Программа дисциплины: Теоретико-числовые методы в криптографии

Утверждена
Кафедрой компьютерной
безопасности МИЭМ НИУ ВШЭ
Протокол № 3 от 24.10.2018 г

Автор	Нестеренко А.Ю.
Число кредитов	3
Контактная работа (час.)	52
Самостоятельная работа (час.)	62
Курс	4 курс 3,4 модуль
Формат изучения дисциплины	Без использования онлайн курса

I. ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ

Целью освоения дисциплины является формирование у студентов следующих навыков, необходимых для решения предусмотренных программой специальности 10.05.01 «Компьютерная безопасность» профессиональных задач:

- разработка математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность;
- обоснование и выбор рационального решения по уровню обеспечения защищенности компьютерной системы с учетом заданных требований;
- подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований;
- выполнение экспериментально-исследовательских работ при проведении сертификации средств защиты и анализ результатов;
- проведение аттестации технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности или профилям защиты.

В результате освоения дисциплины студент должен знать:

- методы нахождения корней многочленов над конечными полями;
- алгоритмы построения простых чисел;
- алгоритмы проверки больших целых чисел на простоту;
- алгоритмы факторизации больших целых чисел;
- методы дискретного логарифмирования в циклических группах;

В результате освоения дисциплины студент должен уметь:

- доказывать простоту больших целых чисел;
- строить простые числа заданного размера;
- решать задачу разложения больших целых чисел на множители;
- решать задачу дискретного логарифмирования.

В результате освоения дисциплины студент должен иметь навыки (приобрести опыт):

- вычисления символа Лежандра;
- нахождения корней многочленов над конечным простым полем;
- построения простых чисел заданного размера;
- разложения чисел на множители и вычисления дискретных логарифмов в мультипликативной группе конечного простого поля.

Для освоения учебной дисциплины, студенты должны владеть следующими знаниями:
- знанием школьной программы;
- основными понятиями алгебры, теории конечных групп, колец и полей;
- основными понятиями элементарной теории чисел.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин:
- криптографические методы защиты информации;
- криптографические протоколы;
- методы алгебраической геометрии в криптографии,
а также при написании итоговой выпускной квалификационной (дипломной) работы.

II. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Основные положения:
- «Теоретико-числовые методы в криптографии» читается на протяжение двух модулей весеннего семестра (третий и четвертый модуль) для студентов четвертого курса;
- дисциплина состоит из лекций и практических занятий, а также двух контрольно-проверочных работ, направленных на оттачивание навыков по решению теоретико-числовых задач;
- дисциплина состоит из четырех крупных фрагментов: методы поиска корней многочленов над конечными полями,
- вопросы доказательства простоты чисел, факторизация целых чисел и решение задачи дискретного логарифмирования;

Третий модуль

Тема 1. Сведения из элементарной теории чисел: наибольший общий делитель, алгоритм Эвклида вычисления НОД и его модификации, бесконечность множества простых чисел, основная теорема арифметики.

Тема 2. Сравнения первой степени. Китайская теорема об остатках. Функция Эйлера. Показатели и первообразные корни. Теоремы о существовании и количестве первообразных корней. Алгоритмы построения первообразных корней.

Тема 3. Теория и свойства многочленов от одной переменной, лемма Безу, основная теорема арифметики для многочленов. Дифференцирование

многочленов. Решение полиномиальных сравнений по составному модулю -- сведение решений в конечных кольцах к случаю конечного простого поля. Метод подъема решения.

Тема 4. Сравнения старших степеней по простому модулю. Квадратичные вычеты. Символы Лежандра и Якоби. Алгоритмы вычисления символа Лежандра.

Тема 5. Вычисление корней второй степени. Алгоритм Тонелли-Шенкса вычисления квадратных корней по простому модулю. Алгоритм, основанный на квадратичных расширениях конечного простого поля.

Тема 6. Методы вычисления корней третьей степени. Элементы теории двучленных сравнений. Вероятностный алгоритм вычисления корней многочленов старших степеней.

Тема 7. Простые числа. Бесконечность множества простых чисел. Методы построения таблиц простых чисел.

Тема 8. Вероятностные тесты проверки на простоту: числа Кармайкла, тест Соловея-Штрассена и тест Милера-Рабина.

Четвертый модуль

Тема 1. Алгоритмы доказательства простоты чисел с использованием разложения n-1 на простые множители (теоремы Лемера и Поклингтона).

Тема 2. Алгоритмы доказательства простоты чисел с использованием разложения n+1 на простые множители (теорема Морисона).

Тема 3. Рассмотрение обобщения указанных алгоритмов. Алгоритмы построения строго простых чисел.

Тема 4. Полиномиальный алгоритм доказательства простоты.

Тема 5. Цепные дроби. Понятие подходящей дроби. Квадратичные иррациональности и их разложения в цепные дроби. Наилучшие приближения действительных чисел.

Тема 6. Экспоненциальные методы факторизации целых чисел. Метод Ферма, методы Полларда-Флойда и Брента. p-1 метод Полларада, p+1 метод Вильямса. Методы оптимизации рассмотренных алгоритмов.

Тема 7. Решето Крайчика. Метод непрерывных дробей (Лемера), метод Моррисона-Бриллхарда, метод квадратичного решета и его дальнейшие модификации.

Тема 8. Алгоритмы вычисления индексов (решения задачи дискретного логарифмирования): метод согласования, методы Нечаева и Поллига-Хеллмана. Методы, основанные на поиске длин циклов в последовательностях: методы Полларда, Госпера, а также параллельный метод Винера.

Тема 9. Индекс методы решения задачи дискретного логарифмирования. Решение систем линейных уравнений в кольцах вычетов. Индекс-метод Адлемана и его модификации.

III. ОЦЕНИВАНИЕ

Формы контроля:

Тип	Форма контроля	4 курс	Приме

контроля		1 модуль	2 модуль	3 модуль	4 модуль	чания
Текущий	Контрольная работа			*	*	
Итоговый	Экзамен в устной форме				*	

Контроль знаний производится по окончании третьего и четвертого модулей. По окончании каждого из модулей проводится контрольная работа с целью обретения навыков практического решения теоретико-числовых задач.

По окончании четвертого модуля проводится устный экзамен с целью проверки усвоения теоретических знаний. В ходе устного экзамена студенту предлагается выбрать билет, содержащий два теоретических вопроса из перечня, приведенного ранее. В случае успешного ответа на вопросы из билета, студенту могут быть заданы дополнительные вопросы (не более четырех), позволяющие оценить степень его знаний по дисциплине.
Максимальная оценка за экзамен: 10 баллов.

При сдаче экзамена студентам запрещается пользоваться печатной литературой, а также специальными вычислительными средствами и программами, и программ, а также сетью Интернет.

Порядок формирования оценок по дисциплине

В ходе проведения контрольных работ студент получает баллы, формирующие накопленную оценку Q1. На каждой из контрольных работ максимальное число баллов составляет пять. Накопленная оценка является суммой баллов за контрольные работы.
Накопленная оценка учитывается при проведении экзамена.

Итоговая оценка Q по предмету определяется из соотношения 0.5Q1+0.5Q2, где Q1 накопленная оценка за две контрольные работы, Q2 оценка, полученная на устном экзамене. Округление происходит в большую сторону, например, величина Q = 3,5 дает студенту 4 балла.

В случае, если студент не может получить положительную оценку Q по предмету (4 и более балов) назначается пересдача. В ходе пересдачи студент должен решить поставленную перед ним практическую задачу и успешно ответить на теоретический вопрос. В случае неуспешной пересдачи назначается комиссия.

IV. РЕСУРСЫ

1. Основная литература

Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации: учебник для академического бакалавриата. Изд. 2-е, испр. М.: изд. Юрайт, 2016. – 473 с

2. Дополнительная литература

Нестеренко А.Ю. Теоретико-числовые методы в криптографии. М.: МИЭМ, 2012

3. Программное обеспечение

Не требуется.

4. Профессиональные базы данных, информационные справочные системы, интернет-ресурсы (электронные образовательные ресурсы)

№	Наименование	Условия доступа
1.	Вузовская электронно-библиотечная система учебной литературы	URL: http://miem.hse.ru/
2.	База научно-технической информации (ВИНИТИ РАН)	URL: http://www.vniti.com/

5. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине обеспечивают использование и демонстрацию тематических иллюстраций, соответствующих программе дисциплины в составе:

- ПЭВМ с доступом в Интернет (операционная система, офисные программы, антивирусные программы);

- мультимедийный проектор с дистанционным управлением.