Task 1, 2

Intro

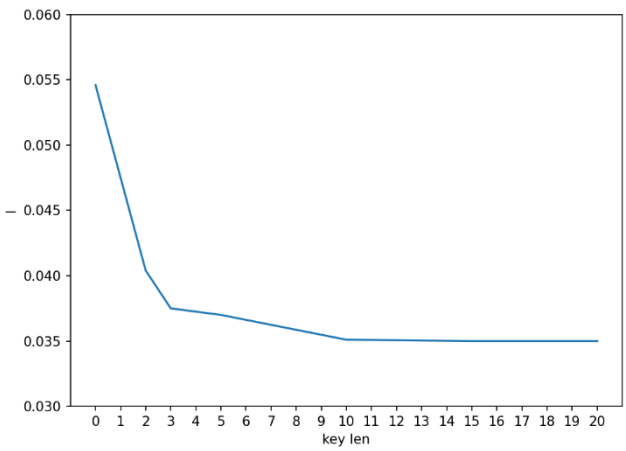
Текст для шифрування – шматок перекладу книги “Mein Kampf” на 1500 символів.

Ключі шифрування утворені з перших `[2, 3, 5, 10, 15, 20]` символів `"уйдиизмоейдиректории"`.

Індекси відповідності

I відкритого тексту і зашифрованих помітно відрізняються. I зашифрованого тексту прямує до $\frac{1}{32}$, що відповідає мові з рівномірним алфавітом (кожна літера має однакову частоту).

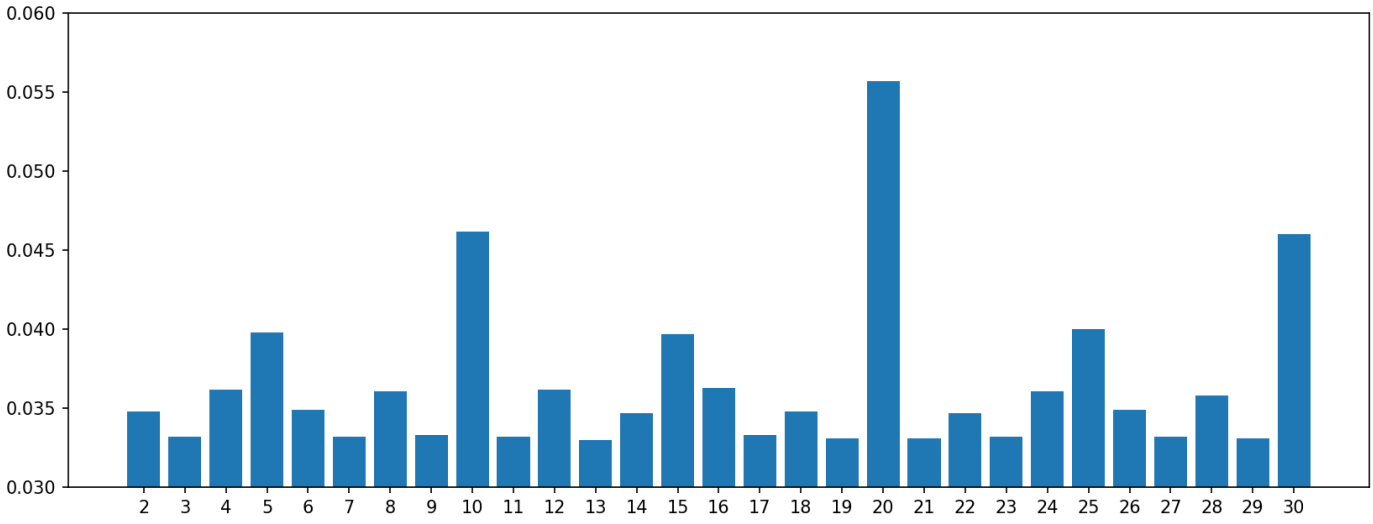
```
open text, I = 0.0546
key_len = 2, I = 0.0404
key_len = 3, I = 0.0375
key_len = 5, I = 0.037
key_len = 10, I = 0.0351
key_len = 15, I = 0.035
key_len = 20, I = 0.035
```



Task 3

Знаходження довжини ключа

I для кожного $r \in [2; 30]$ рахувалось як середнє I його блоків.




```
{20: 0.0557, 10: 0.0462, 30: 0.046, 25: 0.04, 5: 0.0398, 15: 0.0397,
16: 0.0363, 4: 0.0362, 12: 0.0362, 8: 0.0361, 24: 0.0361, 28: 0.0358}
```

(r, у яких $I \in [0.035; 0.06]$ і відсортовано за спаданням)

Видно, що для $r = 20$ значення I найбільш наближене до "природнього " 0.055 з пунктів 1-2.

Знаходження найпоширеніших літер у блоках

Отже, довжина ключа = 20, тож можна розбити ШТ на блоки і рахувати частоти.

```
б: 0.1107
щ: 0.1107
о: 0.0977
ы: 0.1498
ь: 0.1336
п: 0.0912
я: 0.1336
у: 0.1075
ю: 0.1498
у: 0.0977
п: 0.1107
х: 0.0945
н: 0.1238
ы: 0.1075
й: 0.1173
у: 0.1107
э: 0.1498
б: 0.1075
щ: 0.1046
н: 0.1078
```

Найпоширеніші літери відкритих текстів, визначено в попередній лабі

```
letters - without ' '
'о'   0.1122104632  151959
'е'   0.0867052322  117419
'и'   0.0805290379  109055
'а'   0.072554038   98255
'н'   0.0713843714  96671
'т'   0.0668157302  90484
'с'   0.0585025313  79226
'р'   0.0489029945  66226
'в'   0.0465584922  63051
'л'   0.0370099067  50120
```

Далі шукаю ключ-літеру для кожного блока і виходить ключ **улановсеребряныепули**

Шматок (500 символів) розшифрованого тексту виглядає так:

Эта система красного карлика никогда не имела названия только зубодробительно длинный номер в каталоге исследовавший ее киберзонд отметил наличие трех газовых гигантов двух астероидных полей кометного облака и занес все эти данные в сектор второй очереди по мнению инка киберзонда система не представляла никакой ценности для пославших его людей наверное будь у него задействованы контуры второго уровня самостоятельности и азарта он бы поспорил сам с собой что в ближайшую тысячу лет люди здесь не появятся и проспорил бы люди появились в этой системе не через тысячу лет а всего лишь чер …