Лекции по курсу "Решетки, алгоритмы, теория чисел и современная криптография"

Лекторы к.ф.-м.н. А.В.Шокуров, д.ф.-м.н. Н.Н.Кузюрин

Государственный комитет по высшему образованию
Московский физико-технический институт

Рабочая программа курса

Решетки, алгоритмы, теория чисел и современная криптография

Курс —
Семестр —
Лекции — 36 часов экзамен — семестр

Программу составили д.ф.-м.н. Н.Н.Кузюрин и к.ф.-м. А.В. Шокуров

Программа обсуждена на заседании кафедры

_„____“_____200 г.

Заведующий кафедрой

Тема 1. Введение. Базовые понятия криптографии. Связь с теорией чисел.

Лекция 1. Криптография с открытым ключом. Криптосистема RSA и проблема факторизации натуральных чисел.

Лекция 2. Дискретный логарифм. Сложность в худшем случае. Сложность в среднем. Сложность в среднем дискретного логарифма. Понятие односторонней функции.

Лекция 3. Задача о рюкзаке. Предварительные сведения из теории решеток.

Тема 2. Необходимые сведения из теории колец, полей и решеток

Лекция 5. Понятие кольца. Кольца с однозначным разложением на множители. Поле. Примеры полей.

Лекция 6. Конечные поля. Расширения полей: алгебраические и трансцендентные. Нормальные и сепарабельные расширения.

Лекция 7. Основные понятия теории решеток. Критерий полноты решетки. Лемма Минковского.

Лекция 8. Примеры некоторых решеток. Структура группы единиц порядков поля алгебраических чисел.

Тема 4. Алгоритмические аспекты теории решеток и их применение в криптографии

Лекция 9. Оценки сложности выполнения арифметических операций. Делимость и алгоритм Евклида.

Лекция 10. Сложность решения систем линейных диофантовых уравнений

Лекция 11-12. Полиномиальный алгоритм проверки простоты чисел.

Лекция 13. Кратчайший ненулевой вектор решетки. Ближайший вектор к заданному вектору решетки. Приближенные алгоритмы.

Лекция 14. Приведенный базис в решетке. Алгоритм Ловаса.

Лекция 15. Результаты Айтаи о сложности поиска короткого вектора в случайной решетке.

Лекция 16. Некоторые криптосистемы на решетках.

Рекомендуемая литература

1. З.И. Боревич, И.Р. Шафаревич, Теория чисел, Москва, Наука, 1985.

2. А. Схрейвер, Теория линейного и целочисленного программирования, т 1, 2, М. Мир, 1980.

3. О.Н. Василенко, Теоретико числовые алгоритмы в криптографии, МЦНМО, 2003.

4. Н. Коблиц, Курс терии чисел и криптографии, Научное издательство „ТВП“Москва, 2001.

5. Введение в криптографию, (под редакцией В.В. Ященко), МЦНМО, 2000.

Дополнительная литература.

1. M. Agrawal, N. Kayal, N. Saxena, Primes is in P, Annals of Mathematics, 2004, v. 160, pp. 781–793.

2. M. Ajtai, Generating Hard Instances of Lattice Problems, In 28th ACM Symposium on Theory of Computing, Philadelphia, 1996, 99–108.