

ЗАДАНИЕ 1.

1. Шифр замены (код Цезаря)

Генерация ключа.

Вход: файл алфавита alphabet.txt.

Выход: файл ключа key.txt (случайная перестановка входного алфавита).

Шифрование.

Вход: файл ключа key.txt, файл открытого текста open.txt.

Выход: файл шифротекста: encrypted.txt

Расшифрование:

Вход: файл ключа key.txt, файл шифротекста: encrypted.txt.

Выход: файл открытого текста: decrypted.txt

Все операции должны вызываться независимо друг от друга.

2. Шифр замены (квадрат Полибия)

Генерация ключа.

Вход: файл алфавита alphabet.txt, записанный в виде прямоугольной матрицы.

Выход: файл ключа key.txt (случайная перестановка строк и столбцов входной матрицы).

Шифрование.

Вход: файл ключа key.txt, файл открытого текста open.txt.

Выход: файл шифротекста: encrypted.txt (Каждую букву шифровать парой чисел: строка, столбец).

Расшифрование:

Вход: файл ключа key.txt, файл шифротекста: encrypted.txt.

Выход: файл открытого текста: decrypted.txt

Все операции должны вызываться независимо друг от друга.

3. Парный шифр

Генерация ключа.

Вход: файл алфавита alphabet.txt (четное число символом) и файл с произвольной фразой на этом алфавите password.txt.

Выход: файл ключа key.txt (сначала выбирают все буквы из фразы без повторов в порядке по первому вхождению во фразу. Если остались буквы из алфавита, то они дописываются в алфавитном порядке. Затем эта перестановка алфавита делится пополам и вторая половина подписывается под первой).

Шифрование.

Вход: файл ключа key.txt, файл открытого текста open.txt.

Выход: файл шифротекста: encrypted.txt (Каждую букву шифровать её парной из верхней или нижней строки ключа).

Расшифрование:

Вход: файл ключа key.txt, файл шифротекста: encrypted.txt.

Выход: файл открытого текста: decrypted.txt

Все операции должны вызываться независимо друг от друга.