Крипта

Курсовой проект

-взлом подстановки индивидуальный

-атака фридмана индивидуально

-разработка и обоснование стойкости блочного многораундового симметричного алгоритма шифрования\расшифрования на основе криптограф. Примитивов:

1 подстановка над алфавитом ascii

2 перестановка размер блока

3 гаммировани

Существует алгоритм машины тьюринга решающий задачу при любых исходных данных