Мета роботи: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера

Постановка задачі:

1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта)

Текст був згенерований у генераторі текста за посиланням https://fish-text.ru та збережений у файлі text.txt. Зміст файлу був відредагований.

Було вибрано такі ключі для шифрування: «МЫ», «ПЕС», «МАЗУТ», «ИНДЕКСАЦИЯ», ШТ були збережені в такі файли типу key_<*назва ключа*>.txt

Далі були пораховані індекси відповідності:

```
key_МЫ.txt
key -  МЫ  | length -  2  | affinity index -  0.04050376756491047
key_ПЕС.txt
key -  ПЕС  | length -  3  | affinity index -  0.03751657559056042
key_РЫБА.txt
key -  РЫБА  | length -  4  | affinity index -  0.03631961259079903
key_МАЗУТ.txt
key -  МАЗУТ  | length -  5  | affinity index -  0.03412648430583318
key_ИНДЕКСАЦИЯ.txt
key -  ИНДЕКСАЦИЯ  | length -  10  | affinity index -  0.035281723105167154
```

Індекси відповідності для значень r

Далі потрібно розшифрувати файл encrypted:

1) Знаходемо ймовірну довжину ключа. Для цього ми ділимо на сегменти ШТ та знаходимо для кожно сегмента індекс відповідності. Після цього знаходимо середнє арифметичне ІВ і порвівнюєм його з теоритичним значенням 0.0553

```
most probable length
[0.05528168514213951, 14]
```

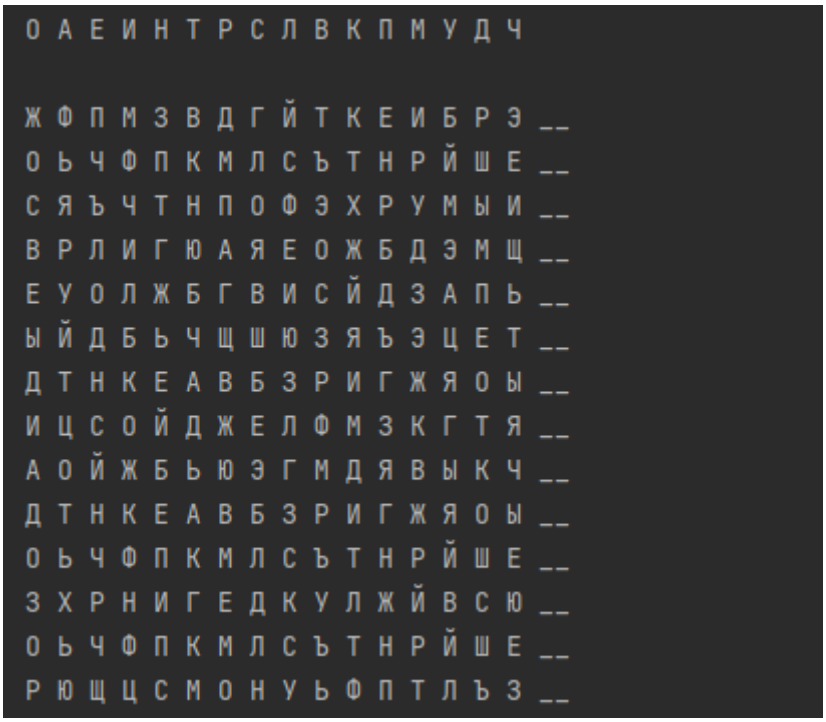
2) Далі виберимо найбільш вживані літери

```
popular = ["О", "А", "Е", "И", "Н", "Т", "Р", "С", "Л", "В", "К", "П", "М", "У", "Д", "Ч"]
```

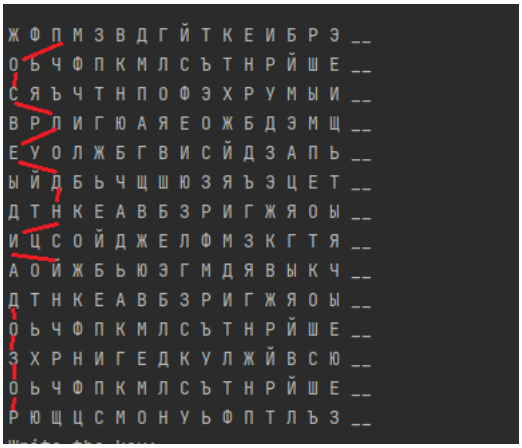
3) Для кожної із літери створимо стовпчик з 14 елементів. Цей стовпчик – це результат формули

$$k = (y^* - x^*) \bmod m,$$

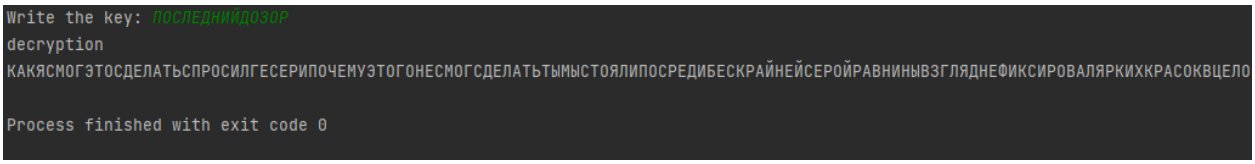
Найшовши індекс найбільш вживану літеру для кожного із сегментів(а їх 14, так як довжина ключа 14), я вставив індекси найбільш вживаних букв в російські мові. Оримав табличку



З цієї таблички треба вибрати з кожного рядка по 1 букві, щоб знайти ключ



Ключ – ПОСЛЕДНИЙДОЗОР



Текст розшифровано

Висновки: Під час виконання даної роботи я вивчила принципи шифру Віженера, я ознайомився з частотним аналізом, індексом відповідності та як працює шифр Віженера. Я навчився автоматизовувати процес розшифрування завдяки мови програмування