию: С.В. Агиевич

Ответственный за выпуск: О.А. Кастрица

Пояснительная записка

Дисциплина «Криптографические методы» знакомит студентов с криптографическими методами защиты информации.

Основой для изучения курса являются дисциплины «Математический анализ», «Геометрия и алгебра», «Дискретная математика», «Теория вероятностей и математическая статистика» и «Теория информации», изучаемые в 1–5 семестрах. Сведения, излагаемые в курсе «Криптографические методы», используются при изучении курсов «Теоретические основы информационной безопасности», «Программно–аппаратные средства обеспечения информационной безопасности», а также при изучении ряда дисциплин специализации.

Курс «Криптографические методы» призван дать студентам сведения, необходимые для разработки, анализа и эксплуатации средств криптографической защиты информации.

В соответствии со стандартом специальности учебная программа предусматривает для изучения дисциплины 136 аудиторных часов, в том числе лекционных – 68, лабораторных – 28 ч., практических – 28 ч. и 12 ч. контролируемой самостоятельной работы.

Содержание

Введение

История криптографии. Абоненты, коммуникации и угрозы. Задачи криптографии и криптоанализа. Криптосистемы (шифрсистемы). Шифры перестановки, замены, Виженера, Вернама. Представление о современных криптосистемах.

Элементы теории Шеннона

Совершенные криптосистемы. Энтропия, условная энтропия, удельная энтропия. Расстояние единственности.

Элементы теории конечных полей

Определения. Подполя и расширения полей. Характеристика поля. Многочлены, идеалы и факторкольца. Существование конечного поля. Единственность конечного поля. Соотношения между подполями. Функция следа. Мультипликативная группа конечного поля.

Булевы функции

Булевы функции и отображения. Преобразование Мебиуса. Преобразование Уолша-Адамара. Нелинейность. S-блоки.

Блочные криптосистемы

Блочно-итерационные криптосистемы. Схема подстановки-перестановки. Использование инволютивных подстановок. Схема Фейстеля. Условия атак. Задачи криптоанализа. Сложность атак. Модельная криптосистема. Криптоанализ «грубой силой». Случайные размещения и баланс «время – память». Групповой криптоанализ. Таблицы разностей. Разностный криптоанализ. Конструкция Нюберг. Линейные аппроксимации. Линейный криптоанализ. Режим простой замены. Режим счетчика. Режим цепной обработки. Режим гаммирования с обратной связью. Каскады.

Свойства линейных рекуррентных последовательностей

Порядок многочлена. Примитивные многочлены. Период л.р.п. Минимальный многочлен. Постулаты Голомба.

Поточные криптосистемы

Конечные автоматы. Регистры сдвига с линейной обратной связью. Фильтрующий генератор. Комбинирующий генератор. Генератор с неравномерным движением. Криптосистема A5/1. Сжимающий и самосжимающий генератор. Линейная сложность. Корреляционный криптоанализ. Корреляционно-иммунные функции.

Элементы теории сложности

Вычислительные проблемы. Машины Тьюринга. Предикаты. Сложностные классы. Вероятностные машины. Алгоритмы типа Монте-Карло и Лас-Вегас. Односторонние и свободные от коллизий функции. Логарифмическая функция.

Функции хэширования

Определения и задачи криптоанализа. Блочно-итерационные функции хэширования. Функция хэширования СТБ 1176.1. Атака «дней рождения». Алгоритм Брента. Ключезависимые функции хэширования. Генераторы псевдослучайных чисел на базе функций хэширования.

Криптосистемы с открытым ключом

Функции с лазейкой. Использование функций с лазейкой для построения криптосистем с открытым ключом. Функция Рабина. Функция RSA. RSA и факторизация. Реализация: арифметика больших чисел, алгоритм Евклида, возведение в степень, оптимизация RSA, построение простых чисел, проверка простоты.

Электронная цифровая подпись

Схема ЭльГамаля. Модификации схемы ЭльГамаля. Реализация схемы ЭльГамаля. Схема Шнорра. Система ЭЦП СТБ 1176.2. Слепые подписи. Неопровержимые подписи.

Факторизация и дискретное логарифмирование

Алгоритм p – 1. Ро-методы. Алгоритм Диксона. Квадратичное решето. Метод больших-малых шагов. Метод Поллига – Хэллмана. Индекс-метод.

Практическая криптография

Управление ключами. Протокол Диффи – Хэллмана. Сертификаты открытых ключей. Инфраструктура открытых ключей. Протоколы сети Интернет. Аутентификация.

Литература

Основная

1. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. — Москва: Гелиос АРВ, 2001. —480 с.
2. Бабаш А. В., Шанкин Г. П. Криптография. Аспекты Защиты. — Москва: Солон–Р, 2002. — 512 с.
3. Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В. Математические и компьютерные основы криптологии. — Минск: Новое знание, 2003. — 320 с.
4. Харин Ю.С., Агиевич С.В. Компьютерный практикум по математическим методам защиты информации. — Минск, БГУ, 2001. — 190 с.

Дополнительная

5. Menezes A.J., van Oorschot P. C., Vanstone S.A. Handbook of Applied Cryptography. — CRC Press, 1996. — 816 p.
6. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source code in C. — John Wiley & Sons, 1996. — 675 p.
7. Stinson D. Cryptography. Theory and Practice. – N.Y. CRC, 1995.