ЗАДАНИЕ 3 Анализ шифра перестановки при известной длине периода:

1. Вычисление множества запретных биграмм языка открытых сообщений.
   Вход: файл с большим текстом на языке открытых сообщений.
   Выход: файл алфавита; файл запретных биграмм.
2. Построение вспомогательной таблицы для анализа шифра перестановки при известной длине периода:
   Вход: длина периода k; файл шифрограммы перестановки.
   Выход: файл вспомогательной таблицы.
3. Построение ориентированного леса возможных перестановок.
   Вход: файл вспомогательной таблицы.
   Выход: файл ориентированного леса возможных перестановок.
4. Перебор ключей по ориентированному лесу возможных перестановок.
   Вход: файл ориентированного леса возможных перестановок; файл шифрограммы.
   Выход: файл походящего ключа.

ЗАДАНИЕ 4 Анализ шифра простой подстановки:

1. Реализовать шифр простой подстановки.
   Генерация ключа:
   Вход: файл алфавита.
   Выход: Подстановка этого алфавита или номер сдвига этого алфавита.
   Шифрование:
   Вход: файл алфавита, файл ключа, файл открытого текста.
   Выход:; файл шифрограммы.
2. Частотный анализ:
   1) Создание таблицы частот символов языка открытых сообщений:
   Вход: файл большого текста на языке открытых сообщений.
   Выход: файл частот символов в этом тексте в убывающем порядке.
   2) Создание таблицы частот символов в криптограмме
   Вход: файл криптограммы.
   Выход: файл частот символов в этой криптограмме в убывающем порядке.
   3) Создание списка изотонных отображений между алфавитами открытых сообщений и криптограммы.
   4) Проверка этого списка ключей на криптограмме.

ЗАДАНИЕ 5 Анализ шифра Виженера при известной длине ключа:

1. Атака по частотному анализу.
   1.1) Вычисление таблицы частот языка открытых сообщений.
   Вход: файл большого текста на языке открытых сообщений.
   Выход: файл алфавита со значениями частот в порядке их убывания.
   1.2) Вычисление ключа шифра Виженера при известной длине ключа.
   Вход: файл шифрограммы, файл алфавита со значениями частот, длина ключа.
   Выход: Список наиболее вероятных ключей и расшифрованной ими шифрограммы.
2. Атака по вероятному слову:

2.1) Вычисление таблицы наиболее частых слов в языке открытых сообщений.
Вход: файл большого текста на языке открытых сообщений.
Выход: Файл словаря наиболее частых слов.

2.2) Вычисление ключа шифра Виженере при известной длине ключа.
Вход: файл шифрограммы; файл словаря наиболее частых слов; длина ключа.
Выход: список вариантов расшифрованной криптограммы при проведении вероятного слова (наиболее частого слова).

ЗАДАНИЕ 6 Статистический метод вычисления периода длины гаммы:

1. Вычисление значений гипотезы H(0).

Вход: файл большого текста на языке открытых сообщений.
Выход: файл алфавита со значениями частот в порядке убывания частот ($a_1 = p_1$, $a_2 = p_2, \ldots, a_m = p_m$, где m – длина алфавита); файл со значениями гипотезы H(0):

$$P_j = \sum_{i-k=j(\mathrm{mod}\, m)} p_i p_k \text{ , т.е. файл вида:}$$

$P_0 = \ldots$
$P_1 = \ldots$
$\ldots$
$P_{m-1} = \ldots$

2. Вычисление значений гипотезы H(d) с наиболее вероятной длиной периода d.

Вход: 1) файл криптограммы $Y = y_1 y_2 \ldots y_N$ (например, шифра Виженера) над алфавитом открытых сообщений (т.е. над алфавитом из пункта 1).
2) Два натуральных числа n_1, n_2: $n_1 < n_2$.
3) Файл со значениями гипотезы H(0).

ЗАДАЧА: Пусть y_i — это не сам символ, а его номер в алфавите в естественном порядке от 0 до $m - 1$. Для каждого натурального d ($n_1 \le d \le n_2$) строим последовательность $Z = z_1 z_2 \ldots z_{(t-1)d+r}$, где

$$z_1 = y_1 - y_{1+d},$$
$$z_2 = y_2 - y_{2+d},$$
$$\ldots$$
$$z_j = y_j - y_{j+d},$$
$$\ldots$$
$$z_{(t-1)d+r} = y_{(t-1)d+r} - y_{td+r},$$

где $N = td + r$, $0 \le r < d$ (по теореме о делении с остатком).
Ясно, что $z_i \in \{0, \ldots, m-1\}$. Вычисляем вектор частот в последовательности Z:

P^Z_0 = частота 0 в Z,
P^Z_1 = частота 1 в Z,
$\ldots$
P^Z_{m-1} = частота $m - 1$ в Z,

т.е. значение гипотезы H(d).
Среди H(d), $n_1 \le d \le n_2$, выбрать самые близкие к H(0): $P_0, P_1, \ldots, P_{m-1}$.
Выход: H(d) (оптимальные).
https://drive.google.com/open?id=0B2AKc7ibPQ_WVmNMZkR5YUFtX2M