Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор
_____ А. В. Замятин
« 19 » мая 20 22 г.

Рабочая программа дисциплины

Теоретико-числовые методы в криптографии

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки / специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2022

Код дисциплины в учебном плане: Б1.В.04.01

СОГЛАСОВАНО:
Руководитель ОП
_____В.Н. Тренькаев

Председатель УМК
_____С.П. Сущенко

Томск – 2022

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

– ОПК-3 – Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

– ОПК-10 – Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

– ПК-2 – Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности.

ИОПК-3.3 Выявляет научную сущность проблем, возникающих в ходе профессиональной деятельности, и применяет соответствующий математический аппарат для их формализации, анализа и выработки решения.

ИОПК-10.1 Осуществляет анализ тенденций развития методов и средств криптографической защиты информации.

ИПК-2.2 Разрабатывает математические модели, реализуемые в средствах защиты информации.

2. Задачи освоения дисциплины

Обучить студентов алгоритмам над большими числами, над полиномами, методам генерации простых чисел, методам факторизации чисел и полиномов, задачам дискретного логарифмирования. Наряду с теоретическими основами, изучаются практические алгоритмы решения указанных задач. На лабораторных работах студенты реализуют, отлаживают и исследуют изучаемые алгоритмы. Именно это сочетание — теории и практики, математики и программирования — можно считать отличительной особенностью дисциплины.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений. Дисциплина входит в модуль "Специализация".

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Шестой семестр, экзамен
Седьмой семестр, экзамен

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Введение в математику, алгебра, теория чисел, языки программирования, методы программирования.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 9 з.е., 324 часов, из которых:
-лекции: 64 ч.
-лабораторные: 64 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

6 семестр

Тема 1. Алгоритмы работы с большими числами.

Рассматриваются дихотомический алгоритм возведения в степень, метод Барретта, преобразование Монтгомери, теорема об извлечении корня, вычисление НОД (бинарный алгоритм), быстрое умножение (метод Карацубы, метод Тоома - Кука), дискретное преобразование Фурье (определение, содержательный смысл, быстрое вычисление ДПФ), алгоритм Шёнхаге - Штрассена умножения целых чисел.

Тема 2. Тесты на простоту и методы генерации простых чисел.

Определение чисел Кармайкла, теорема Кармайкла, тест Соловея — Штрассена, тест Миллера — Рабина, метод Люка проверки числа на простоту, простые числа специального вида (Ферма, Мерсенна, сильные простые, надёжные простые), процедура генерации простого числа в Российском стандарте выработки ЭЦП, полиномиальный детерминированный тест на простоту.

7 семестр

Тема 3. Методы факторизации чисел.

Рассматриваются различные методы факторизации чисел. Метод пробных делений, метод Олвея, метод Ферма, методы Полларда, метод Диксона, метод квадратичного решета, метод цепных дробей, алгоритм решета числового поля.

Тема 4. Дискретное логарифмирование не в конечных циклических группах.

Рассматриваются различные методы дискретного логарифмирования: метод Полларда, алгоритм Адлемана, алгоритм Полита - Хеллмана.

Тема 5. Алгоритмы над полиномами: тесты на неприводимость, примитивность, факторизация полиномов.

Рассматриваются критерии неприводимости многочленов по простому модулю. Тест на примитивность многочленов. Также рассматривается факторизация многочленов методом освобождения от квадратов и алгоритм Берлекэмпа. Метод Кантора — Цассенхауза.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения контрольных работ, выполнения лабораторных работ и домашних заданий, и фиксируется в форме контрольной точки не менее одного раза в семестр.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Экзамен в седьмом семестре проводится в письменной форме по билетам. Экзаменационный билет состоит из трех частей. Продолжительность экзамена 1,5 часа.

Вопросы к экзамену

6 семестр

1. Дихотомический алгоритм возведения в степень

2. Алгоритм Барретта приведения чисел по модулю (с обоснованием)
3. Приведение по модулю специального вида
4. Преобразование Монтгомери
5. Произведение Монтгомери
6. Возведение в степень методом Монтгомери
7. Вычисление наибольшего общего делителя: бинарный алгоритм
8. Теорема о вычислении целой части квадратного корня
9. Быстрое умножение: метод Карацубы
10. Быстрое умножение: метод Тоома - Кука
11. Примитивные корни из 1, их свойства.
12. Теорема о матрице Вандермонда, её следствия
13. Теорема о примитивных корнях из 1
14. Дискретное преобразование Фурье: определение, содержательный смысл. Доказать обратимость ДПФ
15. Свертка. Теорема о свертке
16. Быстрое вычисление ДПФ: ключевые идеи
17. Алгоритм быстрого преобразования Фурье (с примером)
18. Определение чисел Кармайкла. Теорема Кармайкла
19. Определение и свойства оснований Ферма
20. Теорема о бесконечном количестве псевдопростых по любому основанию
21. Теорема о достаточности критерия Эйлера
22. Определение и свойства оснований Эйлера
23. Тест Соловея - Штрассена (с примером)
24. Теорема Селфриджа (о сильно псевдопростых числах)
2 5. Теорема Рабина
26. Тест Миллера - Рабина (с примером)
27. Пусть $n = 3 \pmod 4$. Доказать: R,, = E,,
28. Связь теста Миллера - Рабина с задачей факторизации
29. Метод Люка проверки числа на простоту (с примером)
30. Теорема Брилхарда — Лемера - Селфриджа (модификация критерия Люка)
31. Теорема Поклингтона, следствие её
32. Теорема Диемитко, следствие её
33. Процедура генерации простого числа в Российском стандарте выработки ЭЦП
34. Пусть $(a, n) = 1$. Доказать: n простое, если и только если $(x - a)^{n} = x^{n} — a \pmod n$
35. Полиномиальный детерминированный тест на простоту (AKS-тест)

7 семестр

1. Факторизация: метод пробных делений
2. Факторизация: метод Олвея
3. Факторизация: метод Ферма (с примером)
4. Факторизация: метод Ферма с просеиванием
5. Метод Флойда определения периода последовательности (с примером)
6. Факторизация: r-метод Полларда (с примером)
7. Факторизация: $(p - 1)$-метод Полларда (с примером)
8. Факторизация: метод Диксона (с примером)
9. Факторизация: метод квадратичного решета (с примером)
10. Метод квадратичного решета: этап просеивания (с примером)
11. Факторизация: метод цепных дробей (с примером)
12. Дискретное логарифмирование: r-метод Полларда (с примером)
13. Дискретное логарифмирование: алгоритм Адлемана (с примером)
14. Дискретное логарифмирование: алгоритм Полита - Хеллмана (с примером)
15. Критерии неприводимости многочленов по простому модулю
16. Тесты неприводимости многочленов (с примерами)

17. Тест на примитивность многочленов
18. Возвратные многочлены. Доказать: /(x) примитивный, если и только если/*(x) 19. примитивный
19. Факторизация многочленов: освобождение от квадратов
20. Теоремы Берлекэмла
21. Факторизация многочленов: алгоритм Берлекэмла
22. Метод Кантора — Цассенхауза: разложение полинома на делители с неприводимыми множителями одинаковой степени
23. Метод Кантора — Цассенхауза: второй этап, случай $p > 2$
24. Метод Кантора — Цассенхауза: второй этап, случай $p = 2$
25. Метод решета числового поля факторизации целых чисел (с примером для и ^{1} 65)

Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Темы лабораторных работ:

1. Алгоритмы возведения в степень
2. Методы приведения по модулю
3. Быстрые алгоритмы умножения чисел
4. Тесты на простоту: Ферма, Соловея — Штрассена, Миллера — Рабина
5. Методы генерации простых, надёжных простых и сильных простых чисел
6. Методы факторизации: пробных делений, Олвея, Ферма, решета, Полларда, методы случайных квадратов
7. Методы дискретного логарифмирования: Гельфонда, Полларда, Адлемана, Полита — Хеллмана
8. Проверка полиномов на неприводимость
9. Проверка полиномов на примитивность

Контрольные работы:

1. Методы умножения Карацубы и Тоома — Кука
2. Дискретное преобразование Фурье
3. Дискретное логарифмирование: методы Полита — Хеллмана, Полларда, Адлемана
4. Алгоритмы над полиномами: освобождение от квадратов, факторизация методом Берлекэмпа, проверта на примитивность

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle»

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине (Приложение 1).

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М.: Мир, 1979.

– Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2002.

– Кнут Д. Искусство программирования для ЭВМ. Том 2. Получисленные алгоритмы. М.: Мир, 1977.

– Черёмушкин А.В. Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002.

– Панкратова ИА. Теоретико-числовые задачи в криптографии. Томск: РИО ТГУ, 2010.

– Панкратова И.А. Теоретико-числовые методы в криптографии. Томск: РИО ТГУ, 2009.

б) дополнительная литература:

– Фергюсон Н., Шнайер Б. Практическая криптография. М.-С.-Пб.-Киев: Диалектика, 2005.

– Харин Ю.С., Берник В.И, Матвеев Г.В., Агиевин С.В. Математические и компьютерные основы криптологии. Минск: Новое знание, 2003.

в) ресурсы сети Интернет:

– Общероссийская Сеть КонсультантПлюс Справочная правовая система. http://www.consultant.ru

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook);

– публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system

– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index

– ЭБС Лань – http://e.lanbook.com/

– ЭБС Консультант студента – http://www.studentlibrary.ru/

– Образовательная платформа Юрайт – https://urait.ru/

– ЭБС ZNANIUM.com – https://znanium.com/

– ЭБС IPRbooks – http://www.iprbookshop.ru/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

Останин Сергей Александрович, заведующий кафедрой компьютерной безопасности, канд. техн. наук, доцент.