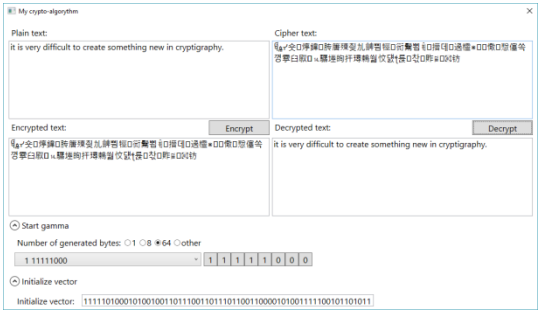
УДК 004.056.55

Блочная система шифрования RSK

Несенчук А.А., Стухальский А.Л., Романенко Р.А.
Белорусский национальный технический университет

Цель работы состоит в создании собственной улучшенной криптосистемы. Основными задачами являются: 1) анализ преимуществ и недостатков существующих криптосистем; 2) решение обнаруженных проблем существующих алгоритмов; 3) создание приложения, реализующего разработанную концепцию.

Программа реализована на C++ и C#. Пользовательский интерфейс (рисунок) разработан с помощью фреймворка стандартных компонент. Вариант программы на C++ в разы быстрее чем на C#.



Интерфейс приложения, реализующего алгоритм шифрования RSK

Разработанный алгоритм шифрования имеет пропускную способность 2,5 гигабайта в секунду (Измерения производились на процессоре Intel Core i5-U 2.5 ГГц с ОЗУ DDR3 1600 МГц.), что превосходит AES [1] примерно в 3 раза. Значительный прирост в скорости связан с преобразованием одного выбранного блока, а не набора блоков, которые могут находиться в памяти далеко друг от друга. Повышение криптостойкости связано с использованием нескольких уровней защиты, а не множественного повтора одних и тех же процедур.

Литература

Hardware AES Showdown [Электронный ресурс] / grantmcwilliams.com. – 6.7.2011 г. – Режим доступа: http://grantmcwilliams.com/tech/technology/387-hardware-aes-showdown-via-padlock-vs-intel-aes-ni-vs-amd-hexacore. – Дата доступа: 1.5.2017.