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-Гамаля. 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 находится 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 траффик 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.

Библиотека БГУИР