ЗАДАНИЕ 1 Тест Казиски:

1. Реализовать шифр простой перестановки на основе генерации ключа моноциклической перестановки.
2. Реализовать тест Казиски по вычислению длины ключа простой перестановки (программа выявления одинаковых участков криптограммы, вычисления расстояния между соседними такими участками (от первого символа до первого), и вычисления НОД этих расстояний).
3. Программа перебора ключей моноциклической перестановки при известной длине ключа.

ЗАДАНИЕ 2 Анализ Фридмана:

1. Вход: две последовательности букв одной и той же длины:

$$y = (y_0, y_1, \ldots, y_{N-1})$$
$$z = (z_0, z_1, \ldots, z_{N-1})$$

Выход: Индекс совпадения:

$$I(y, z) = \frac{1}{N} \sum_{i=0}^{N-1} \delta(y_i, z_i), \text{ где } \delta(y_i, z_i) = \begin{cases} 1 & (y_i = z_i) \\ 0 & (y_i \neq z_i) \end{cases},$$

Используя эту программу провести сравнительный анализ значений индексов совпадения для случайных последовательностей, для последовательностей английского языка, для последовательностей русского языка.

Результаты исследования внести в таблицу следующего вида:

	$I(y, z) \times 100$ случ	$I(y, z) \times 100$ англ	$I(y, z) \times 100$ рус
Пример 1			
Пример 2			
Пример 3			
Пример 4			

2. Вход: две последовательности букв одной и той же длины:

$$y = (y_0, y_1, \ldots, y_{N-1})$$
$$z = (z_0, z_1, \ldots, z_{N-1})$$

Выход: Средний Индекс совпадения: $I_{ср}(y, z) = \sum_{i=0}^{25} p_i^y p_i^z$ для английского языка,

где буквы алфавита обозначены индексом от 0 до 25 по алфавиту.

При этом $p_i^y = \frac{\text{число символов } i \text{ в } y}{N}$, $p_i^z = \frac{\text{число символов } i \text{ в } z}{N}$.

По работе программы провести сравнительный анализ значений индексов совпадения для случайных последовательностей, для последовательностей английского языка, для последовательностей русского языка.

Результаты исследования внести в таблицу следующего вида:

	$I_{ср}(y, z) \times 100$ случ	$I_{ср}(y, z) \times 100$ англ	$I(y, z) \times 100$ рус
Пример 1			
Пример 2			
Пример 3			
Пример 4			

3. Реализовать шифр Виженера с выбором файла алфавита и файла ключа длины k. Пусть $y = (y_0, y_1, y_2, \ldots)$ шифрограмма или открытый текст. Для положительного целого числа l пусть

$$y^{(+l)} = (y_l, y_{l+1}, y_{l+2}, \ldots).$$

Т.е. $y^{(+l)}$ есть сообщение, полученное из y сдвигом вперёд на l символов. Используя программу из 1 и 2 провести сравнительный анализ значений индексов совпадения:

l сдвиг	$I(y, y^{(+l)})\times 100$ для открытого	$I(y, y^{(+l)}) \times 100$ для шифрограммы при $k = 5$	$I(y, y^{(+l)}) \times 100$ для шифрограммы при $k = 7$
1			
2			
…			
15			

fb.com/FacultyCSaIT/
https://drive.google.com/open?id=0B2AKc7ibPQ_WdEVSX1dNX0pGOEk