Министерство образования Республики Беларусь

Учебно-методическое объединение высших учебных заведений Республики Беларусь по естественнонаучному образованию

УТВЕРЖДАЮ
Первый заместитель Министра образования Республики Беларусь
_____ А.И. Жук
16.06.2010
(дата утверждения)
Регистрационный № ТД-Р.217/тип.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ

Типовая учебная программа для высших учебных заведений по направлению специальности

1-98 01 01-01 Компьютерная безопасность (математические методы и программные системы)

СОГЛАСОВАНО
Председатель Учебно-методического объединения вузов Республики Беларусь по естественнонаучному образованию
_____ В.В. Самохвал
_____
(дата)

СОГЛАСОВАНО
Начальник Управления высшего и среднего специального образования
_____ Ю.И. Миксюк
16.06.2010
(дата)

Проректор по учебной и воспитательной работе Государственного учреждения образования «Республиканский институт высшей школы»
_____ В.И. Шупляк
_____
(дата)
12.05.2010
(дата)

Эксперт-нормоконтролер
_____
18.05.2010
(дата)

Минск 2009

СОСТАВИТЕЛИ:
С.В. Агиевич, доцент кафедры математического моделирования и анализа данных Белорусского государственного университета, кандидат физико-математических наук

РЕЦЕНЗЕНТЫ:
Кафедра информационных технологий автоматизированных систем Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»
В.И. Берник, заведующий отделом теории чисел Института математики Национальной академии наук Беларуси, доктор физико-математических наук, профессор

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ В КАЧЕСТВЕ ТИПОВОЙ:
Кафедрой математического моделирования и анализа данных Белорусского государственного университета
(протокол № 2 от 02.09.2008 г.)

Научно-методическим советом Белорусского государственного университета
(протокол № 1 от 01.12.2008 г.);

Научно-методическим советом по специальности 1-98 01 01 Компьютерная безопасность Учебно-методического объединения вузов Республики Беларусь по естественнонаучному образованию
(протокол № 1 от 11.03. 2009 г.)

Ответственный за выпуск: Агиевич С.В.

Пояснительная записка

Криптографические методы защиты информации обеспечивают конфиденциальность, контроль целостности и проверку подлинности данных с помощью ключезависимых или бесключевых криптографических преобразований.

Дисциплина «Криптографические методы» знакомит студентов с методами построения криптографических преобразований, а также методами оценки их надежности. Дисциплина дает представление об основных типах криптографических систем: блочных, поточных, криптосистемах с открытым ключом, систем электронной цифровой подписи, функций хэширования.

Изучаемые криптографические методы основываются на использовании объектов и применении методов широкого набора математических дисциплин: алгебры, теории чисел, теории вероятностей, математической статистики, теории информации, теории сложности.

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

Изучение криптографических методов преследует две основные цели: во-первых, дать студентам теоретические основы построения надежных криптографических преобразований, и, во-вторых, сформировать навыки использования криптографических преобразований для построения систем защиты информации. Для достижения второй цели предназначен компьютерный практикум.

В результате изучения дисциплины обучаемый должен:

знать:

- методы построения надежных блочных и поточных криптосистем, функций хэширования, криптосистем с открытым ключом и систем электронной цифровой подписи;
- задачи и основные методы криптоанализа;
- стандартные криптосистемы и использование криптографии на практике.

уметь:

- применять полученные знания для создания надежных систем защиты информации.

В соответствии с типовым учебным планом направления специальности 1-98 01 01-01 «Компьютерная безопасность (математические методы и программные системы)» учебная программа предусматривает для изучения дисциплины всего 280 часов, в том числе 136 аудиторных часов: лекции – 68 часов, лабораторные занятия – 28 часов, практические занятия – 40 часов.

Примерный тематический план

№	Название раздела, темы	Количество аудиторных часов			
		Всего	В том числе		
			Лекции	Лаб. занятия	Практические занятия
	Раздел I. Криптография с секретным ключом				
1.	Введение в криптографию	4	4		
2.	Классические криптосистемы	6	2		4
3.	Элементы теории Шеннона	4	2		2
4.	Элементы теории конечных полей	10	6		4
5.	Булевы функции в криптографии	10	2	6	2
6.	Блочные криптосистемы	22	10	8	4
7.	Свойства линейных рекуррентных последовательностей	4	2		2
8.	Поточные криптосистемы	8	6		2
	Раздел II. Криптография с открытым ключом				
9.	Протокол Диффи – Хэллмана	4	2		2
10.	Элементы теории сложности	2	2		
11.	Односторонние функции	4	4		
12.	Криптосистемы с открытым ключом	10	4	2	4
13.	Генерация простых чисел	6	2	2	2
14.	Функции хэширования	12	6	4	2
15.	Электронные цифровые подписи	10	4	2	4
16.	Факторизация и дискретное логарифмирование	10	6	2	2
17.	Эллиптические кривые в криптографии	10	4	2	4
	Всего	136	68	28	40

Содержание

Раздел I. Криптография с секретным ключом

1. Введение в криптографию

История криптографии. Абоненты, коммуникации и угрозы. Задачи криптографии и криптоанализа. Криптосистемы (шифрсистемы). Типы атак. Сложность атак.

2. Классические криптосистемы

Шифр сдвига. Аффинный шифр. Шифр простой замены. Шифр Хилла. Шифр перестановки. Шифр Виженера.

3. Элементы теории Шеннона

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

4. Элементы теории конечных полей

Подполя и расширения полей. Характеристика поля. Существование конечного поля. Единственность конечного поля. Соотношения между подполями. Функция следа. Мультипликативная группа конечного поля.

5. Булевы функции в криптографии

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

6. Блочные криптосистемы

Блочно-итерационные криптосистемы. SP-криптосистемы. AES. Использование инволютивных подстановок. Криптосистемы Фейстеля. Атака «грубой силой». Баланс «время – память». Таблицы разностей. Разностная атака. Конструкция Нюберг. Линейные аппроксимации. Линейная атака. Режим простой замены. Режим счетчика. Режим цепной обработки. Режим гаммирования с обратной связью.

7. Свойства линейных рекуррентных последовательностей

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

8. 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.

Раздел II. Криптография с открытым ключом

9. Протокол Диффи – Хэллмана

Идея криптографии с открытым ключом. Головоломки Меркля. Протокол Диффи – Хэллмана. Реализация протокола Диффи – Хэллмана.

10. Элементы теории сложности

Вычислительные проблемы. Машины Тьюринга. Предикаты. Сложностные классы. Вероятностные машины. Алгоритмы типа Монте-Карло и Лас-Вегас.

11. Односторонние функции

Определение. Функция Рабина. Функции с лазейкой. Лазейка функции Рабина. Функция RSA. Функция Эль-Гамаля.

12. Криптосистемы с открытым ключом

Использование функций с лазейкой для построения криптосистем с открытым ключом. Криптосистема RSA. RSA и факторизация. Реализация: арифметика больших чисел, алгоритм Евклида, возведение в степень, оптимизация RSA.

13. Генерация простых чисел

Язык PRIMES. Проверка простоты. Тесты Ферма и Миллера – Рабина. Построение простых. Теорема Диемитко.

14. Функции хэширования

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

15. Электронные цифровые подписи

Использование функций с лазейкой для построения систем ЭЦП. ЭЦП ЭльГамаля. Реализация ЭЦП ЭльГамаля. ЭЦП Шнорра. Система ЭЦП СТБ 1176.2.

16. Факторизация и дискретное логарифмирование

Алгоритм p – 1. ρ-методы. Выбор модуля RSA. Метод больших-малых шагов. λ-метод. Метод Поллига – Хэллмана. Алгоритм Диксона. Квадратичное решето. Индекс-метод.

17. Эллиптические кривые в криптографии

Основные понятия. Сложение точек. Кривые над конечными полями. Кратная точка. ЭЦП Шнорра на эллиптических кривых.

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

1. Menezes A.J., van Oorschot P. C., Vanstone S.A. Handbook of Applied Cryptography. — CRC Press, 1996. — 816 p.
2. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source code in C. — John Wiley & Sons, 1996. — 675 p.
3. Stinson D. Cryptography. Theory and Practice. – N.Y. CRC, 1995 — 434 p.