А. Л. Чмора

Информационная безопасность в компьютерных сетях

Современная прикладная криптография

Москва
АйТи
1999

Информационная безопасность в компьютерных сетях. *Современная прикладная криптография.* — **М.: АйТи, 1999. — 242 с.**
В настоящей книге, посвященной вопросам информационной безопасности, рассматриваются криптографические методы и технология защиты информации в компьютерных сетях. В первую очередь книга будет полезна разработчикам сетевых решений, администраторам ЛВС, провайдерам, студентам и аспирантам технических университетов, специализирующихся в области компьютерных технологий.

Л$\frac{0000000000\text{–}000}{\text{Р00(00)–00}}$

ISDN 0-000000-00-0

Памяти Виктора Панченко — талантливого математика и криптографа

Содержание

Предисловие

Давно отошли в прошлое времена, когда слова «криптография», «шифр», «секретный ключ» и т.п. у подавляющего большинства людей ассоциировались лишь с недавно просмотренным кинофильмом или модным шпионским романом. В настоящее время технологии защиты информации прочно вошли в повседневную жизнь. Кредитные карточки для получения наличных в банкоматах, банковские операции, переписка по Internet, защита файлов в компьютере от любопытных коллег и многое другое — все это немыслимо без применения современной криптологии. Растущая потребность в специалистах по защите информации так или иначе удовлетворяется — «природа не терпит пустоты». За рубежом изданы десятки учебников и монографий, посвященных криптографии и различным аспектам ее применения, издается множество специализированных журналов. К сожалению, в России дело обстоит совсем иначе. По пальцам можно пересчитать учебные пособия, изданные благодаря энтузиазму нескольких вузов. Еще легче сосчитать периодические специализированные издания. В связи с этим появление книги А.Л.Чморы «Информационная безопасность в компьютерных сетях. *Современная прикладная криптография*» является заметным событием. Книга начинается с описания базовых концепций. Описана большая часть разработанных к настоящему времени криптосистем с симметричными ключами. Подробно рассмотрены системы с открытыми ключами и методы аутентификации, методы разделения секретов и элементы финансовой криптографии, некоторые новые идеи. Справедливости ради следует отметить, что книга довольно трудна для первоначального ознакомления с предметом, но обилие материала, в том числе справочного характера, полностью искупает этот недостаток. К тому же она прекрасно дополняет пусть и малодоступные, но все же существующие источники на русском языке. Можно с уверенностью сказать, что эта книга будет способствовать подъему интереса к вопросам защиты информации и найдет своего читателя как среди специалистов, так и среди студентов и аспирантов.

Действительный член Международной Академии информатизации,
доктор технических наук,
профессор Э.М.Габидулин.

Предисловие автора

Почему написана эта книга

Причина появления этой книги — явный недостаток литературы подобного рода на русском языке, с одной стороны, и острый интерес к рассматриваемой теме, с другой.

В настоящее время данная область знания представлена несколькими книгами, учебными пособиями[1] и научно-популярными брошюрами[2]. В 1996 году в издательстве «Мир» вышла книга А. Саломаа, описывающая достижения в области криптографии до 1990 года[3]. В 1997 году группа сотрудников лаборатории МГУ по математическим проблемам криптографии под руководством профессора В.М.Сидельникова при содействии Московского государственного инженерно-физического института опубликовала книгу по криптографическим проблемам защиты банковской информации[4]. В 1997 году Российская Академия Наук и Академия криптографии Российской Федерации выпустили первый том сборника трудов, посвященных исследованиям математических моделей дискретных устройств обработки информации, представляющих интерес с точки зрения криптографии[5]. Издание является приложением к журналу «Дискретная математика». Предполагаемая периодичность выхода — один том в год.

Отметим, что тираж большинства книг и учебных пособий не превышает нескольких сотен экземпляров.

Министерством общего и профессионального образования официально утверждены специальности: 013200 (криптография) и 220600 (организация и технология защиты информации). Ведущим учебным центром по подготовке специалистов-криптографов является Институт криптографии, связи и информатики (ИКСИ) Академии ФСБ России. Для организации обучения по указанным специальностям необходима лицензия Минвуза, которая после соответствующей аттестации выдается учебно-методическим объединением (УМО) по информационной безопасности. В настоящее время лицензию на подготовку специалистов по криптографии имеет только ИКСИ. Подготовку по специальности «организация и технология защиты информации» осуществляют в МИФИ (факультет информационной безопасности) и РГГУ (факультет защиты информации).

В Московском Университете организуется новое подразделение под названием «Учебно-научный центр по проблемам информационной безопасности». В его состав войдут Высшие курсы переподготовки и повышения квалификации по информационной безопасности.

Основное содержание предлагаемой книги касается вопросов криптографической защиты информации в компьютерных сетях. Автор постарался включить в книгу материал, который по тем или иным причинам не вошел в упомянутые выше издания. Отметим, что книга писалась не как математическая работа, а как практическое введение в криптографию,

[1] Варфоломеев А.А., Пеленицин М. Б. Методы криптографии и их применение в банковских технологиях. — М.: МИФИ, 1995.

Фомичев В.М. Симметричные криптосистемы. Краткий обзор основ криптологии для шифрсистем с секретным ключом. — М.: МИФИ, 1995.

Варфоломеев А.А., Домнина О.С., Пеленицин М.Б. Управление ключами в системах криптографической защиты банковской информации. — М.: МИФИ, 1996.

Ростовцев А.Г., Матвеев В.А. Защита информации в компьютерных системах. Элементы криптологии. — СПб.: СПбГТУ, 1993.

[2] Жельников В. Криптография от папируса до компьютера. — М.: ABF, 1996.

Дориченко С.А., Ященко В.В. 25 этюдов о шифрах. — М.: ТЕИС, 1994.

[3] Саломаа А. Криптография с открытым ключом. — М.: Мир, 1996.

[4] Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. Методические материалы. — М.: МИФИ, 1997.

[5] Российская Академия наук. Академия криптографии Российской Федерации. Труды по дискретной математике. Том 1. — М.: ТВП, 1997.

ставшую неотъемлемой частью современных сетевых технологий. Для интересующихся теоретическими результатами приведены обширные ссылки на академическую литературу. По соображениям объема пришлось многое оставить за рамками данной работы. Так, в книге не рассматриваются:

1) Теоретико-информационные вопросы криптографии и аутентификации — граница Шеннона, расстояние единственности, граница Симмонса, граница «квадратного корня». По счастливой случайности фундаментальный труд К.Э.Шеннона был переведен на русский язык и опубликован в 1963 году[6].

2) Классическая криптография — одноалфавитные и многоалфавитные криптосистемы (шифры Полибия, Цезаря, криптосистемы Хилла, Плейфера, Виженера, Бьюфорта, аффинные криптосистемы, роторные машины), перестановки и подстановки, перемешивание и рассеивание, методы классического криптоанализа (частотный, метод Казиски для периодических криптосистем с неизвестным периодом). Несмотря на название, книга А. Саломаа содержит прекрасное введение в данную область.

3) Теоретико-числовая и сложностная проблематика. Методы дискретного логарифмирования (алгоритмы Гельфонда, Полига-Хэллмана, для полей простого порядка, Хэллмана-Рейнери, Копперсмита, логарифмирование на эллиптических кривых), алгоритмы модульного возведения в степень, факторизации больших целых чисел (экспоненциально- и субэкспоненциально-трудоемкие алгоритмы Шермана-Лемана, Полларда, Полларда-Штрассена, Диксона, Бриллхарта-Моррисона, квадратичного решета, числового решета, обобщенного числового решета) и тесты на простоту подробно рассматриваются в упомянутых выше изданиях. Понятие полиномиальной сложности, классы P и NP вводятся в известной книге М.Гэри и Д.Джонсона[7].

4) Криптографические протоколы на основе интерактивных систем доказательства. Элементы теории доказательства с нулевым знанием[8].

Вследствие ограниченного объема в книгу не вошел материал по современной стеганографии — цифровым «водяным знакам» и другим методам аутентификации мультимедийной информации. Возможно, эта тема заслуживает отдельного рассмотрения.

Уровень подготовки читателя

Необходимый уровень образования читателя этой книги должен соответствовать типичной математической подготовке студента, прослушавшего ряд курсов помимо математического анализа. Однако для полного «погружения» в мир криптографии необходима специальная математическая подготовка — прежде всего владение основами теории чисел[9] и теории конечных полей[10] в объеме университетского курса.

Автор постарался раскрыть содержание основных идей современной криптографии, не прибегая к строгому языку математики, пытаясь представить математические рассуждения, там где они необходимы, в интуитивно понятной форме. Насколько ему это удалось — судить читателю.

Обзор содержания

Глава I представляет собой изложение методологии информационной безопасности согласно «Оранжевой книге» и рекомендациям CCITT X.800. Вводятся основные понятия и рассматривается общая концепция информационной безопасности.

Глава II посвящена описанию криптографических методов. Разделы с первого по третий содержат изложение базовых принципов и моделей современной криптографии. Криптографические методы иллюстрируются на примере протокола SSL. Четвертый раздел посвящен

[6] Шеннон К.Э. Теория связи в секретных системах. В кн.: Шеннон К.Э. *Работы по теории информации и кибернетике.* — М.: ИЛ, 1963, с. 243-332.

[7] Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

[8] В некоторых источниках вместо термина «знание» используется термин «разглашение».

[9] Виноградов И.М. Основы теории чисел. Издание пятое, переработанное. Государственное издательство технико-теоретической литературы. Москва-Ленинград. 1949.

Боревич З.И., Шафаревич И.Р. Теория чисел. — М.: Наука, 1985.

[10] Лидл Р., Нидеррайтер Г. Конечные поля. — М.: Мир, 1988. (в 2-х томах).

симметричным криптосистемам и блочным шифрам. Вводится понятие принципа итерирования и конструкция Фейстеля. Рассматриваются режимы шифрования блочных шифров. Отдельные разделы посвящены стандартам DES и ГОСТ 28147-89. Описываются ключевые идеи некоторых криптоаналитических атак, в том числе силовой атаки на основе распределенных вычислений. Пятый раздел представляет собой краткое введение в теорию поточных шифров. Стоимость силовой атаки с учетом технологических достижений и адекватная длина ключа симметричной криптосистемы, позволяющая противостоять подобной атаке, рассматриваются в шестом разделе. Описание универсального метода расширения ключевого пространства при ограничении разрядности секретного ключа приводится в седьмом разделе. Восьмой раздел посвящен обсуждению асимметричных криптосистем. Особое внимание уделяется вопросу практической криптостойкости RSA, а также специальной методике выбора делителей модуля, известной под названием «разбалансированной RSA». Девятый раздел является введением в технологию хэш-функций. Дается описание широко распространенных на практике алгоритмов MD4, MD5, MD2, RIPEMD, стандартов SHS и ГОСТ Р 34.11-94. Десятый раздел посвящен цифровой подписи и содержит описание общей концепции цифровой подписи, стандартов DSS и ГОСТ Р 34.10-94.

Глава III посвящена изложению методологии управления ключами — одной из основных задач практической криптографии. Изложение охватывает множество различных аспектов проблемы, начиная с генерации, распределения, проверки, использования, обновления и хранения ключей симметричных криптосистем и заканчивая распределением ключей для асимметричных криптосистем.

Глава IV содержит изложение идеи разделения секрета. Описываются классические схемы Блэкли, Шамира и схемы на основе кодов Рида-Соломона. Рассматриваются некоторые практические приложения.

В Главе V рассматриваются протоколы анонимных (неотслеживаемых) платежей, а также электронные микроплатежные схемы на примере систем PayWord и MicroMint.

В Главе VI излагается метод депонирования ключей. Приводится общее описание криптоалгоритма Skipjack, стандарта EES, проектов Clipper и Capstone.

Как обеспечить паритетный уровень, учитывая противоречивые требования национальной и коммерческой безопасности? В Главе VII описывается возможный подход к решению этой проблемы.

Криптография не стоит на месте. Новые криптографические идеи — криптография с временным (ударение на последнем слоге) раскрытием и квантовая криптография описываются в Главе VIII.

Глава IX посвящена аутентификации. В первом и втором разделах излагаются методы аутентификации на основе применения паролей и биометрических измерений. В третьем — криптографические методы аутентификации в компьютерных сетях. Четвертый раздел посвящен анализу криптографических протоколов. BAN-логика — метод формального анализа протоколов — описывается в пятом разделе. Описание широко применяемого на практике протокола аутентификации Kerberos приводится в шестом разделе.

Доказательство принадлежности — важная практическая задача. В Главе X дается последовательное изложение методов доказательства принадлежности при отказе отправителя/получателя от ранее переданных/принятых сообщений.

В Приложении приводятся ссылки на различные криптографические источники в Internet.

Автор с благодарностью примет все предложения и замечания по книге; их следует направлять по адресу: *chmora@iitp.ru*.

Благодарности

Хотелось бы выразить благодарность В.И.Панченко, стимулировавшего интерес автора к криптографии и общение с которым отличалось особой глубиной и содержанием, а также — признательность Институту проблем передачи информации РАН за создание творческой научной атмосферы и всестороннюю поддержку во время работы над этой книги.

Автор выражает искреннюю признательность профессору Московского физико-технического института, д.т.н. Э.М.Габидулину за внимательное отношение к рукописи, критические замечания и полезные рекомендации.

И, наконец, автор благодарит свою супругу Ольгу за проявленное терпение и понимание.

А. Л. Чмора

6 января 1999 года
Москва

Криптогра́фія ж. **тайнописаніе, цыфрованное (шифрованное), тарабарское письмо, знаками вмѣсто буквъ.**

Толковый словарь живаго великорускаго языка. Владиміра Даля. Второе изданіе. Томъ второй. Издательство М.О.Вольфа. 1881 годъ. стр. 194.

Ши́фра ж. **всякій условный письменный знакъ, кромѣ обычныхъ буквъ.**
Шифры мн. или **тарабарская грамота, условные знаки для письма, замѣняющіе въ тайнописи буквы.**
Шифро́вщикъ, **кто пишетъ шифрованнымъ письмомъ, тарабарщиной;** || **мастеръ разгадывать, читать письмо это безъ** *шифра́нта*, **безъ ключа.**

Толковый словарь живаго великорускаго языка. Владиміра Даля. Второе изданіе. Томъ четвертый. Издательство М.О.Вольфа. 1882 годъ. стр. 636.