УЧЕБНАЯ ПРОГРАММА ШИФРОВАНИЯ НА ОСНОВЕ АЛГОРИТМА РАБИНА

И.В. ШАЛИМОВ, В.П. БУРЦЕВА

В современном мире проблема сокрытия информации становится все более и более актуальной. В связи с этим возник спрос на надежные алгоритмы шифрования, к которым относится криптосистема Рабина.

Целью данной работы является: создание учебной программы шифрования, в основе которой лежит алгоритм Рабина; анализ криптосистемы; выявление её плюсов и минусов; оценка стабильности алгоритма, скоростей шифровки, расшифровки и взлома сообщений; сравнение алгоритма Рабина с аналогичными системами шифрования по открытому ключу (RSA, El-Gomal); определение области применения данного алгоритма. Взлом сообщений осуществлялся методом подбора закрытого ключа. Оптимизация подбора закрытого ключа проводилась с помощью решета Сундарама. Программа создана для внедрения в учебный процесс.