КРИПТОГРАФИЧЕСКАЯ СИСТЕМА ШИФРОВАНИЯ МЕТОДОМ КАРДАНО

А.С. Куликовский, В.П. Бурцева

Данная работа посвящена исследованию шифра Кардано и созданию программы для шифрования этим методом в учебных целях и направлена на то, чтобы продемонстрировать современные информационные технологии, позволяющие защитить пользовательскую информацию от несанкционированного доступа при минимальных временных затратах в процессе шифрования. В ходе проекта рассмотрен механизм работы данного метода. Разработана программа для шифрования, дешифрования и взлома сообщений. При этом для оптимизации взлома зашифрованного сообщения использовался метод дихотомии. Проведена оценка криптографической устойчивости алгоритма и рассчитаны скорости шифрования и дешифрования сообщений. Проанализированы достоинства и недостатки именно этого метода шифрования, что дает возможность прогнозировать развитие шифрования в будущем, в частности, при создании нового класса квантовых компьютеров.