Предисловие

На протяжении последнего десятилетия криптография гораздо больше способствовала разрушению безопасности цифровых систем, чем ее усовершенствованию. В начале 90-х годов прошлого века криптография считалась настоящей панацеей, способной обеспечить безопасность в Internet. Одни воспринимали криптографию как грандиозный технологический "уравнитель" — математический аппарат, позволяющий уравнять права и возможности защиты данных среднестатистического обывателя и крупнейших государственных разведывательных служб. Другие видели в ней оружие, применение которого может привести к гибели наций, если будет потерян контроль за поведением людей в киберпространстве. Третьи представляли, что это настоящий рай для наркоторговцев, террористов и распространителей детской порнографии, которые смогли бы общаться между собой в атмосфере полной секретности. Даже неисправимым реалистам стало казаться, что криптография — то самое средство, которое приведет к расцвету глобальной коммерции в новом интерактивном сообществе.

Прошло 10 лет, и ожидания не оправдались. Несмотря на распространение криптографии, наличие государственных границ в Internet стало ощутимым более чем когда-либо. Способность обнаруживать и прослушивать переговоры членов криминальных группировок гораздо больше зависит от политики и человеческих ресурсов, нежели от математического аппарата. У частных лиц нет никаких шансов дотянуться до уровня хорошо финансируемых государственных разведслужб. И наконец, наблюдавшийся расцвет глобальной коммерции никак не связан с внедрением криптографии в широкие массы.

В большинстве случаев применение криптографии не дало пользователям Internet практически ничего, кроме ложного ощущения безопасности. Криптография обещала обеспечить безопасность обмена данными, но сделать это так и не удалось. И это плохо для всех (за исключением, разумеется, злоумышленников).

Причины подобного провала кроются не столько в криптографии как в математической науке, сколько в криптографии как в инженерной дисциплине. На протяжении последнего десятилетия мы разработали, реализовали и выпустили в свет массу криптографических систем. Как ни печально, превратить математические перспективы криптографической безопасности

в реальную безопасность оказалось намного сложнее, чем можно было предположить. Это и есть самая трудная часть программы.

Многие разработчики относятся к криптографии как к некоему волшебному порошку. Стоит только "посыпать" им аппаратное или программное обеспечение, как оно тут же приобретет то самое магическое свойство безопасности. Слишком многие потребители полагаются на волшебное действие этого порошка, слепо доверяя слову "зашифрованный" в громких рекламных кампаниях. Недалеко от них ушли и серьезные аналитики, которые на основании длины ключей шифрования провозглашали один продукт более безопасным, нежели другой.

Каждая система безопасна настолько, насколько безопасно ее самое слабое звено, а математический аппарат криптографии никогда не был ее слабым звеном. Фундаментальные концепции, лежащие в основе криптографии, безусловно, важны, однако гораздо важнее то, как они реализуются и используются на практике. Спорить о том, какой должна быть длина ключа — 112 или 128 бит, все равно что вкопать в землю огромный столб и надеяться, что злоумышленник в него врежется. Вы можете долго выяснять, какой высоты должен быть столб — километр или полтора километра, а злоумышленник просто обойдет его стороной. Однако безопасность — это не столб, а настоящий забор: т.е. целый комплекс неких вещей, делающих криптографию действительно эффективной.

Практически во всех книгах по криптографии, изданных на протяжении последних 10 лет, ощущается стойкий привкус "волшебного порошка". Все восхваляют преимущества "тройного" DES, скажем, со 112-битовым ключом шифрования, не упоминая о том, как следует генерировать или использовать ключи этого алгоритма. Книга за книгой описывает сложные протоколы, не затрагивая общественных или бизнес-ограничений, в рамках которых приходится применять эти протоколы, и рассматривает криптографию как чисто математическую дисциплину, не тронутую рамками и реалиями земного мира. Однако именно эти рамки и реалии определяют различие между мечтами о криптографическом чуде и суровыми буднями цифровой безопасности.

Книга *Практическая криптография* тоже посвящена этой дисциплине, однако здесь речь идет вовсе не о той "незапятнанной" криптографии, которая упоминалась выше. Назначение этой книги состоит в том, чтобы открыто описать все ограничения и аспекты применения криптографии в реальной жизни, а также рассказать о разработке действительно безопасных криптографических систем. В некотором смысле данная книга является продолжением книги Брюса Шнайера *Applied Cryptography* [86], впервые опубликованной более 10 лет назад. Однако, в отличие от книги *Applied Cryptography*, дающей широкое представление о криптографии и тысячах ее возможностей, *Практическая криптография* охватывает достаточно узкую, строго определенную

область знаний. Мы не предлагаем вам десятки вариантов; мы рассматриваем *один* вариант, описывая то, как его правильно реализовать. Книга *Applied Cryptography* демонстрирует поразительные возможности криптографии как математической науки — что возможно и что достижимо, в то время как *Практическая криптография* содержит конкретные советы, предназначенные для людей, которые разрабатывают и реализуют криптографические системы.

Настоящая книга — это попытка сократить разрыв между теорией криптографии и ее применением в реальной жизни, а также научить разработчиков использовать ее для повышения безопасности систем.

Мы позволили себе взяться за написание этой книги, поскольку оба являемся опытными специалистами в области криптографии. Брюса хорошо знают по его книгам *Applied Cryptography* (она упомянута выше) и *Secrets and Lies* [88], а также по информационному бюллетеню *Crypto-Gram*. Нильс отточил свое криптографическое мастерство, разрабатывая криптографические системы платежей в институте CWI (Национальный исследовательский институт математики и информатики Нидерландов) в Амстердаме и позднее в нидерландской компании DigiCash. Брюс разработал знаменитый алгоритм шифрования Blowfish, и мы оба принимали участие в разработке алгоритма Twofish. Исследования Нильса привели к появлению первого представителя нового поколения эффективных протоколов анонимных платежей. Общее количество написанных нами научных статей выражается трехзначным числом.

Что еще более важно, мы оба имеем обширный опыт в разработке и построении криптографических систем. С 1991 по 1999 годы консалтинговая компания Брюса Counterpane Systems предоставляла услуги по проектированию и анализу для нескольких крупнейших компьютерных и финансовых корпораций мира. В последние годы компания Counterpane Internet Security, Inc. занимается предоставлением услуг по слежению за безопасностью и ее обеспечению для больших корпораций и правительственных служб по всему миру. Нильс тоже работал в Counterpane перед тем, как основал собственную консалтинговую компанию MacFergus. Мы живем и дышим криптографией. Мы наблюдаем, как она "прогибается" под тяжестью реалий разработки программных систем и, что еще хуже, под тяжестью реалий бизнеса. Мы позволили себе издать эту книгу, поскольку уже десятки раз писали ее для клиентов, которых консультируем.

Как читать эту книгу

Книгу *Практическая криптография* вряд ли можно назвать справочником. В ней прослеживается процесс проектирования криптографической си-

стемы от выбора конкретных алгоритмов через всевозможные наслоения вопросов безопасности до построения инфраструктуры, необходимой для работы этой системы. На протяжении книги обсуждается одна-единственная проблема криптографии, лежащая в основе практически каждой криптографической системы: как обеспечить безопасность общения двух людей. Сконцентрировав все внимание на одной проблеме и одной философии проектирования, применяемой для ее решения, мы верим, что можем рассказать больше о реальных аспектах разработки криптографических систем.

Мы оба уже издавали книги и прекрасно знаем, что это не имеет никакого отношения к точным наукам. Как бы мы ни старались, нам не удастся избежать ошибок. Простите за откровенность, но мы просто реально смотрим на вещи. (Что интересно, криптографические системы страдают от той же проблемы; это обсуждается в нескольких главах.) Конечно же, мы приложили все усилия к тому, чтобы довести свою книгу до совершенства, и вместе с тем разработали процедуру, гарантирующую, что все наши ошибки (а они, увы, неизбежны) когда-нибудь будут исправлены.

- Прежде чем приступать к чтению книги, посетите Web-узел `http://www.macfergus.com/pc` и загрузите текущий список исправлений.
- Если вы обнаружите в книге ошибку, проверьте, не встречается ли она в списке исправлений.
- Если ее там нет, пожалуйста, сообщите о ней по адресу:

  `practical-cryptography@macfergus.com`

  Мы непременно добавим ее к списку.

На наш взгляд, криптография — это самая интересная вещь во всей математике. Мы постарались наполнить книгу этим ощущением и надеемся, что вам понравится результат. Спасибо, что вы с нами.

Январь 2003 года

Нильс Фергюсон
Амстердам
Нидерланды
`niels@macfergus.com`

Брюс Шнайер
Миннеаполис, Миннесота
США
`schneier@counterplane.com`