Б. Я. Рябко, А. Н. Фионов

ОСНОВЫ СОВРЕМЕННОЙ КРИПТОГРАФИИ И СТЕГАНОГРАФИИ

Москва
Горячая линия–Телеком
2010

ŋqdqɐǝ⅄ ɓɆ ɗǝdɆɓ⅄зǝ ɗ ɕɔɑɓɔɐ Ɉqdd⅄qɐè

УДК 621.391
ББК 32.801.4
Р98

Рябко Б. Я., Фионов А. Н.

Р98 Основы современной криптографии и стеганографии. – М.: Горячая линия – Телеком, 2010. – 232 с.: ил.

ISBN 978-5-9912-0150-6.

В монографии изложены основные подходы и методы современной криптографии и стеганографии для решения задач, возникающих при обработке, хранении и передаче информации. 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. Рассмотрены вопросы, связанные с использованием случайных и псевдослучайных чисел в системах защиты информации. Приведено описание основных идей и методов современной стеганографии. Подробно описаны алгоритмы, лежащие в основе криптографических отечественных и международных стандартов. Многие из приведенных в книге результатов исследований, полученных авторами в последние годы, признаны специалистами в России и за рубежом.

Для исследователей и специалистов, работающих в области защиты информации, будет полезна для аспирантов и студентов.

ББК 32.801.4

Научное издание

Рябко Борис Яковлевич
Фионов Андрей Николаевич
Основы современной криптографии и стеганографии

Подписано в печать 30.08.10. Печать офсетная. Формат 60×90/16. Уч. изд. л. 14,5.
Тираж 1000 экз. (1-й завод 500 экз.)
ООО «Научно-техническое издательство «Горячая линия–Телеком»

ISBN 978-5-9912-0150-6

Электронный архив библиотеки МГТУ им. Н.Э. Баумана

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.

Стеганография, как и криптография, возникла в глубокой древности, но ее расцвет наступил вместе с появлением современных информационных технологий. Методы стеганографии предназначены для передачи сообщений таким образом, что сам факт передачи информации остается скрыт от наблюдателей. Например, в открыто передаваемую цифровую фотографию может быть «спрятано» несколько килобайт текста, который извлекается получателем при помощи специальных алгоритмов. Важно то, что при этом человек не замечает каких-либо искажений в фотографии, содержащей спрятанный текст. В настоящее время методы стеганографии нашли самое широкое применение в системах защиты авторских прав: вла-

дельцы цифровых фильмов, фотографий, музыкальных произведений и других данных встраивают туда скрытые метки, что позволяет по «пиратской» копии определить нарушителя авторских прав.

Эта книга предназначена для исследователей и специалистов по защите информации, но будет полезна аспирантам и студентам, специализирующихся в области информационных технологий. Все необходимые сведения из теории чисел и теории вероятностей приводятся в книге, причем не в виде отдельных разделов, а по мере необходимости. Такой стиль, как мы надеемся, поможет 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 и стеганографию на строгом математическом уровне и во всей общности, но, как нам кажется, рассмотрели основные идеи и методы, как мы надеемся, без их вульгаризации. При этом, хотя главное внимание в книге уделяется объяснению основных идей и принципов, в ней содержится также точное описание целого ряда практически используемых методов, в том числе и российских стандартов на криптографические алгоритмы.

Мы надеемся, что эта книга поможет читателям не только понять основные задачи и методы современной криптографии и стеганографии, но и оценить красоту и изящество идей и результатов, лежащих в основе этих наук.

ОГЛАВЛЕНИЕ