

Національний технічний університет України «КПІ» імені
Ігоря Сікорського
Фізико-технічний інститут

Лабораторна робота 2

Криптографія

Виконали:

студенти ФБ-14

Кот Микита Сергійович

Чавалах Артем Дмитрович

Перевірила:

Селюх П. В.

Мета роботи

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

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

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.

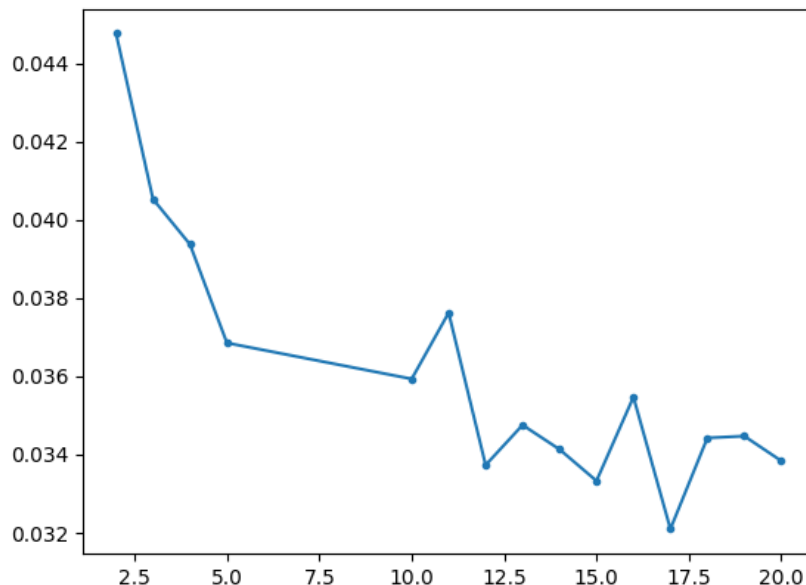
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

Відредагований текст (без пробілів, локеркейс, розділових знаків).

вдольтихтрудныхионьченьутолляющихповедахповедадриллимавтобусомизодногоконцаветавдругойдлинныхочередяхгдескапливаются
залосьбыкителисегородадигающихсятакмедленночтопоройловитьэтодвижениеудаётсявовсеигдетактрудносохранитьрадостноена
строениепрополительнорысковиопотчихкаждыйпредставляетсобойфантастикусталоистиратьсяиизраженияотомительномохиданийкогдапо
длиннеемеласенимиллозатыахизавязетсместеслишкомраноисвершенонопредставляеткакпростиверендомочалдеиставово
енялеткакпрятныйпрогулоксдружьямикогдаужееновоистипреданыссобытияизвестнысмыслизвученыиисвидеипредложеномемдл
ибеседподходиткконцуиначеулетногоокострагденеочесдуматьиочёматаолькослушатьзабавныесториивеселитьсяинаслаждатьсяиз
ныневедетбудеткестурассказыватькакойнибудьсмыслованекдотпричинеобыкновенныйанекдоткоротышуканчивающийсятогдакогдавоз
духешивучитперевеетословодлиннойблестящийанекдоткоторыйнепешалётсмядленноиленивоизавязетсраскручиваетсислов
ооричныйдаллордгрезанитересслухательласвнприкрадётсяитакжестепенноводитнафинишужеривуелослечногонаканунебастро
одобноилинисверкнувайесредиградысерыхтучнесколькочасовсобиравшихсянабегеобрушаветнасобравшихсяконцовкогулушетфина
льныммакордонкоторыйвсвоюочередьупогаевдвухносахприведеннаменузвонкойтишиножиданиярушаеойлишьмоногомрасказч
ика

Шифрування шифром Віженера з ключами:

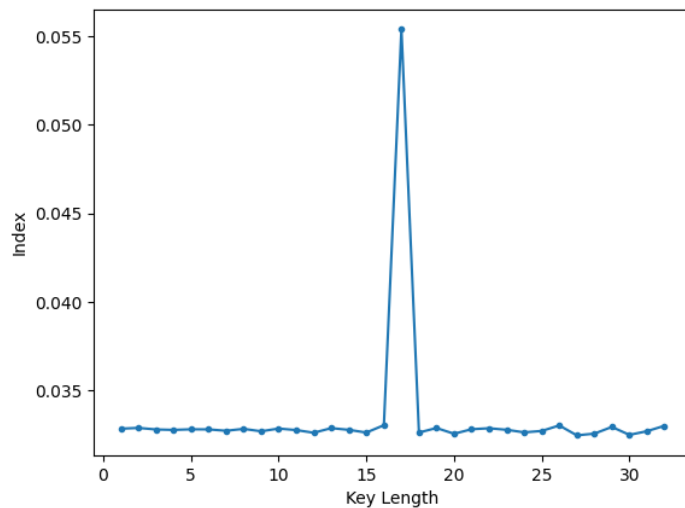
```
Index of clean text: 0.05336402505194377
Key: фу
Index: 0.044759137475800535
Key: кот
Index: 0.04052587584033445
Key: база
Index: 0.0393709341191511
Key: баран
Index: 0.03685178895898585
Key: авиасигнал
Index: 0.035932409608657706
Key: абракадабра
Index: 0.037623655950865795
Key: авантюристка
Index: 0.03373115929848154
Key: дальновиденье
Index: 0.03475459775438163
Key: кактусоводство
Index: 0.03413253013425911
Key: легковолполный
Index: 0.033327501449394684
Key: битторренттрекер
Index: 0.035470432920184376
Key: максимизировать
Index: 0.03209823179565994
Key: заграникомандировка
Index: 0.034425267837846184
Key: автомобилестроитель
Index: 0.03447100810403167
Key: латиноамериканизация
Index: 0.03383864892401742
```



Як можна побачити, спочатку індекс відповідності великий, коли маємо чистий текст та при меншому значенні ключа. Коли ключ стає більшим, індекс зменшується зі збільшенням ключа стає більш-менш однаковим.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (варіант 9).

Спочатку визначаємо індекс відповідності зашифрованого тексту. Потім визначаємо індекс для різних r .



Index of encrypted text: 0.0328460148020796

```
Index for r=1: 0.0328460148020796
Index for r=2: 0.03288907383913786
Index for r=3: 0.03280270806685515
Index for r=4: 0.032776586401747916
Index for r=5: 0.03281053998522203
Index for r=6: 0.032805493488069416
Index for r=7: 0.03272796104838353
Index for r=8: 0.03283440009895609
Index for r=9: 0.03269883173876473
Index for r=10: 0.03285327344856936
Index for r=11: 0.03276673213881401
Index for r=12: 0.032616530753538216
Index for r=13: 0.032876786821307354
Index for r=14: 0.03278042052494595
Index for r=15: 0.03262709665317097
Index for r=16: 0.03304101176307603
Index for r=17: 0.05539037433155081
Index for r=18: 0.03262856070999888
Index for r=19: 0.03288426955603722
Index for r=20: 0.03255886368565288
Index for r=21: 0.03281434392668897
Index for r=22: 0.03286955316619862
Index for r=23: 0.032783212941565554
Index for r=24: 0.032637774210807914
Index for r=25: 0.03271734599351552
Index for r=26: 0.033028484053788214
Index for r=27: 0.032470414513807624
Index for r=28: 0.03256476584763565
Index for r=29: 0.03294449398258896
Index for r=30: 0.032496753050019894
Index for r=31: 0.03270273941847026
Index for r=32: 0.033009000177655956
```

Знаходимо ключ для цього значення.

Ключ: боаямахчэндшпиэь

[illegible]

Замінімо на боаямахчэндшпиль (э -> л)

Бачимо, що виділений текст став більш читабельним, тобто заміна правильна

Тепер спробуємо отримати з ф -> у, щоб було **пльвущ** (щось типу плывущий -ая). За неї відповідає перша літера ключа

Це літера в, отримали ось це:

Пуыкстаючгозамкан акщосночькалепыв ущочнадыведомойб

Тепер ключ **воаяамахчЭНДШПиль** і судячи з усього тексту, то друга літера ключа теж правильна, оскільки далі є слово “ показати ”, у якого ть знаходяться на початку періоду

Далі спробуємо все ж таки дістати слово плывущая або щось подібне. Спочатку буква а(3 літера):

Вона відповідає літері о, але о не підходить, оскільки в ключі навряд буде дві о поспіль, але все одно перевірили і для я

Текст став більш нечитабельним, тепер плывущий:

a -> ж

$$\mathbb{R} \rightarrow \mathbb{H}$$

Тепер ключ **вожнамахчэндшпиль**. Сам текст вже можна більш менш читати. Зацікавив фрагмент надыведомойбеззной, в якому ‘ю’ взагалі незрозуміло, а замість беззной повинно бути бездної

Буква з знаходиться на 3 місці, тобто буква ж неправильна. Спробуємо “пливущей”:

Літера й:
 путьстаючгозамканакрасночькалепывущейнадыоведомойбездноимьпетпоказатьсяявечьдм

Пошук літер здійснювали ось так:

```
for i in russian_alphabet:
    ans = vigenere_decrypt(cleaned_text, "во"+i+"намахчэндшпиль")
    if "калепывущей" in ans:
        print(f"Литера {i}:")
        print(ans)
```

[illegible]

У ході виконання лабораторної роботи зіткнулися із труднощами з визначенням ключа для зашифрованого тексту. Була невелика проблема із відступами в зашифрованому тексті, не одразу їх помітили. Довго і складно визначали ключ

У ході виконання лабораторної роботи, ми набули практичних навичок щодо шифрування та розшифрування текстів шифром Віженера, оцінили значення індекса відповідності при маленькому та більшому розмірі ключа. На реальному прикладі розшифрували текст, знайшли ключ.