МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ "КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Виконав студент групи ФБ-14
Шовкун Богдан

2023

Тема: Криптоаналіз шифру Віженера

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

Варіант 10

Хід 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.

Ключі:

```
keys = ["аб", "где", "ежзи", "йклмн", "опрстуфхцчшщьыьэюя"]
```

Текст:

```
Склон балки покрывала плотная, густая масса ежевики и барбариса – идеальное место для гнездовья и кормежки, поэтому неудивит
Самозабвенно расточали трели зеленушки, щебетали чечетки и славки-завирушки, то и дело раздавалось звучное «теньк-теньк» зяб
невольно взглянув на небо. Туч не было. Но зяблики всегда тенькают к дождю. А немного бы дождя не помешало.

Место напротив устья котловинки было прекрасной позицией, обещавшей удачную охоту, особенно здесь, в Брокилоне, пристанище в
дриады охотились очень редко, а человек отваживался заходить сюда и того реже. Жаждущий мяса и шкур ловчий сам становился об
пришельцам. Мильва имела случай убедиться в этом на собственной шкуре.

Чего-чего, а уж зверья в Брокилоне было предостаточно. Однако Мильва сидела в засаде уже больше двух часов, а на расстоянии
она не могла – стоявшая месяцами сушь выстлала почву хворостом и листьями, хрустевшими при каждом шаге. Сейчас только неподв
принести добычу.

На лук присела бабочка адмирал. Мильва не стала ее пугать. Наблюдая за тем, как бабочка складывает и раскрывает крылышки, он
которому все еще не могла нарадоваться. Она была, как говорится, лучницей от Бога, обожала хорошее оружие. А то, которое сей
```

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

```
Index of clean text: 0.05414476079081951

Key: аб
Encrypted text written to encrypted_2.txt
Index: 0.04390564112357003

Key: где
Encrypted text written to encrypted_3.txt
Index: 0.039690164883364264

Key: ежзи
Encrypted text written to encrypted_4.txt
Index: 0.03857184629982159

Key: йклмн
Encrypted text written to encrypted_5.txt
Index: 0.038261533779308125

Key: опрстуфхцчшщьыьэюя
Encrypted text written to encrypted_18.txt
Index: 0.032870450490234106


Process finished with exit code 0
```

Ключ який складається з двох символів має найбільший індекс відповідності. Це говорить про те, що текст зашифрований з цим ключем менш ефективно “маскує” ВТ.

В той час ключ який містить 18 символів краще “замаскує” ВТ.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

10 варіант.

Спочатку розбиваю текст на блоки довжини r:

```
def to_blocks(text, r):
    return [text[i::r] for i in range(r)]
```

Далі розраховую індекси відповідностей для різних r, де r це довжина ключа:

```
def calculate_index(text, r):
    blocks = to_blocks(text, r)
    index = 0.0

    for block in blocks:
        freqs = Counter(block)
        total_pairs = sum(f*(f-1) for f in freqs.values())
        index += total_pairs / (len(block) * (len(block) - 1))

    return index / r

1 usage
def freq_count(text):
    freqs = Counter(text)
    most_freq = max(freqs, key=freqs.get)
    return most_freq
```

Тепер я обчислюю найчастіший символ у ШТ:

```
def freq_count(text):
    freqs = Counter(text)
    most_freq = max(freqs, key=freqs.get)
    return most_freq
```

Після цього я шукаю ключ за домомогою формули k = (y - x) mod m, де y буква, що частіше за всіх зустрічається у ШТ, а x це буква, що частіше за всіх зустрічається у московській мові. M - довжина алфавіту.

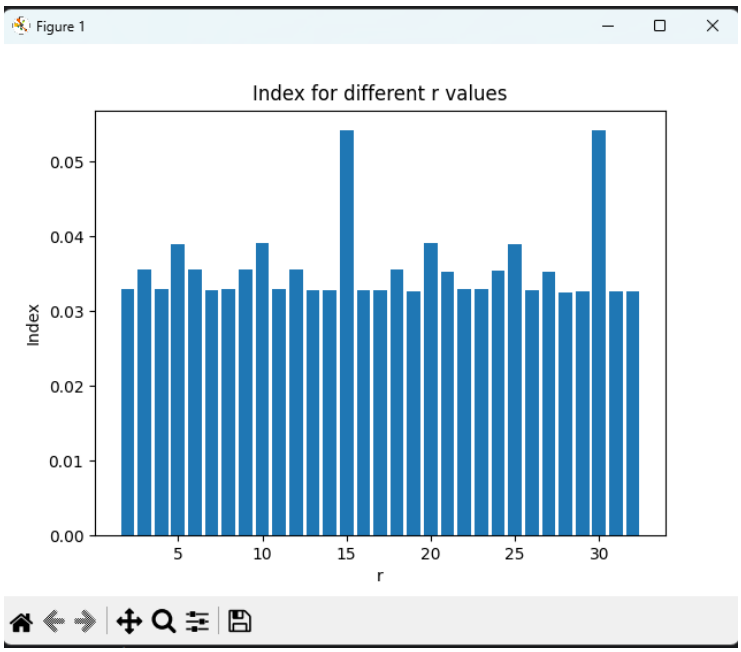
```python
def find_key(text, r):
    russian_letter_o = 14
    mod = len(alphabet)
    blocks = to_blocks(text, r)
    key = ''.join([alphabet[((alphabet.index(freq_count(i)) - russian_letter_o) % mod)] for i in blocks])
    print(f'possible key: {key}')
    return key
```

Нарешті створюю діаграму індексів відповідностей для різних r:

```python
indexes = []
r_values = list(range(2, 33))

for i in r_values:
    ic = calculate_index(filtered_text, i)
    indexes.append(ic)

plt.bar(r_values, indexes)
plt.xlabel('r')
plt.ylabel('Index')
plt.title('Index for different r values')
plt.show()
```



Бачу що при r = 15 індекс відповідності найбільший. Викликаю функцію Find_key() та ввожу туди значення r = 15:

```
find_key(filtered_text, r=int(input('Value for r = ')))
```

```
Value for r = 15
possible key: крадущяйгявтени
```

Отримую потенційний ключ. На диво слова в ньому дуже легко розпізнати. Ключ: “крадущийсявтени”

Далі викликаю функцію decryprt() зі своїм ключем:

```
def decrypt(encrypted_text, key):
    decrypted_text = ""
    key_len = len(key)
    mod = len(alphabet)

    for i in range(len(encrypted_text)):
        char = encrypted_text[i]
        if char in alphabet:
            key_index = i % key_len
            key_char = key[key_index]
            shift = alphabet.index(key_char)
            new_char_code = (alphabet.index(char) - shift) % mod
            decrypted_char = alphabet[new_char_code]
            decrypted_text += decrypted_char
        else:
            decrypted_text += char

    return decrypted_text
```

```
Your key: крадущийсявтени
```

Отримую текст в якому можно спокійно розібрати слова.

```
Your key: крадущийсявтени
тихотактихочтослышнокакмотылькицепляютсяхрупкимикрылышкамизаночнуюпрохладупораужеотправлятьсяпосвоимде
```

Записую отриманий текст в окремий файл:

```
decrypted_text = decrypt(filtered_text, key=input('Your key: '))
print(decrypted_text)

with open('decrypted_text.txt', 'w', encoding='utf-8') as file:
    file.write(decrypted_text)
```

Назва твору “Крадущийся в тени”. Автор Олексій Пєхов.

Повний текст:

Тихотактихочтослышнокакмотылькицепляютсяхрупкимикрылышкамизан
очнуюпрохладупораужеотправлятьсяпосвоимделамстражадавнопрошлано
ясегоднячтотослишкомосторожничаюнекоенеобъяснимоечувствозаставляе
тменязадержатьсявозлестеныздания погруженноговтеньтеньмояподругамо
ялюбовницамоянапарницаяпрячусьвтенияживувнейтолькоонавсегдаготова
принятьменяспастиотстрелзлобносверкающихвлуннойночиклинковилиотк
ровожадныхзолотыхглаздемоновтенькакговоритдобрыйжрецсаготабратфо
ркогдахватитлишкувовремянашихредкихвстречтеньявляетсясестройтьмыа
оттьмынедалекоидоненазываемогочушьненазываемыйитьмаабсолютнораз
ныевещиэтовсеравночтосравниватьограивеликанатеньэтожизньтеньэтосво
бодатеньэтоденьгитеньэтовластьтеньэторепутацияужгарреттеньзнаетобэто
мнепонаслышкетеньпоявляетсятолькотогдакогдасуществуетхотябыкрупиц
асветатакчтосравниватьеестьмойпоменьшеймереглупономоемустаромуучи
телюяестественноэтонеговорюяйцакурицунеучатнаузкойночнойулочкеска
меннымидомамизаставшимитихиевременанераздавалосьнизвукалишьпоск
рипывалажестянаявывесканадлавкойбулочникаотгуляющегопокрышамгор
одаслабоговетеркамедленныйсерожелтыйночнойтуманкоторымславиласьн
ашастолицаговорятфокускакоготомаганедоучкипрошлогооткоторогонемог
утизбавитьсяипоныневсеархимагикоролевствазастилалмощеннуюгрубымк
амнемиизбитуютелегамимостовуютихотихословновсклепебогатеяпослетог
окакегонавестиластаямелкихгородскихворишекскрипитвывескагуляетвете
рокмедленноиленивоплывутоблакапоночномунебуноявсеещестоюслившис
ьстеньюзданияистараясьнешевелитьсяинтуицияимойжитейскийопытзастав
ляютвслушиватьсявтишинуночногогороданиоднадажепустыннаяулицанем
ожетбытьтакойтихойособенноэтагдеживуттолькооднилавочникивночидол
жныбытьзвукикрысышуршащиевмусорехрапящийтутжепьяницакоторогоу
жеуспелипочиститькарманникипреждечемзабитьсявкакуюнибудьщельнан
очьхрапизоконседыхдомовкрадущаясявотьмегрязнаясобакатяжелоедыхани
еновичкаразбойникавожиданиисвоейжертвызастывшеговомглесзажатымв
потнойладониножомшумвлавкахимастерскихдажепоночамвнекоторыхизн

ихкипеларабо таничегоэтогонебылонатемнойузкойулочкеукутаннойвперин
утумананичегокрометишиныимракаветероксильнеезагулялвкрышахстарых
зданийитяжелыесерыеоблакапонеслисьпонебусловностадобольшихпушист
ыховецобнажаянебесныйкуполбеспечныйгулякаветерласковотрепалволос
ыноянесмелнакинутьдажекапюшонсаготчтожеэтокакбыотвечаянамоюмол
итвуславныйбогвсехворовдалушамбольшечуткостишагиторопливыешагич
еловекакоторыенесмогприглушитьдажетуманрасползающийсясерожелтой
накипьюнадкаменнойомостовойвсоседнейвыемкерасполагающейсянастенез
даниянапротивязаметилмимолетноеколебаниевотьмектотопрячетсяявсмот
релсявчернильнуюночьнетпоказалосьслишкомволнуюсьвожиданиинесуще
ствующихнеприятностейстареюнаверноечьятотребовательнаярукаудержал
аменянаместекакбыговорястойобождиещеневремяхсанкорменясожричтож
епроисходитнатихойтемнойулочкеремесленниковчеловекпоказалсяиззапо
воротаулицыибыстрымшагомпереходящимвбегнаправилсявмоюсторонуду
ракилихрабрецеслиодиншастаетвтемнотескореевсегопервоехрабрецыдолг
онеживутвнашеммирехотядуракитожееслионинешутынашегославногокоро
лякакоенеотложноеделозаставиловыйтиегонаночнуюулицугдедажемаслян
ыефонаринегорелипопробуйтенайтифонарщикакоторыйвысунетвэтовремя
носвкромешнуютьмуэтоведьнетихиевременакогдаребенокспокойномогпро
йтивсамуюглухуюночьизодногоконцаавендумавдругойиснимничегобынес
лучилосьчеловекприближалсявысокийхорошоможносказатьбогатоодетыйр
укалежитнарукоятиприличногомечаслужитважнойшишкенаверноеоблакас
нованаползлинанебозакрывсвоимтеломвыступившиенанебезвездыикполно
йтьмедобавиласьтьмакромешнаяяуженесмогразглядетьлицаспешащегочел
овекаонпоравнялсясомнойидаженезаметилтихостоящуювтенитеньеслибыя
захотелипротянулрукутоснялбыунегоспоясапузатыйкошелекноянемелкийк
арманникчтобыпадатьтакнизковременамолодостидавнокануливлетудаисуд
ьбаподсказывалачтосейчаснестоитнеточтодергатьсяадажеглубокодышатьв
нишенапротивтьмавновьпришлавхаотическоедвижениевскипаяиклубясьче
рнымцветкомсмертииязамерледенеяотужасаизтьмывырваласьтьмаприняво
бличьекрылатогосуществадемонасрогатойголовойчерепомнакоторойсияли
алыеузкиеглазаикаклавинасгоркарликовупаланаспешащегочеловекапридав
ивегосвоимвнушительнымвесомчеловекиздалвопльраненойкошкипопытал
сявыхватитьбесполезныймечнотьмасмялавсосалапоглотиланочногопутник
аисуществокембыононибыловзмыловночноеоблачноенебоуносяссобойсве
жеемясоаможетидушуугольночерныйсилуэтнамигмелькнулвоблачномноч
номнебеиисчезястаралсяуспокоитьдыханиетварьнезаметилатогоктовсеэтов
ремянаходилсянапротивнееноеслибыяшевельнулсяеслибыяхотьнамигшеве
льнулсяилихотябызадышалчутьгромчетоонабыбросиласьнаменяизнишизд
аниягдеподжидалалегкуюдобычуповезловочереднойразмнеоченьповезлоу
дачавораженщинакапризнаявлюбоймигможетотвернутьсянопокаонасомно

йямогузаниматьсясвоимворовскимремесломвтемномуглусоседнегозданият
ихопискнулакрысазанейдругаявнебеохотясьзаприпозднившимисяиюньски
мимотылькамипролетелалетучаямышьопасностьминоваламожнопродолжа
тьпутьяотделилсяотстеныистараясьдержатьсянаиболеетемныхучастковули
цыдвинулсядальшеничтонеговорилооослучившемсянесколькоминутназадул
ицабыламолчаливымиединственнымсвидетелемночнойохотыдемонаксчаст
ьюлунынебылопушистыеоблакавновьнаползлииспряталиотгородазвездып
оэтомутенибылосколькоугоднобыстрымшагомнеиздаваясапогаминиедино
гозвукаяперемещалсяотзданиязданиюизтенивтеньулицапекарейосталасьп
озадиясвернулвпереулокнаправоздесьтуманбылгущеонобволакивалменямя
гкимилапамиглушилшагискрывалотглазлюдейинелюдейвтенипососедству
раздалосьшушуканьеязамервсматриваясьвсерожелтуюмглуворымолодыещ
енкикудавамдомастераподжидаютночногогулякуилиготовятсяпочиститьсп
ящихгорожанзеленыслишкомшумятслишкомнеопытныворыпрофиперегов
ариваютсяжестаминеиздаютшумадажевтакойночикогдагустеющийлипкий
тумангаситвсезвукияпроскользнулрядомснимиаворишкидаженезаметилит
еньтеньвтенисложноувидетьнеопытномуглазувозниклодурацкоедетскоеже
ланиевыскочитьизтуманаигромкосказатьбуимвлицоновполнеможнонарват
ьсянаслучайныйножтемболеечтонечегопугатьмолокососовтемныйпереуло
ккончилсяинависшиемрачныестеныдомоввидавшихвэтоммиреирадостьиго
ререзкоразошлисьвстороныяпосмотрелнанебоветервсетакиразогналленивы
еоблакаинебопревратилосьвскатертьнакоторойбогатейрассыпалмонетысот
ниитысячизвездмерцалимнеснебаэтойхолоднойлетнейночьюсветлокакдне
мздесьгорелиодиночныефонарикакникакянаходилсянаоднойизцентральны
хплощадейгородаифонарщикинесмотрянасвойстрахбылиобязанывыполнят
ьсвоюработупламяфонарейзакованноевстеклянныеколпакиразбрасывалово
кругсебяпятнадрожащегосветаихаотичныетенимолчаливоплясалинастенах
угрюмыхдомовэтоплохонадеюсьчтопогонщикветерсноваприведетсерыхпу
шистыховецнанебоапокапридетсядержатьсятенижмущейсякстенамвысоки
хзданийкотораясталабледнойипугливойотвездесущегосвета

Висновок: У ході виконання лабораторної роботи я набув навичок щодо шифрування та розшифрування текстів шифром Віженера. При розшифруванні заданого тексту зміг знайти ключ та розшифрувати текст.

Також порівнював значення індексів відповідності для ключів різної довжини.

Мій котик Маркус