МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:

студенти гр. ФБ-14

Цибулено-Сігов І. М.

Татаренко А. О.

Перевірила

Селюх П. В.

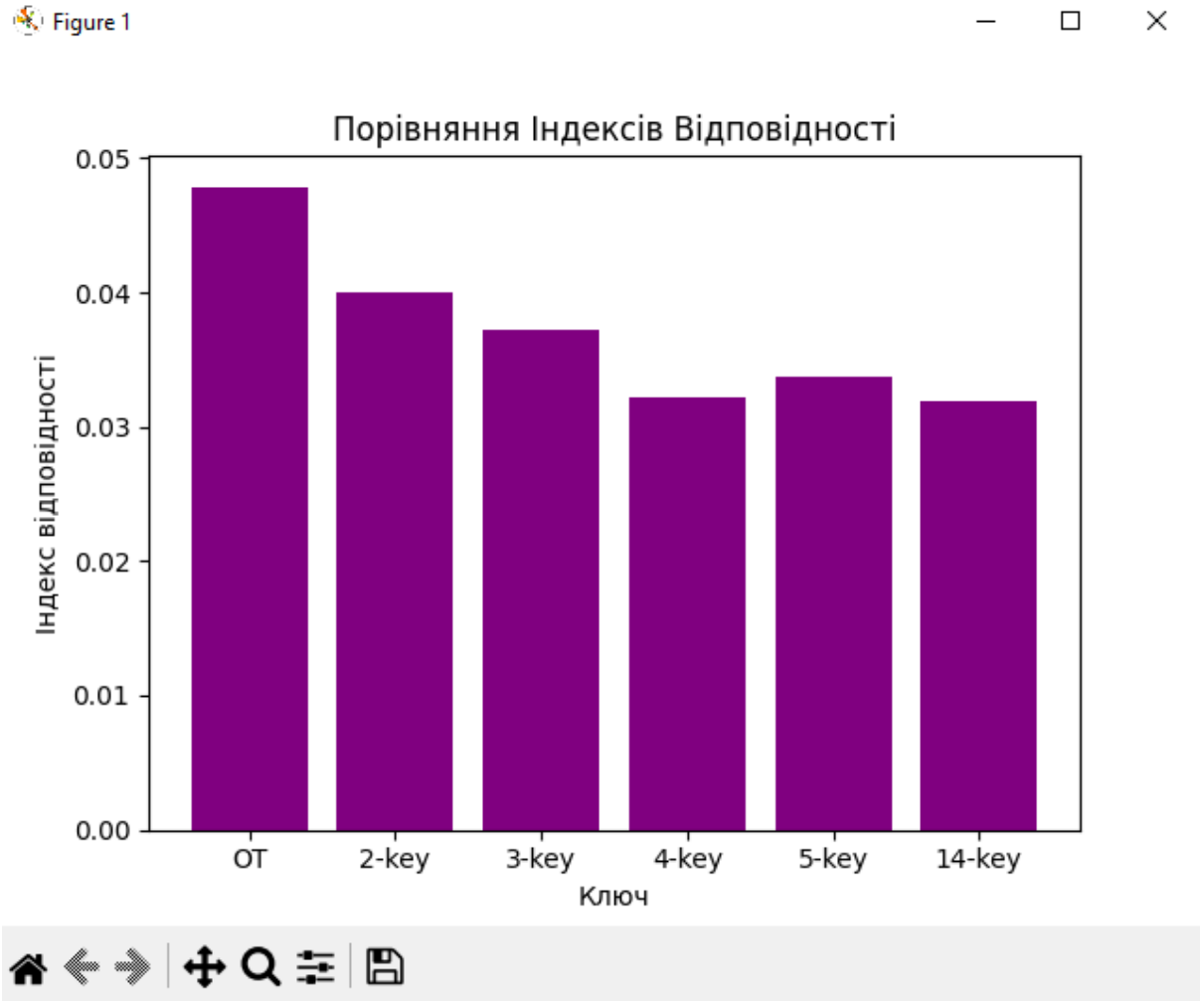
Київ 2023

Порядок виконання роботи

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.

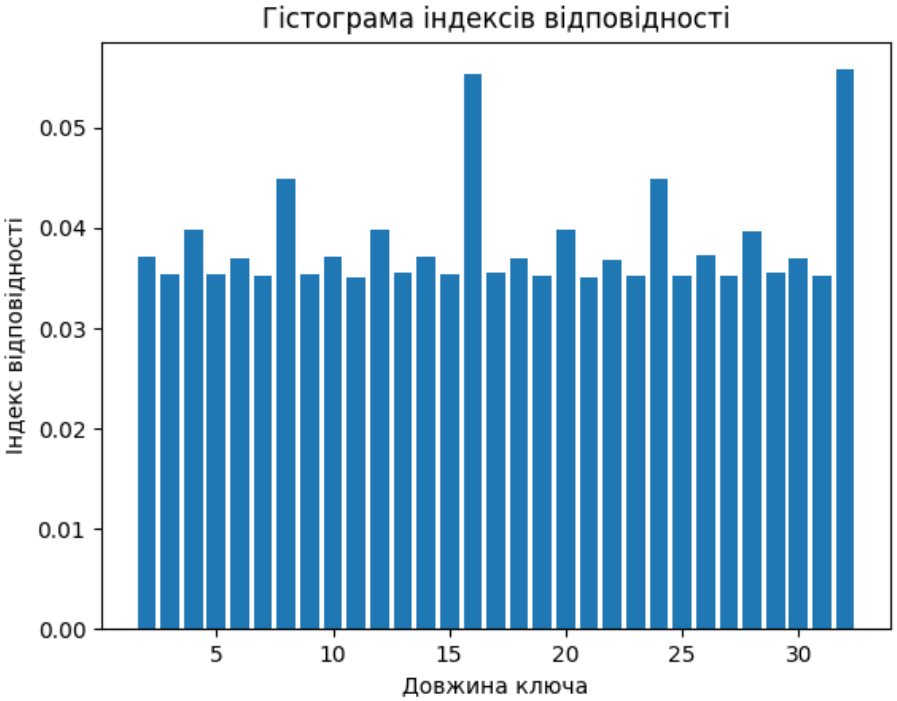
```
IOC for Open Text: 0.04779787744954941
IOC for 2-key ciphertext: 0.04004783742807906
IOC for 3-key ciphertext: 0.03723409264264123
IOC for 4-key ciphertext: 0.03216972870151517
IOC for 5-key ciphertext: 0.03369525298277664
IOC for 14-key ciphertext: 0.03187592402512407
```

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



Довший ключ додає більше варіацій у процесі шифрування. Якщо ключ дуже короткий і періодичний, то шаблони тексту можуть стати видимими на кількох рівнях, що може допомогти у розшифруванні тексту.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).
   Спочатку визначаємо довжину ключа:




```
Довжина ключа 2: Індекс відповідності = 0.03709682620655367
Довжина ключа 3: Індекс відповідності = 0.03535245194471151
Довжина ключа 4: Індекс відповідності = 0.039793511667390036
Довжина ключа 5: Індекс відповідності = 0.035435129393625094
Довжина ключа 6: Індекс відповідності = 0.037052368586566846
Довжина ключа 7: Індекс відповідності = 0.03522360497899179
Довжина ключа 8: Індекс відповідності = 0.04491213203766699
Довжина ключа 9: Індекс відповідності = 0.03545025157077616
Довжина ключа 10: Індекс відповідності = 0.03709763005817014
Довжина ключа 11: Індекс відповідності = 0.03506214646542888
Довжина ключа 12: Індекс відповідності = 0.0397888484387092
Довжина ключа 13: Індекс відповідності = 0.03550919719241092
Довжина ключа 14: Індекс відповідності = 0.037093872461702884
Довжина ключа 15: Індекс відповідності = 0.03538437139093187
Довжина ключа 16: Індекс відповідності = 0.05539766505382551
Довжина ключа 17: Індекс відповідності = 0.03552434946057639
Довжина ключа 18: Індекс відповідності = 0.037051140206933175
Довжина ключа 19: Індекс відповідності = 0.03531599104429486
Довжина ключа 20: Індекс відповідності = 0.03979839848540342
Довжина ключа 21: Індекс відповідності = 0.03505669694788307
Довжина ключа 22: Індекс відповідності = 0.03688094981192191
Довжина ключа 23: Індекс відповідності = 0.03526676001305197
Довжина ключа 24: Індекс відповідності = 0.04486292731353409
Довжина ключа 25: Індекс відповідності = 0.03531687664602463
Довжина ключа 26: Індекс відповідності = 0.037310868874659356
Довжина ключа 27: Індекс відповідності = 0.03524759105524548
Довжина ключа 28: Індекс відповідності = 0.03969086727168179
Довжина ключа 29: Індекс відповідності = 0.0355849038850587
Довжина ключа 30: Індекс відповідності = 0.0369283288698687
Довжина ключа 31: Індекс відповідності = 0.03527346532158509
Довжина ключа 32: Індекс відповідності = 0.05582349044633528
```

Відкритий текст

Мова	Індекс збігів
російська	0.0553

найближче значення отримуємо при довжині ключа r = 16

k = (y - x) modm
“о” - найбільш вживана літера рос алфавіту, підставляємо її замість x, визначаємо найчастішу букву для кожного з 16 блоків та підставляємо в y, число літер m = 32. Отримали ключ ‘декелисоборойдей’

```
Введіть довжину ключа: 16
декелисоборойдей
пооитноеделоуьлтусьнасильнолаеловжуаневоткнобьвореьсиэтудовчфьногсьстнуюистсцузнамснаверноефьчшечжхгдебытонскыловнсрекультущцость
```

Використавши отриманий ключ, бачимо вже більш змістовний текст, але все одно видно, що він не розшифрований до кінця. Тепер спробуємо вгадати неправильні літери. Очевидно, що перші два слова - ‘понятное дело’, знайдемо зміщення літер ‘о’ та ‘н’ (-1) і ‘и’ та ‘я’ (-9). Змістимо відповідні букви в ключі на n*(-1) позицій. новий ключ - ‘делолисоборойдей’

```
Введіть ключ: делолисоборойдей
понятноеделоуьлтурунасильнолаеловеканевоткнобьвордусиэтудовчфьногрустнуюистсцузналинаверное
```

Тепер текст іще зрозуміліше, однак трапляються фрагменти “рандомного набору літер”
Спробуємо замість “о” підставити другу за популярністю літеру - “е” (з першої лаби), зміщення ‘о’ з ‘е’ - 9

```
Введіть ключ: делолисоборотней
понятноеделокультурунасильновчеловеканевоткнешь
```

#лаби також

Висновки

Нами було засвоєно методів частотного криптоаналізу, ми здобули навички роботи та аналізу шифрів на прикладі шифру Віженера. Ми розраховували індекси відповідності та порівнювали їх між собою для визначення закономірності. Також нами було виконано шифрування і розшифрування (підбір ключа) наданих текстів за допомогою здобутих вище навичок.

кошенятко після лаби