

ОСОБЕННОСТИ РЕАЛИЗАЦИИ АЛГОРИТМОВ ЭЛЛИПТИЧЕСКОЙ КРИПТОГРАФИИ

Е.В. Горбунова, В.А. Липницкий

Среди современных систем защиты информации от несанкционированного доступа широкую популярность получили криптографические системы с открытым ключом. Первыми криптосистемами с открытым ключом, пригодными для шифрования и для цифровой подписи, стали криптосистемы RSA, Рабина, Эль-Гамала. Основу криптографической стойкости первых двух систем составляет сложность задачи факторизации натуральных чисел, а третьей — проблема дискретного логарифма. К их недостаткам следует отнести постоянно растущую длину ключей, связанную с развитием компьютерной техники. Специалисты в области кибербезопасности высказывают мнение о том, что названные системы находятся в опасности из-за возможного математического прогресса в решении задач, обеспечивающих их криптостойкость. Они советуют отказаться от существующих сертификатов и серьезно подумать об освоении новых криптографических систем. Наиболее приемлемыми для этого считают криптосистемы на основе эллиптических кривых.

Эллиптическая криптография стала возможной, благодаря разработанной в алгебраической геометрии стройной теории эллиптических кривых над произвольными полями, в частности, благодаря наличию на этих кривых структуры абелевой группы. Правда, реальное криптографическое применение получили эллиптические кривые над полями Галуа, особенно, над конечными полями характеристики два.

Основным преимуществом эллиптической криптографии является тот факт, что она обеспечивает эквивалентный уровень защиты данных при гораздо меньшей длине ключей по сравнению с криптосистемой RSA и ей подобными. Также, скорость работы эллиптических алгоритмов гораздо выше из-за небольших размеров используемых полей и благодаря структуре двоичного конечного поля, которая наиболее близка для компьютеров.

Авторами данного доклада создан банк алгоритмов для конкретной работы с эллиптическими криптосистемами. Среди них алгоритмы построения конечных полей, вычислений в них, алгоритмы нахождения точек суперсингулярных эллиптических кривых над конечными полями характеристики 2, алгоритмы криптографических протоколов на названных эллиптических кривых. В докладе рассматриваются индивидуальные особенности и достоинства перечисленных алгоритмов и их программных реализаций.

ОТСЛЕЖИВАНИЕ МАРШРУТА ПЕРЕМЕЩЕНИЙ ФАЙЛА МЕЖДУ КОМПЬЮТЕРАМИ ЛОКАЛЬНОЙ СЕТИ

А. К. Доронин

Задача отследить маршрут перемещений файла между компьютерами в локальной сети часто возникает при работе с документами. К примеру, необходимо узнать, где в данный момент находится файл, который должен передаваться по очереди. Без использования специальных дорогих программ, отслеживающих весь трафик локальной сети, решить данную задачу весьма сложно. В данной работе предложен метод, позволяющий добиться решения без использования значительных затрат с помощью альтернативных потоков данных.

Альтернативные потоки данных (далее — АПД) — это метаданные, связанные с объектом файловой системы NTFS. В NTFS файл, кроме основных данных, может быть связан с одним или несколькими АПД. Для составления маршрута перемещений файла между ПК можно отслеживать события изменения и создания файлов, и записывать имя текущего ПК в АПД файла, если последнее изменение происходило на другом ПК. После анализа такой истории составить полный маршрут перемещений файла между ПК несложно. Данный подход позволяет сохранять историю в файле при перемещении файла между ПК, так как АПД при передаче на NTFS остаются неизменными.

Для реализации метода необходимо разработать программы мониторинга и управления. Программа управления должна иметь функцию задания маски имен отслеживаемых файлов, а также функцию графического отображения маршрута перемещений. Модуль мониторинга должен устанавливаться на конечных ПК локальной сети и следить за изменениями целевых файлов по предложенной выше схеме.

Литература

1. *Алиев А.Т.* Разработка моделей, методов и алгоритмов перспективных средств защиты информации в системах электронного документооборота на базе современных технологий скрытой связи: дис. ... канд. техн. наук: 05.13.13/А. Т. Алиев; Ростов-на-Дону, 2008 – 216 с

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ БЕСПРОВОДНЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

А.П. Жук, А.А. Гавришев, В.А. Бурмистров

Сегодня в мире основными технологиями беспроводной передачи информации являются GSM, 3G, HSPA+/HSPA+ Advanced (4G), WiMAX, LTE (4G). В последнее время данные технологии активно внедряются во многие системы передачи информации, например в охранно-пожарные системы безопасности. Однако, в силу уязвимости беспроводного канала связи для несанкционированного доступа актуальным является вопрос обеспечения его защищенности. В настоящее время защищенность радиоканала, в основном, обеспечивается средствами криптографической защиты информации (СКЗИ). СКЗИ имеют следующие минусы: дороговизна, значительное время выполнения команд шифрования-расшифрования, изученность основных алгоритмов. Альтернативным методом защиты радиоканала является применение генераторов стохастических ортогональных сигналов [1], заключающимся в том, что для передачи сообщений, сменяемых от одного информационного символа к другому, предлагается использовать сформированные стохастическим образом ортогональные системы сигналов, описываемые собственными векторами диагональной симметрической матрицей A размерностью N . При этом используется свойство ортогональности собственных векторов, заключающееся в том, что собственные векторы, соответствующие различным собственным значениям нормального оператора, попарно ортогональны. Данный метод отличается увеличенным числом структур сигналов и уменьшенной вероятностью их раскрытия за счет расширения диапазона n возможных значений диагональных коэффициентов матрицы A .

Литература

1. *Жук А.П. и др.* Способ передачи информации на основе хаотически формируемых ансамблей дискретных многоуровневых сигналов / Патент РФ № 2428795, 10.09.2011.

ПРОТОКОЛОВ ЗАЩИТЫ ИНФОРМАЦИИ КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ ПРЯМЫХ

А.М. Захаревич

В последнее время все больше и больше внедряются в нашу повседневную жизнь информационные технологии, пытаясь захватить в ней все: от важнейших государственных проектов до решения обычных бытовых проблем. Вместе с огромной пользой и, казалось бы, неограниченными возможностями новые технологии приносят и новые проблемы. Одной из них является проблема защиты информации от несанкционированного посягательства теми, кто доступа к этой информации иметь не должен. В связи с этим почти одновременно с развитием информационных и компьютерных технологий начали развиваться и технологии защиты информации, развитие которых с некоторой точки зрения гораздо более критично, чем развитие непосредственно информационных технологий. Ведь с совершенствованием систем защиты, совершенствуются и методы взлома, обхода этих защит, что требует постоянного пересмотра и увеличения надежности защиты информации.

Практически любая "современная" криптосистема может быть "переложена" на эллиптические кривые, но не для всех схем это дает выигрыш в стойкости. Например, для