Міністерство освіти і науки України
Національний технічний університет україни
"київський політехнічний інститут імені ігоря сікорського"
Фізико-технічний інститут

Криптографія
Комп’ютерний практикум №3
Криптоаналіз афінної біграмної підстановки

Виконали:
Студенти гр. ФБ-11
Поліщук Олександра
Маленко Сергій
3 варіант

Мета роботи: Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Порядок виконання роботи:

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.

Функції розширеного алгоритму Евкліда та розв'язку лінійних рівнянь містяться у **linear.py.**

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом). Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).

З першої лабораторної роботи ми взяли найчастіші біграми та їх відповідні значення:

```
7   BIGRAMS_FREQUENCY_OPEN_TEXT = {'ст': 0.01811,
8                                  'ни': 0.01727,
9                                  'то': 0.01631,
10                                 'пр': 0.01376,
11                                 'ос': 0.01336,
12                                 'ра': 0.01295,
13                                 'но': 0.01255,
14                                 'ко': 0.01168,
15                                 'по': 0.01102,
16                                 'ен': 0.01075}
```

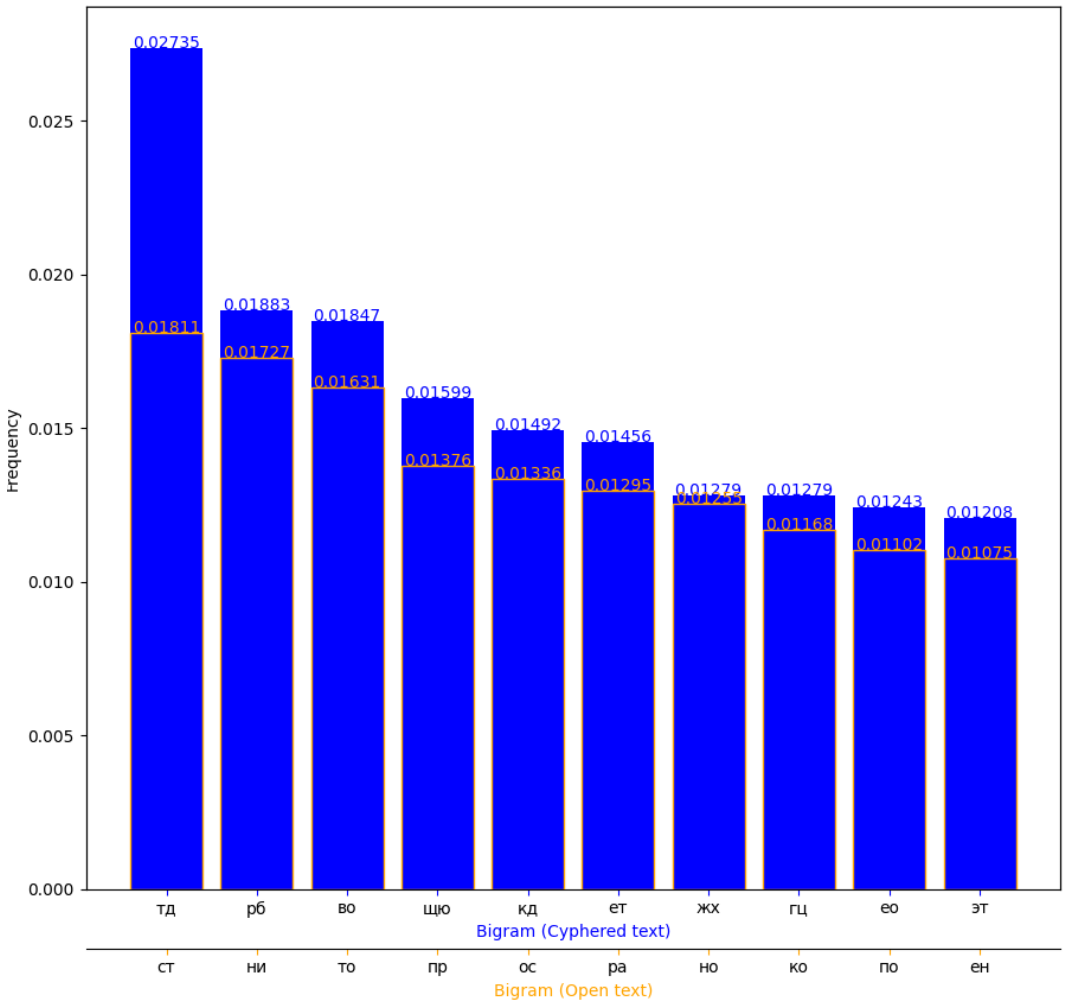
Також задля подальшої роботи, окремий масив містить неможливі біграми.

```
17  IMPOSSIBLE_BIGRAMS = ['аы', 'оы', 'иы', 'ыы', 'уы', 'еы', 'аь', 'оь', 'иь', 'ыь', 'уь', 'еь',
    'юы', 'яы', 'эы', 'юь', 'яь', 'эь', 'ць', 'хь', 'кь']
```

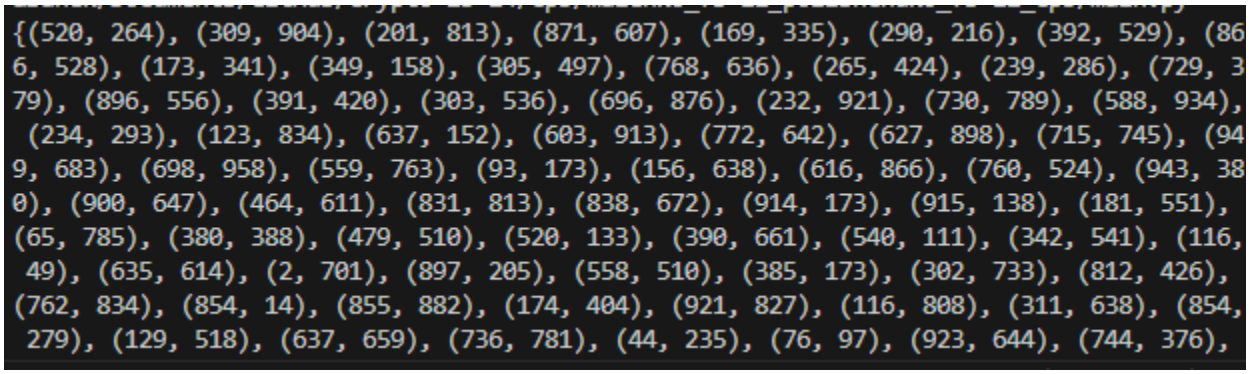
Ми співставляли не 5, а 10 біграм відкритого та шифрованого текстів. Задля перегляду детального співставлення, ми використали **matplotlib.**

10 найчастіших біграм шифрованого тексту:

```
[('тд', 0.027353463587921848), ('рб', 0.018827708703374777), ('во', 0.01847246891651865)
, ('щю', 0.015985790408525755), ('кд', 0.01492007104795737), ('ет', 0.014564831261101243
), ('жх', 0.012788632326820605), ('гц', 0.012788632326820605), ('ео', 0.0124333925399644
76), ('эт', 0.012078152753108348)]
```

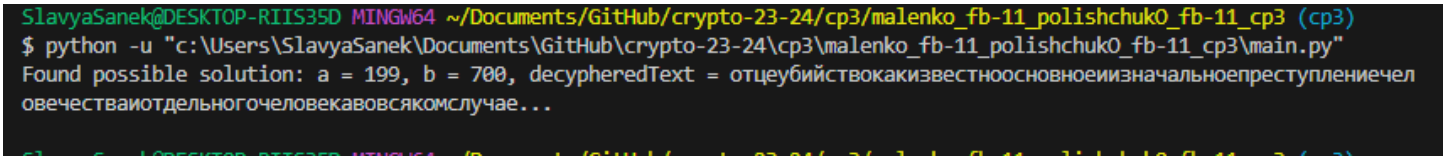


За допомогою функції **generate_keys** ми згенерували усі можливі ключі, яких виявилось доволі багато.



3. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Щоб знайти потрібний ключ, кожен розшифрований текст ми перевірили на неможливі біграми(масив котрих зберігали заздалегідь). У випадку коли текст не містить жодну з неможливих біграм – це є наш текст та можливий ключ.



(a, b) = (199, 700)

Отцеубийство, как известно, основное и изначальное преступление человечества и отдельного человека. Во всяком случае…

Це стаття - Зігмунд Фрейд «Достоєвський та батьковбивство»

Висновки: під час роботи над даним комп’ютерним практикумом ми дослідили моноалфавітні підстановки та мали змогу порівняти їх з поліалфавітними, як результат виконання 2 практикуму. Ми дослідили поняття модулярної арифметики та використали на практиці під час пошуку ключів для шифрованого тексту.