УДК 004.438

РЕАЛИЗАЦИЯ АЛГОРИТМОВ ШИФРОВАНИЯ С ОТКРЫТЫМ КЛЮЧОМ

Студент гр. 113116 П.В. Синцов,
канд. физ.-мат. наук, доцент И.В. Прусова, ассистент А.Б. Севрук

Белорусский национальный технический университет

Криптография сегодня – это важнейшая часть всех информационных систем: от электронной почты до сотовой связи, от доступа к сети Internet до электронной наличности. В последнее время она стала объектом широкомасштабных научных исследований. Одной из причин этого послужило большое число новых приложений в области защиты информации. Возможно, даже более важной причиной огромного роста научных исследований в криптографии явилась плодотворная идея криптографии с открытым ключом, создавшая новые перспективы и возможности в обмене информацией.

В настоящее время существует множество методов криптографической защиты с открытым ключом. Все эти алгоритмы медленны. Они шифруют и дешифрируют данные намного медленнее, чем симметричные алгоритмы. Однако алгоритмы на основе эллиптических кривых потенциально могут послужить основой для более быстрых криптосистем с открытыми ключами и меньшими размерами ключей. Тем не менее, их скорость недостаточна для шифрования больших объемов данных. Поэтому асимметричные алгоритмы обычно используются в асимметричных криптосистемах для шифрования симметричных сеансовых ключей, которые используются для шифрования самих данных.

Наиболее простой критерий такой эффективности – вероятность раскрытия ключа или мощность множества ключей (M). По сути это то же самое, что и криптостойкость. Для ее численной оценки можно использовать также и сложность раскрытия шифра путем перебора всех ключей. Однако этот критерий не учитывает других важных требований к криптосистемам:

- невозможность раскрытия или осмысленной модификации информации на основе анализа ее структуры,
- совершенство используемых протоколов защиты,
- минимальный объем используемой ключевой информации,
- минимальная сложность реализации (в количестве машинных операций), ее стоимость,
- высокая оперативность.