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.