

НЕКОТОРЫЕ НЕМАТЕМАТИЧЕСКИЕ ПОДХОДЫ К ПОСТРОЕНИЮ АЛГОРИТМОВ ШИФРОВАНИЯ

Трунов Д.Н., магистр, d.n.trunov@gmail.com

Самозанятое лицо, г. Покровск, Украина

Криптография, занимающаяся вопросами шифрования информации, является разделом прикладной математики, а принципы построения криптографических систем защиты информации основаны на использовании математических функций специального вида [1]. Отсюда и математические подходы к оценкам стойкости алгоритмов шифрования: алгоритм признаётся стойким, если удаётся математически доказать невозможность его вскрытия.

Проблема, однако, в том, что с учётом современного состояния теории сложности вычислений, стойкость криптографических систем может быть установлена лишь с привлечением каких-либо недоказанных предположений [2]. Задача, на которой основан конкретный алгоритм, может быть признана вычислительно сложной на основании того факта, что на протяжении длительного времени не было обнаружено более простого способа её решения. Но иногда подобные способы находятся, и тогда такой алгоритм перестаёт быть стойким.

Возникает вопрос: так ли уж надёжны существующие математические подходы к построению и оценке криптографических систем (алгоритмов шифрования) и можно ли создать надёжный алгоритм, не опираясь на такие подходы? С одной стороны, нужно согласиться, что существующие подходы позволяют избегать создания и применения заведомо ненадёжных и слабых алгоритмов. С другой стороны, возможно, они отвергают ряд вполне надёжных алгоритмов по той лишь причине, что эту надёжность нельзя доказать.

Какие же это алгоритмы? Во-первых, все сложные алгоритмы. Сложные программные системы считаются по определению менее надёжными [3]. Сложные системы обязательно модульные, а взаимодействие модулей создаёт дополнительные возможности для взлома защиты. Сложные системы трудны для анализа и понимания их устройства, а это является необходимым условием безопасного управления ими.

Во-вторых, алгоритмы, созданные объединением нескольких других алгоритмов. Само по себе объединение алгоритмов не даёт гарантии создания надёжной системы, поэтому каждое объединение рассматривается и оценивается отдельно (например, трёхкратный DES). Впрочем, есть утверждение, что последовательное шифрование взломать по крайней мере не легче, чем самый сильный из шифров последовательности [4]. А это уже определённое преимущество.

Остановимся подробнее на сложных системах. Основными криптографическими методами в современных алгоритмах шифрования являются рассеивание (диффузия) и перемешивание [4, 5]. Рассеивание распространяет влияние отдельных битов открытого текста на как можно большее количество битов шифротекста, а перемешивание служит для маскировки взаимосвязей между открытым текстом, шифротекстом и ключом. Интуитивно кажется понятным, что чем выше степень рассеивания и перемешивания, тем более надёжным будет алгоритм. Вполне возможно, что сложные алгоритмы как раз обеспечивают эту степень на должном уровне.

Чередование различных методов шифрования должно повысить стойкость алгоритмов к взлому. Многократность применения такого чередования тоже должна повысить стойкость. То же можно сказать и об увеличении длины блока (для блочных шифров) и ключа шифрования. Но в таком случае может понадобиться разбивать длинный блок на подблоки и ключ на подключи, а это уже модульная система, которая считается сложной для анализа и потенциально ненадёжной. А ненадёжной ли?

Увеличение длины блока, ключа и количества проходов шифрования могут заметно снизить скорость работы алгоритма. Даже если алгоритм действительно станет надёжнее, можно ли как-то оценить, оправдано ли такое увеличение надёжности уменьшением скорости? Впрочем, возможности современных процессоров в некоторых случаях позволяют игнорировать медленность некоторых алгоритмов.

Надёжность алгоритмов определяют иногда по наличию или отсутствию успешных атак на него. Но что считать успешной атакой? Для одних атакой является нахождение способа вскрытия за меньшее число операций, чем грубой силой, а для других — практическое вскрытие за приемлемое время [6]. Предположим, для вскрытия алгоритма А грубой силой понадобится 2^{256} операций, а для алгоритма Б — 2^{1024} . Для алгоритма А не найдено способов вскрыть его быстрее, а для алгоритма Б такой способ нашёлся (успешная атака?) и он требует 2^{800} операций. Разве от этого алгоритм Б стал менее надёжным по сравнению с алгоритмом А?

То есть, если отойти от строгой математической доказуемости, то надёжный алгоритм шифрования создать всё-таки можно. Скорее всего, для этого придётся увеличивать длину блока и размер ключа. Вероятно, придётся значительно увеличить количество проходов шифрования. Обязательно делать упор на увеличение степени рассеивания и перемешивания, и чем выше будет эта степень, тем лучше. Качество такого рассеивания и перемешивания нужно проверять на промежуточных этапах шифрования, и оно должно расти с каждым новым проходом.

Видимо, придётся смириться также с увеличением сложности алгоритма и снижением скорости его работы. В составных алгоритмах нужно оценивать отдельно каждый модуль, его взаимодействие с другими модулями и их общий эффект на степень упомянутых рассеивания и смешивания.

И в целом ориентироваться на защиту от практического вскрытия, а не от гипотетических атак, которые не приводят к реальному вскрытию шифра.

И несколько слов о потоковых шифрах. В алгоритмах подобного типа шифрование каждого отдельного бита, символа или байта производится независимо от других бит, символов или байт. Как в них добиваться рассеивания и перемешивания? Один из возможных вариантов — реализовать генератор потока ключей для такого алгоритма по тем же принципам, на которых строятся блочные шифры. Тогда в них тоже можно реализовать описанные выше подходы.

Литература

1. Гатченко Н.А., Исаев А.С., Яковлев А.Д. «Криптографическая защита информации» - СПб: НИУ ИТМО, 2012. - 142 с.
2. Введение в криптографию / Под общ. ред. В.В. Ященко. - 4-е изд., доп. М.: МЦНМО, 2012. - 348 с.
3. Абашев А.А., Жуков И.Ю., Иванов М.А., Метлицкий Ю.В., Тетерин И.И. Ассемблер в задачах защиты информации — М.: КУДИЦ-ОБРАЗ, 2004. - 544 с.
4. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Триумф, 2002. - 816 с.
5. Брассар Жиль. Современная криптология. Руководство — М.: Полимед, 1999. - 176 с.
6. Bruce Schneier. Crypto-Gram Newsletter [Электронный ресурс] URL: <https://www.schneier.com/crypto-gram/archives/2002/0915.html>

Анотація

Розглянуті загальноприйняті підходи побудови та оцінювання надійності криптографічних систем захисту інформації, що базуються на математичній доказовості. Показані деякі недоліки таких підходів. Представлені альтернативні підходи, не засновані на строгій математичній доказовості.

Ключові слова: кріптографія, інформація, розсіювання, перемішування.

Аннотация

Рассмотрены общепринятые подходы к построению и оценке надёжности криптографических систем защиты информации, основанные на математической доказуемости. Показаны некоторые недостатки таких подходов. Представлены альтернативные подходы, не основанные на строгой математической доказуемости.

Ключевые слова: криптография, информация, рассеивание, перемешивание.

Abstract

Common mathematically provable approaches to building and assessing the reliability of cryptographic information security systems considered. Some disadvantages of such approaches are shown. Alternative approaches, not based on strict mathematical provability, are presented.

Keywords: cryptography, information, diffusion, confusion.