Глава 1
Введение

> Я с детства был вскормлен науками, и так как меня уверили, что с их помощью можно приобрести ясное и надежное познание всего полезного для жизни, то у меня было чрезвычайно большое желание изучить эти науки. Но как только я окончил курс учения, завершаемый обычно принятием в ряды ученых, я совершенно переменил свое мнение, ибо так запутался в сомнениях и заблуждениях, что, казалось, своими стараниями в учении достиг лишь одного: все более и более убеждался в своем незнании.
>
> *Рене Декарт.*
> *Рассуждение о методе, чтобы верно направлять свой разум и отыскивать истину в науках*

Криптография сегодня — это уже целая отрасль знаний, захватывающая огромные разделы других наук, целью которой является изучение и создание криптографических преобразований и алгоритмов. В настоящее время четко различаются две ветви развития криптографии: классическая традиционная криптография и современная «асимметричная» криптография.

Речь в книге идет о классической традиционной криптографии, о симметричных криптосистемах, блочных и поточных шифрах. Прочтя книгу, читатель сможет свободно ориентироваться в классических схемах шифрования и криптоанализа, существующих архитектурах построения блочных и поточных шифров, а также в современных и перспективных методах их анализа.

Авторы надеются, что данная книга совместно с другими книгами по рассматриваемой теме, более отдаленными от практической стороны криптографии и несущими больше теоретической информации, послужит хорошим учебным и справочным пособием по реализации и верификации программного обеспечения шифрования данных.

Дополнительно к книге прилагается CD-ROM с проиндексированным содержанием. Список всех файлов с исходными текстами, упоминание о которых можно найти в книге, находится чуть ниже вместе с краткими их описаниями.

Структура глав, или Как читать эту книгу

Книга, которую вы держите в своих руках, насыщена довольно разнообразным материалом. К сожалению, нет простых путей в изучении сложных вещей. По этой причине главы и разделы этой книги, возможно, придется читать в разном порядке — в зависимости от подготовки и уровня знаний читателя. Сейчас, в самом ее начале, неплохо сделать маленькую остановку и в краткой форме позна-

CD

```
  library                    Различные документы для углубленного
                             изучения
      aes                    Документы по принятию нового стандарта
          daemen             Описание SQUARE
      common
      cryptocompress         Сжатие в криптографии
          bwt
      decrypt                Дешифрование шифров
          lucifer            Шифр "Люцифер"
          v
              freq           Частотный анализ
              hill           Шифр Хилла
              keylength      Длина ключа
              solve          Алгоритмы решения задач, возникающих
                             при дешифровании
      des                    Шифр DES
          abrahamsen         Один из предшественников DES
          patent
      feistel                Патент Файстеля
          feistel2
          horst
      gene                   Генетические алгоритмы
      libs                   Библиотеки шифрования
      milcrypt               Военная криптография
      misc
      modes                  Режимы шифрования
      navajo                 Криптографы Навахо
      sbox                   Узлы замен
      shannon                Шэннон
      square                 Еще о SQUARE
      wordlists              Словари
  software                   Программное обеспечение
      Far
          PlugIns
  sources                    Исходные тексты к книге
          compress           Сжатие
              chapter6       Исходные тексты сжатия и шифрования
      bignum                 Обработка больших чисел
      pgpcrack               Подбор паролей к PGP
          visual             Визуальный подборщик
      rc4                    Реализация алгоритма RC4
      scripher               Исходные тексты scripher
          encoder
          release
              scripher
              tools
```

Список всех файлов с исходными текстами на CD

комиться с содержанием каждой главы и некоторых разделов, с тем чтобы определиться, что читать в первую очередь, а что оставить «на потом».

Как наверняка уже успел заметить внимательный читатель, всего в книге семь глав. Основные материалы в ней разделены между всеми главами поровну. Три главы носят вводный характер, остальные три носят прикладной характер. Первая глава является вводной.

Весь материал довольно четко сначала был разделен на два уровня, а затем слит воедино для удобства чтения. Так, в основном в книге более детальные описания криптосистем расположены после общих утверждений и небольших введений в соответствующие области криптографии и криптоанализа. Материал разного уровня обычно достаточно автономен и заключен в различные разделы глав. Однако общая концепция ее состоит в использовании общего и единого логического пути чтения всей книги последовательно. Хотя, конечно, как именно будет читать книгу ее непосредственный владелец — это его личное дело. Но чтобы оценить уровень своей подготовки и, не испытывая трудностей, преодолеть все без исключения страницы данной книги, читатель может ознакомиться с разделом «Для кого и о чем эта книга».

В этой книге авторы уделяют особое внимание вопросам терминологии вообще и русской терминологии в криптографии особенно. Сложившейся специализированной *открытой* отрасли русской терминологии в этой области уже более сорока лет, хотя в последнее время она претерпевает многочисленные изменения и дополнения. Учитывая это, авторы, чтобы избежать возможных недоразумений и недомолвок, пользуются своей привычной терминологией, стараясь использовать не популярные общепринятые толкования, а их стандартизированные эквиваленты. По этой причине всем без исключения мы советуем прочесть раздел «К вопросу о терминологии», поскольку он довольно важен и для начинающего, и для уже подготовленного специалиста. Многие вопросы, освещенные в данной книге, используют только ту терминологию, которая описана в указанном разделе.

Те читатели, которые хотят получить также и практический опыт параллельно с чтением книги, возможно, предпочтут сначала хотя бы пробежать взглядом раздел «Рабочий инструментарий, который может пригодиться читателю». Кроме этого, людям, тяготеющим более к практическому программированию, чем к теоретическим выкладкам, следует обязательно обратить внимание на раздел «Отступление для программистов» второй главы «Теория секретных систем», в котором содержится соответствующая вводная информация и исходные тексты. Они будут активно использоваться в исходных текстах и частях книги «для пишущей братии» во всех остальных главах.

Конечно, в книге, связанной, пожалуй, с самой интригующей научной областью исследований, немало внимания уделяется увлекательным фактам из истории, особенно если они носят полумистический характер. Так, в третьей и пятой главах, целиком посвященных такой животрепещущей теме, как криптоанализ, читатель сможет прочесть даже о шифрах, которые использовались советской разведкой в прошлом, только что ушедшем от нас веке. Приведенные в третьей главе рассказы об известных головоломках могут увлечь не хуже хорошего детектива. Одной из таких головомок, заданных человечеству, являются шифры изве-

стного писателя и мистика Эдгара По, бывшего блистательным криптографом и криптоаналитиком. В конце второй главы дается решение двум его шифрам, проделанное именно с помощью компьютера, то есть, по сути, с помощью компьютерного криптоанализа.

Кроме этого, авторы предлагают рассмотреть и попробовать создать и использовать самостоятельно компьютерные методы криптоанализа, представляя вниманию читателя идеи и исходные тексты программ. Собственно, авторы рассчитывают на то, что в какой-то момент чтения, читателю наверняка захочется попробовать свои силы в криптографии и особенно в криптоанализе, которому в данной книге уделено достаточно внимания, в отличие от многих других подобных изданий. Для этого в каждой из трех основных глав приводятся исходные тексты программ, уже написанных авторами, и зачастую предлагаются методы и алгоритмы их улучшения, что, несомненно, должно помочь читателю осуществить свои желания.

Несмотря на найденное решение довольно сложной проблемы выстраивания около полусотни разделов глав и расположения материала книги в логически стройные последовательности, книгу можно использовать и как справочное пособие при разработке и оценке одноключевых криптосистем. Это верно, поскольку третья глава «Как устроены современные шифры», кроме общей информации о классических системах шифрования наших дней, носит также и справочный характер, представляя более углубленный материал о популярных современных симметричных шифрах, а следующая за ней глава «Дешифрование современных шифров» описывает собственно методы их криптоанализа.

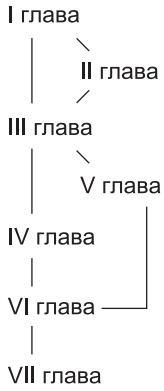
Кроме описания довольно популярных блочных и поточных криптосистем, в книгу было решено включить и довольно нестандартные решения и алгоритмы в области обеспечения конфиденциальности информации. Результатом этого решения стало появление дополнительной главы «Криптографическое сжатие», приведшее также к необходимости краткого изложения теории и методов сжатия.

Вторая глава предоставляет информацию о современной криптографии, начиная с эпохи Клода Шеннона и заканчивая принятым совсем недавно новым стандартом шифрования США. Параллельно с историческими аспектами и рассмотрением различных архитектур построения шифров рассматриваются современные методы криптоанализа, а также их возможные компьютерные реализации. Детально обсуждаются такие параметры симметричных шифров, как размер ключа и управляемые криптографические примитивы.

Каждое ружье, висящее на стене, должно когда-либо выстрелить. Этой непререкаемой истине последовали и авторы книги. Потому в седьмой главе «Прикладные задачи шифрования» все «ружья» оказались при деле. Именно в ней раскрываются решения прикладных задач: конфиденциальной связи, защищенных контейнеров данных, защиты исходных текстов и данных с помощью криптографических методов, о которых рассказано ранее. Кроме этого, в главе представлен пример исследования программного обеспечения на предмет надежности использования криптографических средств шифрования. Авторы провели небольшое исследование метода шифрования криптодиска популярной программы PGPDisk.

Каждая глава имеет самостоятельную нумерацию примеров исходных текстов — листингов программ и рисунков, а также независимый список литературы для углубленного изучения.

Таким образом, логическую цепочку связи глав можно представить приблизительно так:



Количество узких областей исследования в криптологии настолько велико, что трудно себе представить полное описание всех связанных с ней аспектов в одной книге. Книга призвана не только разобраться в уже существующих популярных системах шифрования, но и расширить кругозор читателя в этой области, а также дать реальную возможность научиться создавать и анализировать шифры самостоятельно.

Для кого и о чем эта книга

Книга предзначается в первую очередь для тех, кто интересуется не только теоретическими аспектами криптологии — как криптографии, так и криптоанализа, — но и практическими реализациями используемых в них алгоритмов и методов.

В ней уделено очень много внимания вопросам компьютерного криптоанализа и логике программирования криптосистем. Материал изложен таким образом, что он будет полезен и для неподготовленного читателя, и для высококвалифицированного специалиста, желающего расширить свой кругозор и по-новому взглянуть на криптографический аспект систем информационной защиты. Речь в книге не идет о каких-то конкретных программных продуктах, наоборот — прочтя книгу, подготовленный читатель будет способен самостоятельно создавать программное обеспечение, содержащее криптографические алгоритмы. Однако для этого ему все же пригодятся навыки программиста и математика, хотя бы на начальном уровне.

Кроме стандартных и популярных средств одноключевого шифрования, в книге рассматриваются нестандартные алгоритмы, которые могут использоваться на практике, а также оригинальные и необычные подходы к шифрованию и криптоанализу, что может значительно расширить кругозор даже опытного специалиста. Тем, кто интересуется созданием собственных шифросистем, будет также интересна и полезна информация, связанная с современными требованиями к сертификации и лицензированию средств шифрования.

Таким образом, книга будет чрезвычайно полезной как для студентов вузов соответствующих специальностей, так и просто интересующихся компьютерными технологиями, а также для специалистов в области обеспечения информационной безопасности и разработки соответствующих программных средств. Книга содержит множество математических описаний шифров и может быть полезна в качестве учебного пособия.

Рабочий инструментарий, который может пригодиться читателю

Исследуя вопросы реализации криптографических методов защиты информации, мы неизбежно сталкиваемся с вопросами, касающимися таких факторов, как среда программирования, язык программирования, схемы реализации и верификации программного обеспечения, тестовые испытания.

Все исходные тексты, представленные в данной книге, написаны на языках Си и Perl. Для языка Си использовалась среда разработки программного обеспечения **Borland C++ Builder 5**, а для исполнения скриптов на языке Perl необходим **ActiveState Perl** или иной другой аналогичный интерпретатор.

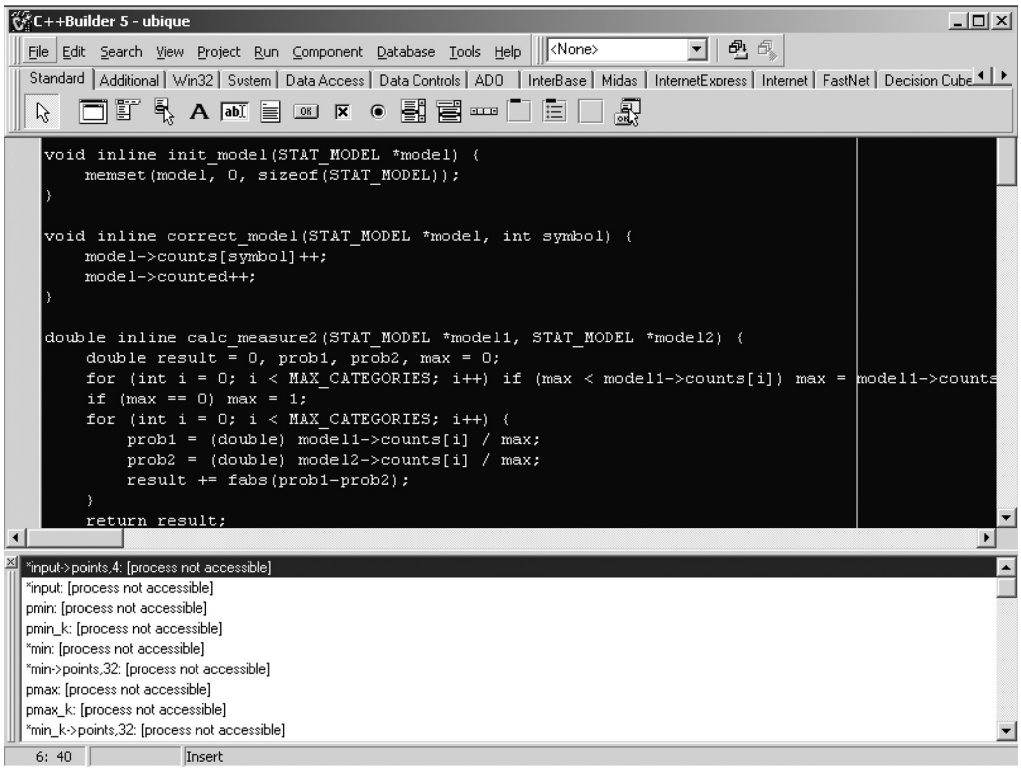


Рис. 1.1. Borland C++ Builder

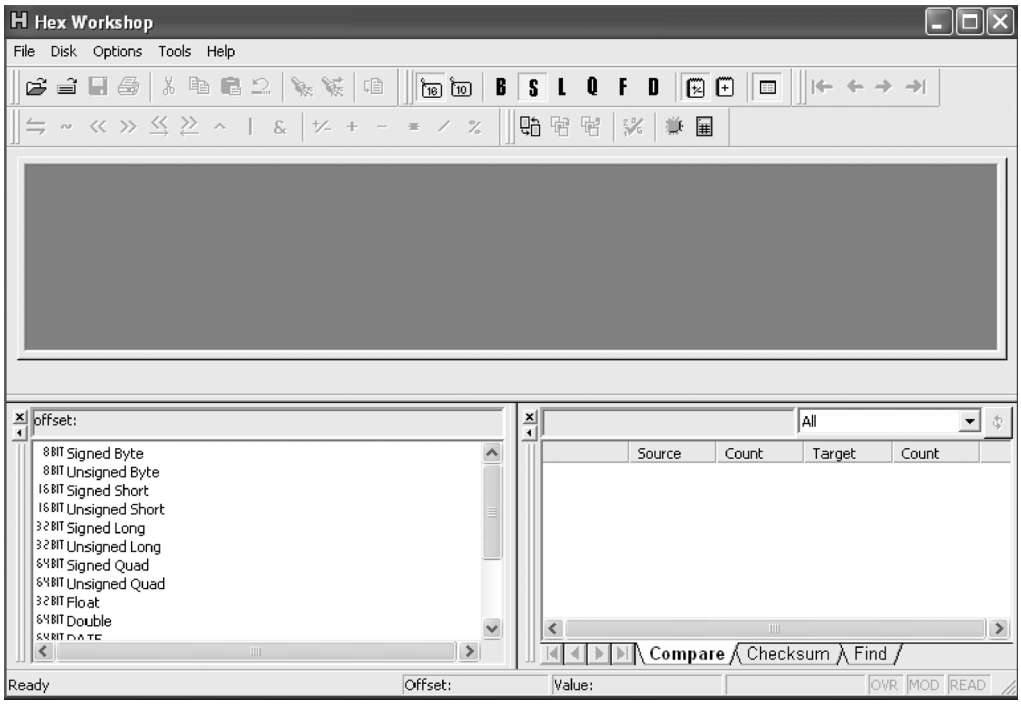


Рис. 1.2. HexWorkshop

Еще одним необходимым в работе инструментом для читателя станет шестнадцатеричный редактор. Можно использовать какой-либо специализированный вроде **HexWorkshop** или, что еще лучше — **HIEW**, но для работы вполне сойдет и встроенный, например, в файловый менеджер Far редактор шестнадцатеричных кодов. Он особенно пригодится для изучения выхода тех шифров, которые реализованы в этой книге.

Собственно говоря, это практически все основные инструменты, которые понадобятся при получении практических навыков и работе с исходными текстами, опубликованными в данной книге.

К вопросу о терминологии

К вопросу о терминологии в криптографии авторы книги стараются относиться весьма деликатно. На сегодняшний день в России существует одна из самых сильных криптографических школ в мире — наследие СССР. Советские криптоаналитики еще долго будут считаться одними из самых сильных специалистов в этой области. Соответственно наработаны и терминология, и большинство принципов таксономии, в том числе и адекватное переложение и адаптация на русский язык вновь появляющихся иностранных терминов.

Тем не менее вся эта информация до последнего времени была конфиденциальной и строжайше охранялась. Само слово «криптография» не вызывало ника-

ких ассоциаций у подавляющего большинства математиков и специалистов по связи. Если необходимо было «закрыть» канал связи, то использовалась специальная аппаратура, которая представлялась для конечных пользователей «черным ящиком», в который надо было лишь воткнуть проводки, нажать на определенные кнопки и повернуть ручки.

С начала 90-х годов ситуация резко изменилась. Выпущено уже несколько сотен различных изданий по теме информационной безопасности, в том числе и по криптографии. Множество книг переведены с иностранных языков, каждый месяц появляются книги русских авторов по прикладной и теоретической криптографии.

К сожалению, количество выпускаемых книг не всегда сопровождается качеством. И особое внимание необходимо уделять именно тому, как вольно обращаются с терминами новоиспеченные «криптоматематики». Некоторые авторы «книг по криптографии» не имеют никакого отношения даже к математике, не говоря уж о кодах и шифрах. Потому и выходят казусы с «шифрацией», «криптованием» и «дешифрированием» данных.

Конечно, никто не застрахован от возможных нелепостей и казусов, связанных с написанием, редактированием, версткой, макетированием и печатью больших объемов текста. Поэтому авторы просят осведомленных читателей отнестись с пониманием к возможным техническим «ляпам».

А для того чтобы избежать технических накладок, авторы предлагают считать верными следующие трактовки зарубежных и отечественных терминов:

- криптографическая атака (cryptoanalitic attack) — попытка криптоаналитика вызвать отклонения от нормального проведения процесса конфиденциального обмена информацией. Соответственно взлом или вскрытие, дешифрование шифра или шифросистемы — это успешное применение криптографической атаки;
- криптоанализ (cryptanalysis) и криптоаналитик (cryptanalytic) — соответственно набор методик и алгоритмов дешифрования криптографически защищенных сообщений, анализа шифросистем и человек, все это осуществляющий;
- дешифрование (deciphering) и расшифрование (decryption) — соответственно методы извлечения информации без знания криптографического ключа и со знанием оного. Термин «дешифрование» обычно применяют по отношению к процессу криптоанализа шифротекста (криптоанализ сам по себе, вообще говоря, может заключаться и в анализе шифросистемы, а не только зашифрованного ею открытого сообщения);
- криптографический ключ (cryptographic key, cryptokey, иногда просто key) — в случае классических криптосистем секретная компонента шифра. Должен быть известен только законным пользователям процесса обмена информации;
- зашифрование (encryption) — процесс зашифрования информации, то есть применения криптографического преобразования данных, эту информацию содержащих;

- аутентичность данных и систем (authenticity of information) — для данных аутентичность можно определить как факт подтверждения подлинности информации, содержащейся в этих данных, а для систем — способность обеспечивать процедуру соответствующей проверки — аутентификации данных;
- аутентификация (authentication) — процедура проверки подлинности данных, то есть того, что эти данные были созданы легитимными (законными) участниками процесса обмена информации;
- гамма-последовательность или просто гамма (gamma sequence, gamma) — обычно этот термин употребляется в отношении последовательности псевдослучайных элементов, которые генерируются по определенному закону и алгоритму. Однако в случае, когда это не так, употребляется модификация термина — например, «равновероятная гамма» или «случайная гамма» — для обозначения последовательностей, элементы которых распределены по равномерному вероятностному закону, то есть значения имеют сплошной спектр;
- гаммирование (gamma xoring) — процесс «наложения» гамма-последовательности на открытые данные. Обычно это суммирование в каком-либо конечном поле (например, в поле GF(2) (см. [4, 6 и 9]) такое суммирование принимает вид обычного «исключающего ИЛИ» суммирования);
- имитозащита — это защита данных в системах их передачи и хранения от навязывания ложной информации. Имитозащита достигается обычно за счет включения в пакет передаваемых данных имитовставки;
- имитовставка — блок информации, вычисленный по определенному закону и зависящий от некоторого криптографического ключа и данных;
- блочные (блоковые) и поточные (потоковые) шифры — авторы сознательно используют термин «блочный» шифр, а не «блоковый», как наиболее популярный и устоявшийся. Понятия «поточного» и «потокового» шифров идентичны и одинаково популярны, однако в силу симметрии авторы предпочитают использовать термин «поточный шифр», но «потоковая обработка информации»;
- криптографическая стойкость, криптостойкость (cryptographic strength) — устойчивость шифросистемы по отношению ко всем известным видам криптоанализа;
- принцип Керкхоффа (Kerchkoff) — принцип изобретения и распространения криптографических алгоритмов, в соответствии с которым в секрете держится только определенный набор параметров шифра (и в обязательном порядке криптографический ключ), а все остальное может быть открытым без снижения криптостойкости алгоритма. Этот принцип был впервые сформулирован в работе голландского криптографа Керкхоффа «Военная криптография» вместе с дюжиной других, не менее известных (например, о том, что шифр должен быть удобным в эксплуатации, а также о том, что шифр должен быть легко запоминаемым);
- развертывание или разворачивание ключа (key shedule) — процедура вычисления последовательности подключей шифра из основного ключа шифрования;

- раунд или цикл шифрования (round) — один комплексный шаг алгоритма, в процессе которого преобразовываются данные;
- подключ шифрования (round key, subkey) — криптографический ключ, вычисляемый и используемый только на этапе шифрования из основного ключа шифрования. Обычно применяется в качестве входа функций усложнения на различных раундах шифрования;
- шифр и шифросистема (cipher, cypher, ciphercode) — обычно выход криптосистемы и сама симметричная криптосистема соответственно. В зависимости от контекста шифр может обозначает «шифровку», то есть зашифрованное с его помощью сообщение, либо саму криптографическую систему преобразования информации.

Список литературы

1. Столлингс В. «Криптография и защита сетей», М: Вильямс, 2001.

2. Медведовский И. Д., Семьянов П. В., Платонов В. В., «Атака через Интернет», СПб: 1999.

3. В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич: «Защита в операционных системах», М: Радио и связь: 2000.

4. Аграновский А. В., Хади Р. А., Ерусалимский Я. М., «Открытые системы и криптография», Телекоммуникации, 2000.

5. Agranovsky A. V., Hady R. A., «Crypto miracles with random oracle», The Proceedings of IEEE SIBCOM'2001, The Tomsk Chapter of the Institute of Electrical and Electronics Engineers, 2001.

6. А. В. Аграновский, А. В. Балакин, Р. А. Хади, «Классические шифры и методы их криптоанализа», М: Машиностроение, Информационные технологии, № 10, 2001.

7. А. А. Молдовян, Н. А. Молдовян, Советов Б. Я., «Криптография»: СПб.: Издательство «Лань», 2000.

8. С. Расторгуев, «Программные методы защиты информации в компьютерах и сетях», М: Издательство Агентства «Яхтсмен», 1993.

9. А. Ростовцев, «Алгебраические основы криптографии», СПб.: Мир и Семья, 2000.

10. Чмора А. Л., «Современная прикладная криптография», М.: Гелиос АРВ, 2001.

11. Устинов Г. Н., «Основы информационной безопасности», М: Синтег, 2000.

12. Анин Б., «Защита компьютерной информации», СПб: БХВ, 2000.

13. Романец Ю. В., Тимофеев П. А., «Защита информации в компьютерных системах и сетях», М: Радио и связь, 2001.

14. Menezes A., van Oorschot P., Vanstone S., «Handbook of Applied Cryptography», CRC press, 1996.

15. Schneier B., «Applied Cryptography», John Wiley & Sons Inc, 1996.

16. Милославская Н. Г., Толстой А. И., «Интрасети: доступ в Интернет, защита», М.: ЮНИТИ-ДАНА, 2000.

17. Gutmann P.: «Network Security», University of Auckland, 1996.

18. Саломаа А.: «Криптография с открытым ключом», Москва: «Мир», 1995. 318 с.

19. Олифер В., Олифер Н.: «Компьютерные сети», Спб.: Издательство «Питер», 1999. 672 с.