УДК 004.056.55+ 003.26

Программный модуль эллиптической криптографии для лабораторных работ

Автор: *О.В. Полищук, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев*

Научный руководитель: *О.А. Щелконогов, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев*

Целью работы являлось создание программного модуля для лабораторного практикума по криптологии на основе эллиптической криптографии.

Актуальность темы продиктована тем, что в учебном пособии [1], которое является основным при проведении лабораторного практикума по предмету «Основы криптографии и криптоанализа» отсутствуют работы, связанные с использованием эллиптических кривых в криптографии. А в настоящее время это одно из самых развивающихся направлений: новые стандарты многих стран по шифрованию и цифровой подписи, в т.ч. Украины (ДСТУ 4145-2002) и России [2], основаны на использовании эллиптических кривых.

Многие широко известные алгоритмы несимметричной криптографии были переведены на использование операций с точками эллиптических кривых. Наиболее существенный выигрыш при этом достигается за счет уменьшения длины ключа при соизмеримой криптостойкости.

В криптографии эллиптические кривые рассматриваются над двумя типами конечных полей: простыми полями нечётной характеристики ($GF(p)$, где $p > 3$ – простое число) и полями характеристики 2. В данной работе рассматривается эллиптическая криптография над простыми полями нечетной характеристики.

Выводы. В работе были рассмотрены основные моменты теории эллиптических кривых применительно к криптографии, изучены основные алгоритмы шифрования, цифровой подписи и распределения ключей. Были созданы рабочие модели этих алгоритмов в среде MathCad и разработаны методические указания для лабораторных работ с целью использования их в учебном процессе по предмету «Основы теории криптографии и криптоанализа» для специальности 6.17010201.

Список литературы:

1. Блінцов В.С. Гальчевський Ю.Л. Практикум з криптології: Навчальний посібник. – Миколаїв: НУК, 2005. – 172 с.

2. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи [Электронный ресурс] – Режим доступа: http://www.gosthelp.ru/gost/gost6784.html.