Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (национальный исследовательский университет)»

УТВЕРЖДЕНО
Директор физтех-школы прикладной математики и информатики
А.М. Райгородский

Рабочая программа дисциплины (модуля)

по дисциплине: Решетки, алгоритмы и современные проблемы криптографии
по направлению: Прикладные математика и физика
профиль подготовки: Радиотехника и компьютерные технологии
Физтех-школа Радиотехники и Компьютерных Технологий
кафедра системного программирования
курс: 4
квалификация: бакалавр

Семестр, формы промежуточной аттестации: 8 (весенний) - Экзамен

Аудиторных часов: 30 всего, в том числе:
лекции: 15 час.
семинары: 15 час.
лабораторные занятия: 0 час.

Самостоятельная работа: 30 час.

Подготовка к экзамену: 30 час.

Всего часов: 90, всего зач. ед.: 2

Программу составили:

А.В. Шокуров, канд. физ.-мат. наук, доцент
С.А. Фомин

Программа обсуждена на заседании кафедры системного программирования 15.05.2020

Аннотация

Цель учебного курса – ознакомление студентов с важнейшими современными инструментами построения криптосистем, использующими методы теории чисел и алгебраической геометрии. Особое внимание уделяется методам, использующим решётки в евклидовом пространстве. Основой для использования такого подхода являются предположения о сложности некоторых задач на решётках.

Важным обстоятельством здесь является принципиальный для криптографии результат Айтаи, свидетельствующий о том, что из сложности задачи определения ближайшего вектора на решётках следует сложность в среднем такой задачи. В курсе даются строгие математические определения необходимых понятий алгебры и теории чисел, а также доказательства важнейших необходимых утверждений.

1. Цели и задачи

Цель дисциплины

Ознакомление студентов с важнейшими современными инструментами построения криптосистем, использующими методы теории чисел и алгебраической геометрии. Важным обстоятельством здесь является важный для криптографии результат Айтаи о том, что из сложности некоторых задач на решетках следует сложность в среднем такой задачи.

Задачи дисциплины

- ознакомить студентов с методами, использующими решетки в евклидовом пространстве. Основой для использования такого подхода являются предположения о сложности некоторых задач на решетках;
- ознакомить студентов с методами криптографии и элементами теории сложности.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-2 Способен использовать современные информационные технологии и программные средства при решении задач профессиональной деятельности, соблюдая требования информационной безопасности	ОПК-2.1 Способен применять современные вычислительную технику и сервисы сети Интернет в области (сфере) профессиональной деятельности
ПК-3 Способен выбирать и применять подходящее оборудование, инструменты и методы исследований для решения задач в избранной предметной области	ПК-3.1 Знает принципы работы и диапазоны рабочих параметров используемого научного оборудования
ПК-4 Способен критически оценивать применимость используемых методик и методов	ПК-4.1 Знает численные порядки величин, характерных для соответствующей профессиональной области

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- связь общих вопросов теории чисел и алгебраической геометрии и криптографии;
- проблемы построения алгоритмов для решения задач теории чисел и алгебраической геометрии;
- основные методы анализа алгоритмической сложности задач из теории чисел и алгебраической геометрии.

уметь:

- разрабатывать, обосновывать и реализовывать новые методы и алгоритмы машинно-независимой оптимизации программ;
- разрабатывать и реализовывать новые языки и их оптимизирующие компиляторы для новых архитектур процессоров, в том числе специализированных;
- применять компиляторные методы и компиляторные среды для решения задач обратной инженерии, защиты программного кода, обнаружения дефектов в программах и др.

владеть:

- навыками освоения большого объема информации;
- навыками самостоятельной работы в Интернете;
- культурой разработки и реализации системного программного обеспечения современных компьютеров;
- навыками грамотной разработки новых языков программирования и их программного обеспечения.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Базовые понятия криптографии. Связь с теорией чисел	5	5		10
2	Элементы теории сложности	5	5		10
3	Анализ сложности в среднем для дискретных задач	5	5		10
Итого часов		15	15		30
Подготовка к экзамену		30 час.			
Общая трудоёмкость		90 час., 2 зач.ед.			

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 8 (Весенний)

1. Базовые понятия криптографии. Связь с теорией чисел

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

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

Задача о рюкзаке. Предварительные сведения из теории решеток.

2. Элементы теории сложности

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

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

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

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

3. Анализ сложности в среднем для дискретных задач

Оценки сложности выполнения арифметических операций. Делимость и алгоритм Евклида.

Сложность решения систем линейных диофантовых уравнений.

Полиномиальный алгоритм проверки простоты чисел.

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

Приведенный базис в решетке. Алгоритм Ловаса.

Результаты Айтаи о сложности поиска короткого вектора в случайной решетке.

Некоторые криптосистемы на решетках.

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Необходимое оборудование для лекций и практических занятий: компьютер и мультимедийное оборудование (проектор, звуковая система).

6.Перечень рекомендуемой литературы

Основная литература

1. Эффективные алгоритмы и сложность вычислений/ Кузюрин Н.Н., Фомин С.А., Издательство МФТИ, 2007. - 313 с. ISBN 5-7417-0198-1.
2. З.И. Боревич, И.Р. Шафаревич, Теория чисел, Москва, Наука, 1985.
3. 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.

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

http://www.thefreecountry.com/programming/compilerconstruction.shtml, http://llvm.org/, http://gcc.gnu.org/, http://suif.stanford.edu/suif/suif2/

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

Программное обеспечение и информационные технологии не требуются.

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Студент, изучающий дисциплину, должен с одной стороны, овладеть общим понятийным аппаратом, а с другой стороны, должен научиться применять теоретические знания на практике.

В результате изучения дисциплины студент должен знать основные определения, понятия, аксиомы, алгоритмы.

Успешное освоение курса требует напряжённой самостоятельной работы студента. В программе курса приведено минимально необходимое время для работы студента над темой. Самостоятельная работа включает в себя:

– чтение и конспектирование рекомендованной литературы,

– проработку учебного материала (по конспектам лекций, учебной и научной литературе), подготовку ответов на вопросы, предназначенных для самостоятельного изучения, доказательство отдельных утверждений, свойств;

– подготовку к экзамену.

Руководство и контроль за самостоятельной работой студента осуществляется в форме индивидуальных консультаций.

Важно добиться понимания изучаемого материала, а не механического его запоминания. При затруднении изучения отдельных тем, вопросов, следует обращаться за консультациями к лектору.

ПРИЛОЖЕНИЕ

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению: Прикладные математика и физика
профиль подготовки: Радиотехника и компьютерные технологии
Физтех-школа Радиотехники и Компьютерных Технологий
кафедра системного программирования
курс: 4
квалификация: бакалавр

Семестр, формы промежуточной аттестации: 8 (весенний) - Экзамен

Разработчики:

А.В. Шокуров, канд. физ.-мат. наук, доцент
С.А. Фомин

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-2 Способен использовать современные информационные технологии и программные средства при решении задач профессиональной деятельности, соблюдая требования информационной безопасности	ОПК-2.1 Способен применять современные вычислительную технику и сервисы сети Интернет в области (сфере) профессиональной деятельности
ПК-3 Способен выбирать и применять подходящее оборудование, инструменты и методы исследований для решения задач в избранной предметной области	ПК-3.1 Знает принципы работы и диапазоны рабочих параметров используемого научного оборудования
ПК-4 Способен критически оценивать применимость используемых методик и методов	ПК-4.1 Знает численные порядки величин, характерных для соответствующей профессиональной области

2. Показатели оценивания компетенций

В результате изучения дисциплины «Решетки, алгоритмы и современные проблемы криптографии» обучающийся должен:

знать:

- связь общих вопросов теории чисел и алгебраической геометрии и криптографии;
- проблемы построения алгоритмов для решения задач теории чисел и алгебраической геометрии;
- основные методы анализа алгоритмической сложности задач из теории чисел и алгебраической геометрии.

уметь:

- разрабатывать, обосновывать и реализовывать новые методы и алгоритмы машинно-независимой оптимизации программ;
- разрабатывать и реализовывать новые языки и их оптимизирующие компиляторы для новых архитектур процессоров, в том числе специализированных;
- применять компиляторные методы и компиляторные среды для решения задач обратной инженерии, защиты программного кода, обнаружения дефектов в программах и др.

владеть:

- навыками освоения большого объема информации;
- навыками самостоятельной работы в Интернете;
- культурой разработки и реализации системного программного обеспечения современных компьютеров;
- навыками грамотной разработки новых языков программирования и их программного обеспечения.

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

С целью контроля освоения обучающимися учебного материала проводится устный опрос в начале занятия по теме прошлой лекции или в конце занятия по пройденной теме.

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

1. Пример: протокол Диффи-Хелмана. Определение односторонних функций. Криптосистемы с открытым ключом.
2. Необходимое условие стойкости криптосистем с открытым ключом – существование односторонних функций. Пример таких систем.
3. Криптосистема Эль-Гамаля. Дискретный логарифм. Сложность в наихудшем случае и в среднем. Теорема о сложности в среднем дискретного алгоритма, если имеется слож-ность в наихудшем случае.

4. Задача о рюкзаке. Связь с теорией решеток.

5. Определение решетки. Основной параллелепипед. Детерминант решетки. Полные ре-шетки. Критерий полноты решетки.

6. Дискретные абелевы группы и решетки.

7. Абелевы группы конечного и бесконечного порядка. Теорема о базисе конечно поро-жденной абелевой группы. Ранг абелевой группы.

8. Свойства базисов абелевых групп.

9. Лемма Минковского о выпуклом теле.

10. Неравенство Адамара. Вторая теорема Минковского. Следствие из теоремы Минков-ского об оценке длины кратчайшего вектора.

11. Делимость и алгоритм Евклида.

12. Полиномиальный алгоритм проверки простоты чисел

13. Алгоритм Гаусса. Сложность алгоритма Гаусса.

14. Задачи SVP и CVP.

15. LLL-алгоритм. Корректность.

16. LLL-алгоритм. полиномиальность.

17. Задача ACVP. Алгоритм решения ACVP.

18. Описание NTRU: алгебраическое и геометрическое.

Примерный перечень билетов:

Билет №1.

1. Необходимое условие стойкости криптосистем с открытым ключом – существование односторонних функций. Пример таких систем.

2. Определение решетки. Основной параллелепипед. Детерминант решетки. Полные ре-шетки. Критерий полноты решетки.

Билет №2.

1. Криптосистема Эль-Гамаля. Дискретный логарифм. Сложность в наихудшем случае и в среднем. Теорема о сложности в среднем дискретного алгоритма, если имеется слож-ность в наихудшем случае.

2. Дискретные абелевы группы и решетки.

Критерии оценивания

Оценка отлично 10 балов - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины, проявляющему интерес к данной предметной области, продемонстрировавшему умение уверенно и творчески применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично 9 балов - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично 8 балов - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, правильное обоснование принятых решений, с некоторыми недочетами.

Оценка хорошо 7 балов - выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но недостаточно грамотно обосновывает полученные результаты.

Оценка хорошо 6 балов - выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности.

Оценка хорошо 5 балов - выставляется студенту, если он в основном знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач достаточно большое количество неточностей.

Оценка удовлетворительно 4 бала - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он освоил основные разделы учебной программы, необходимые для дальнейшего обучения, и может применять полученные знания по образцу в стандартной ситуации.

Оценка удовлетворительно 3 бала - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, допускающему ошибки в формулировках базовых понятий, нарушения логической последовательности в изложении программного материала, слабо владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и с трудом применяет полученные знания даже в стандартной ситуации.

Оценка неудовлетворительно 2 бала - выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных принципов и не умеет использовать полученные знания при решении типовых задач.

Оценка неудовлетворительно 1 бал - выставляется студенту, который не знает основного содержания учебной программы дисциплины, допускает грубейшие ошибки в формулировках базовых понятий дисциплины и вообще не имеет навыков решения типовых практических задач.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Во время проведения экзамена обучающиеся могут пользоваться программой дисциплины, а также справочной литературой, вычислительной техникой, конспектами лекций.

Экзамен проводится путем организации специального опроса, проводимого в устной форме.