**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 <a href="https://fish-text.ru">https://fish-text.ru</a> 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_MЫ.txt
key - MЫ | length - 2 | affinity index - 0.04050376756491047

key_ПЕС.txt
key - ПЕС | length - 3 | affinity index - 0.03751657559056042

key_PЫБА.txt
key - PЫБА | length - 4 | affinity index - 0.03631961259079903

key_MA3YT.txt
key - MA3YT | length - 5 | affinity index - 0.03412648430583318

key_UHДЕКСАЦИЯ.txt
key - ИНДЕКСАЦИЯ | length - 10 | affinity index - 0.035281723105167154
```

Індекси відповідності для значень г

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 = ["0", "A", "E", "N", "H", "T", "P", "C", "Л", "B", "K", "П", "М", "У", "Д", "Ч"]
```

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

$$k = (y^* - x^*) \operatorname{mod} m,$$

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

```
ЖФПМЗВДГЙТКЕИБРЭ __
ОЬЧФПКМЛСЪТНРЙШЕ __
СЯЪЧТНПОФЭХРУМЫИ __
ВРЛИГЮАЯЕОЖБДЭМЩ __
ЕУОЛЖБГВИСЙДЗАПЬ __
ЫЙДБЬЧЩШЮЗЯЪЭЦЕТ __
ДТНКЕАВБЗРИГЖЯОЫ __
ИЦСОЙДЖЕЛФМЗКГТЯ __
ДТНКЕАВБЗРИГЖЯОЫ __
ДТНКЕАВБЗРИГЖЯОЫ __
ДТНКЕАВБЗРИГЖЯОЫ __
ДТНКЕАВБЗРИГЖЯОЫ __
ДТНКЕАВБЗРИГЖЯОЫ __
ОЬЧФПКМЛСЪТНРЙШЕ __
ЭХРНИГЕДКУЛЖЙВСЮ __
ОЬЧФПКМЛСЪТНРЙШЕ __
РЮЩЦСМОНУЬФПТЛЪЗ __
```

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

```
Ж Ф П М З В Д Г Й Т К Е И Б Р Э __

О Б Ч Ф П К М Л С Ъ Т Н Р Й Ш Е __

С Я Ъ Ч Т Н П О Ф Э Х Р У М Ы И __

В Р Л И Г Ю А Я Е О Ж Б Д Э М Щ __

Е У О Л Ж Б Г В И С Й Д З А П Ь __

Ы Й Д Б Ь Ч Щ Ш Ю З Я Ъ Э Ц Е Т __

Д Т Н К Е А В Б З Р И Г Ж Я О Ы __

И Ц С О Й Д Ж Е Л Ф М З К Г Т Я __

А О Й Ж Б Ь Ю Э Г М Д Я В Ы К Ч __

Д Т Н К Е А В Б З Р И Г Ж Я О Ы __

Д Т Н К Е А В Б З Р И Г Ж Я О Ы __

З Х Р Н И Г Е Д К У Л Ж Й В С Ю __

О Ь Ч Ф П К М Л С Ъ Т Н Р Й Ш Е __

Р Ю Щ Ц С М О Н У Ь Ф П Т Л Ъ З __
```

## Ключ – ПОСЛЕДНИЙДОЗОР

```
Write the key: ПОСЛЕДНИИДОЗОР
decryption
КАКЯСМОГЭТОСДЕЛАТЬСПРОСИЛГЕСЕРИПОЧЕМУЭТОГОНЕСМОГСДЕЛАТЬТЫМЫСТОЯЛИПОСРЕДИБЕСКРАЙНЕЙСЕРОЙРАВНИНЫВЗГЛЯДНЕФИКСИРОВАЛЯРКИХКРАСОКВЦЕЛО
Process finished with exit code 0
```

## 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