УДК 004.056.2 + 004.056.55

РАЗРАБОТКА ПАРАЛЛЕЛЬНЫХ АЛГОРИТМОВ ДЛЯ ПРОГРАММНОЙ РЕАЛИЗАЦИИ СИСТЕМЫ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

В.А. УРСУЛ [1*], ***О.Н. МАЛЫХ*** [2]

[1] *магистрант кафедры Системного анализа и информационно-аналитических технологий, НТУ «ХПИ», Харьков, УКРАИНА*

[2] *доцент кафедры Системного анализа и информационно-аналитических технологий НТУ «ХПИ», Харьков, УКРАИНА*

[*] *email: stricx.mt@gmail.com*

В наше время всемирной сетью Internet пользуется практически каждый. Согласно сервису Internet Live Stats, каждую секунду в Google делается более 50 000 поисковых запросов, отправляется почти 2,5 млн электронных писем. Большая часть данных является конфиденциальной, и следовательно, передача их по сети должна быть безопасной. В этом случае на помощь приходят криптографические протоколы, которые позволяют скрыть передаваемую информацию от третьих лиц.

Актуальность и важность проблемы защиты информации можно описать следующими факторами [1]:

1. За последние годы вычислительная мощность и доступность компьютеров, смартфонов и других гаджетов резко увеличилась.
2. Многократно увеличился объем информации, которая хранится и обрабатывается с помощью компьютеров и других средств автоматизации.
3. Развитие всемирной сети Internet, способствует нарушению безопасности систем обработки информации по всему миру.

Таким образом, криптография позволяет решить следующие основные задачи:

1. Обмен информацией с последующей установкой защищенного соединения между каналами передачи данных.
2. Аутентификация и авторизация сторон, которые устанавливают связь.

Целью работы является разработка параллельных алгоритмов для программной реализации системы криптографических преобразований.

Для достижения поставленной цели была обеспечена возможность шифрования и дешифрования данных с помощью криптосистемы *DES*. Также были реализованы методы формирования электронной цифровой подписи – *MAC* и *MD5*. Программное обеспечение было написано на языке программирования *C#*. Разработанное приложение имеет интуитивно понятный интерфейс пользователя.

Список литературы:

1. *Столлингс, В.* Криптография и защита сетей. Принципы и практика / *В. Столлингс* // М.: И.Д.Вильямс. – 2001. – С. 672.