Б. Я. РЯБКО
А. Н. ФИОНОВ

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

2-е издание, стереотипное

Рекомендовано УМО по образованию в области телекоммуникаций в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям: «Многоканальные телекоммуникационные системы», «Радиосвязь, радиовещание и телевидение», «Защищенные системы связи»

Москва
Горячая линия — Телеком
2012

Рецензент: доктор техн. наук, профессор М. Д. Венедиктов

Рябко Б. Я., Фионов А. Н.

Р 98 Криптографические методы защиты информации: Учебное пособие для вузов. – 2-е издание, стереотип. – М.: Горячая линия–Телеком, 2012. – 229 с.: ил.

ISBN 978-5-9912-0286-2.

Изложены основные подходы и методы современной криптографии для решения задач, возникающих при обработке, хранении и передаче информации. Основное внимание уделено новым направлениям криптографии, связанным с обеспечением конфиденциальности взаимодействий пользователей компьютеров и компьютерных сетей. Рассмотрены основные шифры с открытыми ключами, методы цифровой подписи, основные криптографические протоколы, блоковые и потоковые шифры, криптографические хеш-функции, а также редко встречающиеся в литературе вопросы о конструкции доказуемо невскрываемых криптосистем и криптографии на эллиптических кривых. Изложение теоретического материала ведется достаточно строго, но с использованием элементарного математического аппарата. Подробно описаны алгоритмы, лежащие в основе криптографических отечественных и международных стандартов. Приведены задачи и упражнения, необходимые при проведении практических занятий и лабораторных работ.

Для студентов, обучающихся по направлению «Телекоммуникации», будет полезна специалистам.

32.801.4

Адрес издательства в Интернет www.techbook.ru

Учебное издание

Рябко Борис Яковлевич
Фионов Андрей Николаевич

Криптографические методы защиты информации

Учебное пособие

Обложка художника В. Г. Ситникова

Подписано в печать 05.06.2012. Формат 60×90/16. Уч.-изд. л. 14,5. Тираж 500 экз. (1-й завод 200 экз.) Изд. № 120286

ISBN 978-5-9912-0286-2

ПРЕДИСЛОВИЕ

В течение многих столетий криптография, т.е. наука о шифровании, или «закрытии» информации от несанкционированного использования, применялась в основном для защиты сообщений, которыми обменивались государственные чиновники или военные. Поэтому круг людей, применявших криптографию, был весьма ограничен, а сами методы этой науки секретны. Однако в последние десятилетия, когда человечество вступило в стадию информационного общества, криптографические методы защиты информации стали использоваться очень широко, обслуживая, в первую очередь, потребности бизнеса. Причем имеются в виду не только межбанковские расчеты по компьютерным сетям или, скажем, биржи, в которых все расчеты проводятся через Интернет, но и многочисленные операции, в которых ежедневно участвуют миллионы, если не миллиарды «обычных» людей, а именно: расчеты по кредитным карточкам, перевод заработной платы в банк, заказ билетов через Интернет, покупки в Интернет-магазинах и т.д., и т.п. Естественно, все эти операции, как и, скажем, разговоры по мобильным телефонам и электронная почта, должны быть защищены от нечестных или просто чрезмерно любопытных людей и организаций. Поэтому в наши дни в разработку и эксплуатацию систем защиты информации вовлечено множество специалистов, работающих в сфере информационных технологий. Так как многие из таких методов основываются на результатах современной криптографии, то теперь эта дисциплина преподается на факультетах университетов, готовящих специалистов по информационным технологиям.

Предлагаемое учебное пособие в значительной степени базируется на курсе лекций, который профессор Б. Я. Рябко читал сначала аспирантам, а затем студентам Сибирского государственного университета телекоммуникаций и информатики, обучавшимся по специальностям, связанным с программированием и компьютерными сетями, и для которых курс «Защита информации» является обязательным. Как можно заключить из названия, эта книга предна-

значена для студентов и инженеров, специализирующихся в области информационных технологий, поэтому она рассчитана на людей со знанием математики в объеме, даваемом в технических вузах. Все необходимые сведения из теории чисел и теории вероятностей приводятся в книге, причем не в виде отдельных разделов, а по мере необходимости. Такой стиль позволяет поддерживать интерес студентов на лекциях и, как мы надеемся, поможет и читателям книги.

При изложении материала мы старались следовать принципу А. Эйнштейна «Все должно делаться настолько просто, насколько это возможно, но не проще» и соблюдать правило «...Кратко и подробно», сформулированное одним из героев известной поэмы А. Твардовского. Поэтому мы не пытались описать всю современную криптографию на строгом математическом уровне и во всей общности, но, как нам кажется, рассмотрели основные идеи и методы криптографии, применяемые в информационных технологиях, как мы надеемся, без их вульгаризации. При этом, хотя главный упор в книге делается на объяснение основных идей и принципов, в ней содержится также точное описание целого ряда практически используемых методов, в том числе и российских ГОСТов на криптографические алгоритмы.

Содержание первых пяти глав может быть основой семестрового курса. Другие главы могут быть использованы при чтении спецкурсов. Наш опыт показывает, что усвоению материала помогают практические занятия и лабораторные работы в компьютерных классах, в ходе которых студенты реализуют все основные алгоритмы из указанных глав. Поэтому пособие содержит снабженные ответами задачи и темы лабораторных работ.

Мы надеемся, что это учебное пособие поможет читателям не только понять основные задачи и методы современной криптографии, но и оценить красоту и изящество ее идей и результатов.

ОГЛАВЛЕНИЕ

Предисловие **3**

1. Введение **5**
Задачи и упражнения 11

2. Криптосистемы с открытым ключом **12**
2.1. Предыстория и основные идеи 12
2.2. Первая система с открытым ключом — система Диффи–Хеллмана 18
2.3. Элементы теории чисел 21
2.4. Шифр Шамира 28
2.5. Шифр Эль-Гамаля 31
2.6. Односторонняя функция с «лазейкой» и шифр RSA . . 34
Задачи и упражнения 38
Темы лабораторных работ 40

3. Методы взлома шифров, основанных на дискретном логарифмировании **41**
3.1. Постановка задачи 41
3.2. Метод «шаг младенца, шаг великана» 43
3.3. Алгоритм исчисления порядка 45
Задачи и упражнения 50
Темы лабораторных работ 51

4. Электронная, или цифровая подпись **52**
4.1. Электронная подпись RSA 52
4.2. Электронная подпись на базе шифра Эль-Гамаля . . . 55
4.3. Стандарты на электронную (цифровую) подпись 58
Задачи и упражнения 62
Темы лабораторных работ 64

5. Криптографические протоколы 65
5.1. Ментальный покер 65
5.2. Доказательства с нулевым знанием 70
Задача о раскраске графа 71
Задача о нахождении гамильтонова цикла в графе . . . 75
5.3. Электронные деньги 82
5.4. Взаимная идентификация с установлением ключа 88
Задачи и упражнения 95
Темы лабораторных работ 96

6. Криптосистемы на эллиптических кривых 97
6.1. Введение 97
6.2. Математические основы 98
6.3. Выбор параметров кривой 106
6.4. Построение криптосистем 108
Шифр Эль-Гамаля на эллиптической кривой 109
Цифровая подпись по ГОСТ Р34.10-2001 110
6.5. Эффективная реализация операций 111
6.6. Определение количества точек на кривой 117
6.7. Использование стандартных кривых 126
Задачи и упражнения 129
Темы лабораторных работ 129

7. Теоретическая стойкость криптосистем 131
7.1. Введение 131
7.2. Теория систем с совершенной секретностью 132
7.3. Шифр Вернама 134
7.4. Элементы теории информации 135
7.5. Расстояние единственности шифра с секретным ключом 142
7.6. Идеальные криптосистемы 148
Задачи и упражнения 154

8. Современные шифры с секретным ключом 156
8.1. Введение 156
8.2. Блоковые шифры 159
Шифр ГОСТ 28147-89 161
Шифр RC6 164
Шифр Rijndael (AES) 167

8.3. Основные режимы функционирования блоковых шифров . . . 177
Режим ECB . . . 177
Режим CBC . . . 178
8.4. Потоковые шифры . . . 179
Режим OFB блокового шифра . . . 181
Режим CTR блокового шифра . . . 182
Алгоритм RC4 . . . 183
8.5. Криптографические хеш-функции . . . 185

9. Случайные числа в криптографии . . . 188
9.1. Введение . . . 188
9.2. Задачи, возникающие при использовании физических генераторов случайных чисел . . . 190
9.3. Генераторы псевдослучайных чисел . . . 192
9.4. Тесты для проверки генераторов случайных и псевдослучайных чисел . . . 195
9.5. Статистическая атака на блоковые шифры . . . 200

Ответы к задачам и упражнениям . . . 214

Список литературы . . . 218

Предметный указатель . . . 222

Учебное издание

Борис Яковлевич **Рябко**
Андрей Николаевич **Фионов**

Криптографические методы защиты информации

Учебное пособие