ПРОГРАММНАЯ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ ЗАЩИТЫ ИНФОРМАЦИИ НА ТРАНСПОРТЕ

***А. Н. ДАНИЛЬЧЕНКО*, П. М. БУЙ**

The results of research of various algorithms on speed of enciphering and decoding are resulted. The developed program can be used for demonstration of job криптографических of algorithms during training

Ключевые слова: криптография, криптоанализ, шифр, шифрование, дешифрование, криптостойкость, алгоритм, время полного перебора

В современном мире информация имеет большую ценность и поэтому возникает необходимость надежного хранения и возможность передачи по открытым каналам связи. С этой задачей хорошо справляется криптография. Под криптографической защитой информации понимается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий.

Для сравнительных исследований криптографических алгоритмов была разработана программа.

На рисунке 1 представлены результаты исследований скорости шифрования и дешифрования стандартных информационных блоков с помощью криптографических алгоритмов. Для сравнения были выбраны криптографические алгоритмы DES (и его варианты), AES, RSA с различными длинами ключей. Тестирование проводилось на компьютере с процессором Intel Pentium D CPU 915 2.80 ГГц.

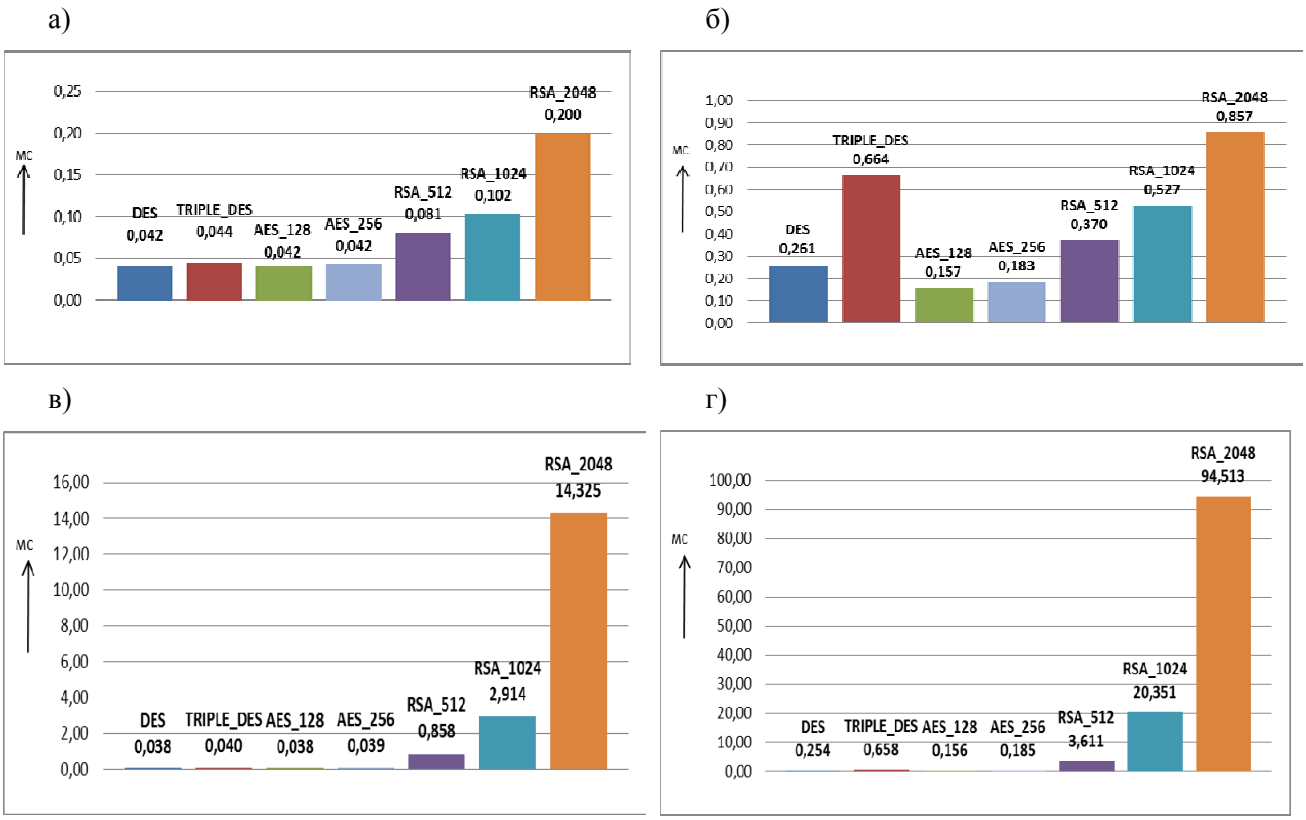

Рисунок 1 – Результаты исследований скорости шифрования и дешифрования
а) – шифрование 16 байт данных; *б*) – дешифрование 16 байт данных;
в) – шифрование 8 кбайт данных; *г*) – дешифрование 8 кбайт данных

Как видно из результатов исследования самым быстрым криптографическим алгоритмом из рассмотренных является DES, но в то же время DES имеет наименьшую криптостойкость. Самым медленным является RSA, так как в его алгоритме происходит оперирование большими числами.