УДК 004.056

РЕАЛИЗАЦИЯ АЛГОРИТМОВ ШИФРОВАНИЯ С ОТКРЫТЫМ КЛЮЧОМ

Студент гр.113228 Синицын И.Г.,
кандидат физ.-мат. наук, доцент Прусова И.В., доцент Буснюк Н.Н.
Белорусский национальный технический университет

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом волновала человеческий ум с давних времен. Эта проблема является предметом изучения такой науки как криптология. Криптология разделяется на два направления – криптографию и криптоанализ. Криптография занимается поиском и исследованием математических методов преобразования информации. Сфера интересов криптоанализа – исследование возможности расшифровывания информации без знания ключей.

Как бы ни были сложны и надежны криптографические системы – их слабое место при практической реализации – проблема распределения ключей. Для того, чтобы был возможен обмен конфиденциальной информацией между двумя субъектами информационной системы, ключ должен быть сгенерирован одним из них, а затем каким-то образом опять же в конфиденциальном порядке передан другому. Наиболее широко используемой и проверенной криптосистемой с открытым ключом является система RSA, придуманная в 1977 году и получившая название в честь ее создателей: Рона Ривеста, Ади Шамира и Леонарда Эйдельмана (Rivest, Shamir, Adleman). Она основана на удивительно простой теоретико-числовой идее и еще в состоянии сопротивляться всем крипто-аналитическим атакам. Идея состоит в искусном использовании того факта, что легко перемножить два больших простых числа, однако крайне трудно разложить на множители их произведение. Возможность гарантированно оценить защищенность алгоритма RSA стала одной из причин популярности этой системы с открытым ключом на фоне десятков других схем. Поэтому алгоритм RSA используется в банковских компьютерных сетях, особенно для работы с удаленными клиентами (обслуживание кредитных карточек).

В работе сделан обзор наиболее распространенных в настоящее время методов криптографической защиты с открытым ключом и разработано приложение для шифрования текста с помощью алгоритма шифрования с открытым ключом RSA в визуальной среде разработки приложений Borland Delphi 7. Тем не менее её 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).