Список литературы

1 Теоретические основы электротехники : в 3 т. / К.С. Демирчан [и др.]. – 4-е изд. – СПб. : Питер, 2006.

2 **Аполлонский, С.М.** Дифференциальные уравнения математической физики в электротехнике / С.М. Аполлонский. – СПб. : Питер, 2012. – 352 с.

3 **Иоссель, Ю.Я.** Расчет потенциальных полей в энергетике / Ю.Я. Иоссель. – Л. : Энергия, 1978. – 351 с.

УДК 378.147:512.5

О ПРЕПОДАВАНИИ ДИСЦИПЛИНЫ «МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ»

Е.И. ЛОВЕНЕЦКАЯ

Белорусский государственный технологический университет, г. Минск

Современный этап развития криптографии, начавшийся после публикации в 1976 г. У. Диффи и М. Хеллманом концепции асимметричного шифрования, характеризуется широким использованием теоретико-числовых и алгебраических понятий и алгоритмов и интенсивным вовлечением в практику новых математических объектов и теорий. Это приводит к необходимости введения в программы подготовки студентов IT-профиля дисциплин, включающих основы теории чисел, модулярной арифметики, алгебраических структур. Так, в Белорусском государственном технологическом университете (БГТУ) для студентов специальности «Программное обеспечение информационной безопасности мобильных систем» предусмотрен курс «Математические основы криптографии», обеспечивающий математическую базу для изучения дисциплины «Криптографические методы защиты информации». Основными задачами изучения курса «Математические основы криптографии» являются формирование у студентов представления о теоретических основах построения надежных криптографических преобразований и развитие умения пользоваться классическими и современными алгебраическими и теоретико-числовыми понятиями, методами, алгоритмами, поскольку даже простая реализация современных криптографических алгоритмов требует достаточно глубокого понимания основ теории чисел и алгебраических структур.

Содержание курса «Математические основы криптографии» включает модулярную арифметику как базу для понимания важнейших алгебраических структур и классического алгоритма передачи ключей Диффи – Хеллмана, понятие о проблеме факторизации целых чисел, лежащей в основе криптосистемы RSA, расширенный алгоритм Евклида, который не только остается в классе самых быстрых инструментов нахождения НОД целых

чисел, поиска обратных классов вычетов, но и применим в кольцах многочленов над конечными полями. Вторая часть курса посвящена знакомству с алгебраическими структурами: группами, кольцами, полями, вопросу построения конечных полей как факторколец, колец многочленов над простыми полями, а также представления элементов конечных полей с помощью примитивного элемента, порождающего мультипликативную группу поля. Аналогия между примитивным элементом конечного поля и первообразным корнем по модулю целого числа позволяет наглядно продемонстрировать принципы построения криптосистем над конечными полями на примере классических криптографических алгоритмов, основанных на действиях над классами вычетов. Заключительная часть курса посвящена описанию построения групп точек эллиптических кривых над конечными полями, что позволяет обсудить алгоритмы эллиптической криптографии, которые обладают более высокой стойкостью по сравнению с их числовыми аналогами и уже широко используются в государственных и международных стандартах по информационной безопасности, в том числе и в Республике Беларусь.

Включение в программу дисциплины наряду с классическими областями алгебры и теории чисел такого современного раздела, как теория эллиптических кривых, необходимость иллюстрации практического применения алгебраических объектов в криптографических схемах и формирования представления о проблеме разработки эффективных теоретико-числовых и криптографических алгоритмов приводят к вопросу создания качественного методического обеспечения дисциплины, позволяющего не только осветить основные понятия, используемые на практике в настоящее время, но и заложить базу для понимания новых результатов и методов в области защиты информации.

Анализ имеющейся литературы и доступных интернет-источников показал, что в большинстве высших учебных заведений, готовящих специалистов IT-профиля, в программы обучения студентов включаются в том или ином виде курсы защиты информации и криптографии, ведется активная работа по созданию учебных пособий, посвященных тем или иным аспектам математических основ криптографии. Назовем несколько учебно-методических пособий, отражающих содержание курсов, которые читаются в технических университетах.

Краткий обзор начнем с работы [1], в которой представлен материал, необходимый для начального введения в теорию криптографических алгоритмов: теория групп, колец и полей, а также прикладная теория чисел. В [2] рассмотрены вопросы стойкости криптографических систем и алгоритмов, элементы теории чисел и теории конечных полей, обсуждаются понятия односторонней функции и хэш-функции, дана общая характеристика различных типов шифров и классов криптосистем. Достаточно краткое, но полное и строгое изложение алгебраических основ теории и практики обработки дискретных сигналов и защиты информации, включая описание теории полей Галуа, приведено в [3].

В пособии [4], помимо указанных выше вопросов, освещаются некоторые аспекты криптографических алгоритмов с использованием эллиптических кривых. Заслуживает внимания также пособие [5], в котором достаточно полно и доступно изложены материалы по основным алгебраическим структурам, модулярной арифметике, полям Галуа, эллиптическим кривым, дано представление о криптосистемах, основанных на модулярной арифметике, и о квантовой криптографии.

Более широкий охват материала представлен в учебниках [6] и [7], которые также весьма полезны при подготовке курсов по математическим основам криптографии. Описание большого количества теоретико-числовых алгоритмов с обоснованием их корректности и оценками трудоемкости можно найти в монографии [8] и более доступных для понимания книгах [9] и [10]. Актуальным вопросам алгоритмической теории чисел посвящена также прекрасно написанная книга [11].

Для введения в теорию эллиптических кривых могут быть использованы книги [12] и [13], посвященные изложению элементов теории эллиптических кривых и их применения в теоретико-числовых и криптографических алгоритмах. Отметим, что в [7], [8], [10], [11] также уделяется внимание вопросам использования эллиптических кривых в криптографии.

Таков краткий перечень наиболее доступных источников, который может быть использован для построения курса по теоретико-числовым и алгебраическим основам криптографии в техническом вузе.

Для методической поддержки дисциплины «Математические основы криптографии» в БГТУ был издан конспект лекций [14] и подготовлен электронный учебно-методический комплекс (ЭУМК) [15], который представляет собой единый pdf-документ, доступный студентам через систему дистанционного обучения (СДО) БГТУ. На наш взгляд, основной функцией дистанционных курсов, включаемых как часть традиционных учебных курсов, является предоставление студентам хорошо структурированной тщательно отобранной информации, необходимой и достаточной для изучения соответствующей дисциплины. ЭУМК обеспечивает студентов как теоретическим материалом, так и набором заданий для проведения практических занятий и самостоятельного решения. Задачи для решения в аудитории подобраны так, чтобы студенты могли освоить основные понятия курса и получить представление о свойствах и способах оперирования с изучаемыми математическими объектами. Для закрепления материала, а отчасти в силу приученности студентов IT-специальностей к работе в режиме выполнения индивидуальных проектов, сформирован комплекс индивидуальных заданий по основным прикладным темам, по которым каждый студент должен отчитаться для получения зачета.

Курс «Математические основы криптографии» обеспечивает знакомство студентов с теоретико-числовыми и алгебраическими структурами, вовлеченными в практику современной криптографии, а также закладывает фун-

дамент для изучения более сложных объектов, которые могут послужить основой для построения криптографических систем в будущем. Необходимым следствием динамичного развития криптографических методов защиты информации должно быть столь же динамичное изменение программы и содержания курса по математическим основам криптографии, чему способствует представление ЭУМК в СДО, где имеется возможность оперативно вносить изменения в размещенные материалы.

Список литературы

1 **Коробейников, А.Г.** Математические основы криптографии : учеб. пособие / А.Г. Коробейников. – СПб. : С.-Петерб. гос. ин-т точной механики и оптики (технич. ун-т), 2002. – 41 с.

2 **Галуев, Г.А.** Математические основы криптологии : учеб.-метод. пособие / Г.А. Галуев. – Таганрог : Изд-во ТРТУ, 2003. – 120 с.

3 **Липницкий, В.А.** Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа : учеб.-метод. пособие по курсу «Высшая математика» для студ. спец. «Сети телекоммуникаций» и «Информатика» всех форм обуч. / В.А. Липницкий. – 2-е изд., испр. – Минск : БГУИР, 2006. – 88 с.

4 **Воронков, Б.Н.** Элементы теории чисел и криптозащита : учеб. пособие / Б.Н. Воронков, А.С. Щеголеватых. – Воронеж : ВГУ, 2008. – 88 с.

5 **Данилова, О.Ю.** Математические основы криптографии : учеб. / О.Ю. Данилова, В.Н. Думачев. – Воронеж : Воронежский ин-т МВД России, 2017. – 300 с.

6 **Нестеренко, А.Ю.** Теоретико-числовые методы в криптографии : учеб пособие / А.Ю. Нестеренко. – М. : Моск. гос. ин-т электроники и математики, 2012. – 224 с.

7 Криптология : учеб. / Ю.С. Харин [и др.]. – Минск : БГУ, 2013. – 511 с.

8 **Василенко, О.Н.** Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М. : МЦНМО, 2003. – 328 с.

9 **Черемушкин, А.В.** Лекции по арифметическим алгоритмам в криптографии / А.В. Черемушкин. – М. : МЦНМО, 2002. – 104 с.

10 **Ишмухаметов, Ш.Т.** Методы факторизации натуральных чисел : учеб. пособие / Ш.Т. Ишмухаметов. – Казань : Казан. ун-т, 2011. – 190 с.

11 **Крэндалл, Р.** Простые числа: криптографические и вычислительные аспекты / Р. Крэндалл, К. Померанс ; пер. с англ.; под ред. и с предисл. В.Н. Чубарикова. – М. : УРСС: ЛИБРОКОМ, 2011. – 664 с.

12 Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы / А.А. Болотов [и др.] – М. : КомКнига, 2006. – 328 с.

13 Эллиптические кривые и современные алгоритмы теории чисел / Ю.П. Соловьев [и др.]. – М. – Ижевск : Институт компьютерных исследований, 2003. – 192 с.

14 Математические основы криптографии: тексты лекций для студентов специальности 1-98 01 03 Программное обеспечение информационной безопасности мобильных систем / авт.-сост. Е.И. Ловенецкая. – Минск : БГТУ, 2019. – 170 с.

15 ЭУМК по учебной дисциплине «Математические основы криптографии» для специальности 1-98 01 03 Программное обеспечение информационной безопасности мобильных систем / И.К. Асмыкович, Е.И. Ловенецкая [Электронный ресурс]. – Режим доступа : https://dist.belstu.by/course/view.php?id=314. – Дата доступа : 27.02.2022.