**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**

**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**

**ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**

**Кафедра Інформаційної Безпеки**

**Лабораторна робота №2 дисципліни**

# ”КРИПТОГРАФІЯ”

**Підготував:**

**студент групи ФБ-06**

**Жак Костянтин**

**Київ 2022**

**Тема роботи**: Криптоаналіз шифру Віженера

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

**Порядок виконання роботи (варіант 8)**

*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.*

```
'''
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.
'''

with open('final.txt', 'r', encoding='utf-8') as file:
    text = file.read()

keys = {'r2': 'нг', 'r3': 'жак', 'r4': 'рево', 'r5': 'водка', 'r10': 'абдулкасим', 'r13': 'пивнаяторпеда',
        'r17': 'материализовывать'}

def encrypt(text, r):
    encrypted = ""
    for i in range(len(text)):
        encrypted += alphabet[(alphabet.find(text[i]) + alphabet.find(r[i % len(r)])) % 32]
    return encrypted

for r, length in keys.items():
    encrypted = encrypt(text, length)
    with open(f"{r}.txt", 'w', encoding='utf-8') as file:
        file.write(encrypted)
```

Отримуємо зашифровані різними ключами тексти:

r2: нг

```
ъиьюягцхтфйънушяфданыеюнхдионочсрсшлчсщдндълчсщкнвсоипхжэсчсщшнпыпупыхыпължиоуызы
```

r3: жак

```
уещбткптпчьбжрхвзлщкшисфобесахронфлтроцзалуиффмсжяосыцогъфкшт
```

r4: рево

```
эксйвелахцюерхнкчжхшюзушшжэщррмьуунцъуопржпцъуохрджщлсксаумььъвъюсиъючръэныусхртю
```

r5: водка

```
пууетвчцпсюедълюхеэкррхфигйпклмьзшлкштцбвпсткрълкяжщяциеютфоогдцоофршгръстщзпфшдръдмхх
```

r10: абдулкасим

```
нжуоэкйгнэьшдгцжзтыцогхэулыьичкпзбцткяфнавсыхшмшилдмяяунрятъмцдящцжэцюонсыдпббцрондхаэдйрсдомвщзтяфйтпуб
```

r13: пивнаяторпеда

```
ьнситяыахабыаяуюфбтььтапмбкувшкнхьычптмригъийаъчпдилкфкррньььдероыоооытнюышикерэмрщабзбфз
```

r17: материализовывать

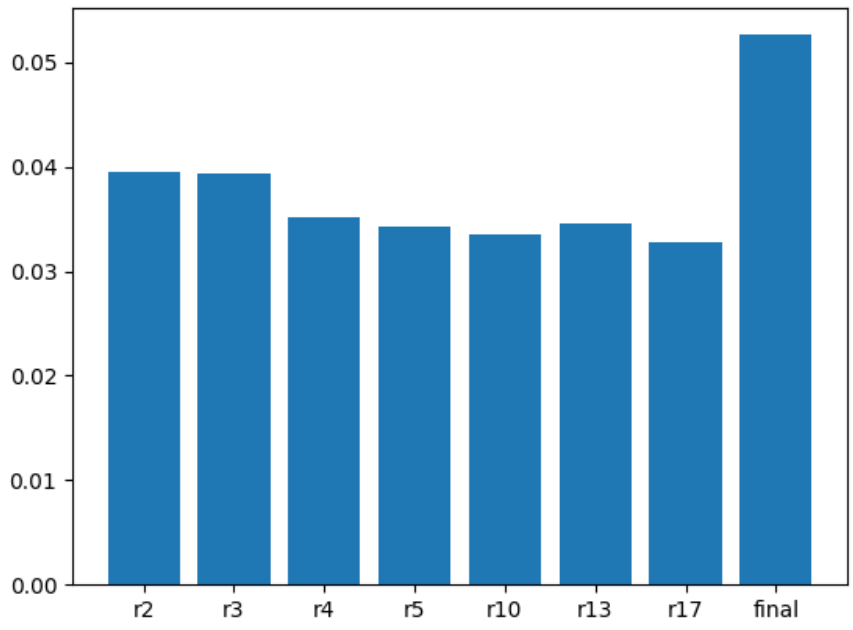
```
щебавийэншкцытлогнуьутщкуйвщвжмохкчиьуьйамхпшрзйасачыюнушохцугвзрмшиътасэрщрйчьжйоафсядкнхмнучхлфйоэдкыогрхмнусюунйдеьжъ
```

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

```python
def count_index(text):
    index = 0
    for char in alphabet:
        index += text.count(char) * (text.count(char) - 1)
    index *= 1 / (len(text) * (len(text) - 1))
    return index
```

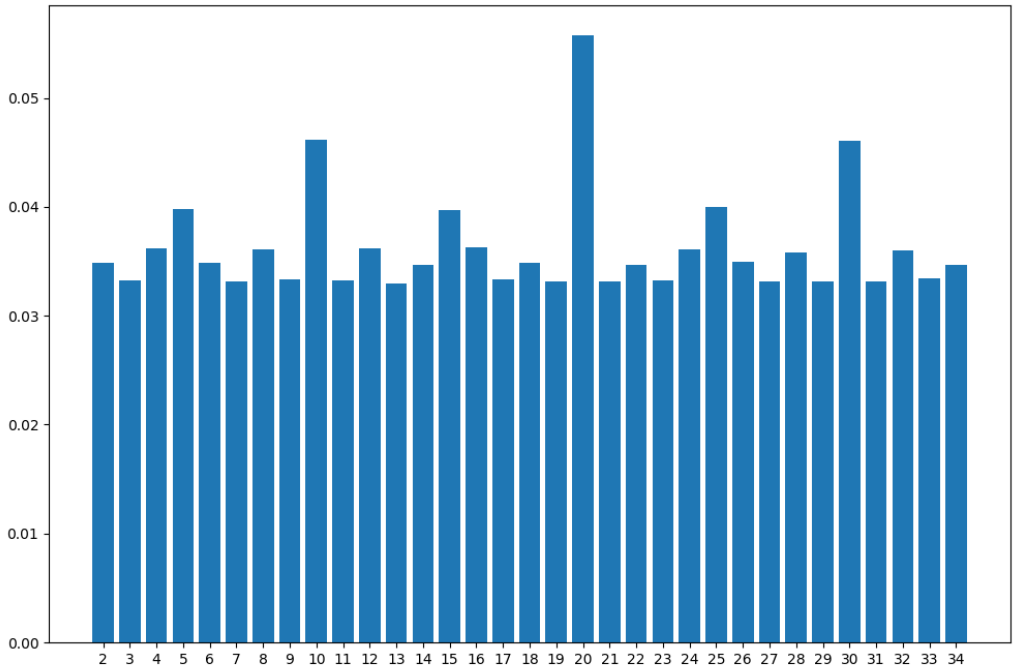
```
r2 index: 0.039463147933165514
r3 index: 0.039371194967107656
r4 index: 0.035103044792588585
r5 index: 0.034286962218825066
r10 index: 0.033516856128090 48
r13 index: 0.034539832875484185
r17 index: 0.03271226767508419
final index: 0.05262391620019693
```

Отримуємо індекси відповідності для зашифрованих текстів та відкритого тексту. Виведемо їх у вигляді діаграми.



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

Розбиваємо текст на блоки та отримуємо наступні значення індексів відповідності:




Як ми бачимо, найбільш приближений до теоретичного значення період 20.

Розшифровуємо ключ довжиною 20:

```
улановсеребряныепули
```

Пару букв не розшифрувало, але можна здогадатися: улановсеребряныепули.

За допомогою ключа розшифровуємо текст:

```
def decrypt(text, key):
    decrypted_text = ''
    for i in range(len(text)):
        decrypted_text += alphabet[(alphabet.find(text[i]) - alphabet.find(key[i % 20])) % 32]
    return decrypted_text

key = 'улановсеребряныепули'
print(decrypt(text, key))
```

```
этасистемакрасногокарликаникогданеимеланазваниятолькозубодроб
```

этасистемакрасногокарликаникогданеимеланазваниятолькозубодробительнодлинныйноме
рвкаталогеисследовавшийеекиберзондотметилналичиетрехгазовыхгигантовдвухастероидн
ыхполейкометногооблакаизанесвсеэтиданныевсекторвторойочередипомнениюинкакиберз
ондасистеманепредставляликакойценностидляпославшихеголюдейнаверноебудьунегоза
действованыконтурывторогоуровнясамостоятельностииазартаонбыпоспорилсамссобойчто
вближайшуютысячулетлюдиздесьнепоявятсяипроспорилбылюдипоявилисьвэтойсистемен
ечерезтысячулетавсеголишьчерезсемьэтобылинетелюдичтопосылализондформальноониво
общенедолжныбылизнатьосуществованииэтойсистемыноутехктоихпосылалбылиденьгимн
огоденегисредипрочегоиххватилонаточтобыполучитьвозможностьознакомитьсясрезультат
амикартографированиязаинтересовавшегоихсекторатаквсистемепоявиласьстанциянаскоро

переделаннаяизсписанногогрузовикаитридесяткабуевраннегооповещенияподсвечивающих
пространствоврадиусепятисветоднейотнеечерезнесколькомесяцевнастанциюпришелпервы
йкорабльэтобылстранныйкорабльсвидуобычныйдесятикилотонниксотникоторыхлетаютка
кповнутреннимаршрутамсолнечнойтакинавнешниеколониинеобычнымжеегоделалисереб
ристыеовалынабортахпонимающийчеловеклегкобымогопознатьвэтиховалахтяжелыеизлуч
ателимайерсапредставлявшиесобойглавныйкалибркрейсероввксфедерациикорабльбылнео
диндругиепохожиенанегоразвдватримесяцазалеталивсистемудатьотдыхкомандеимехániz
мампровестимелкийремонткоторыйотчеготонемогливыполнитьсобственныесервыкорабля
впрочемремонтневсегдабылмелкимодинизкораблейприползнастанциюсперекореженнымб
ортомоставляяпозадитающийсиневатыйследсочащейсяизразбитыхотсековатмосферыоняв
новстретилкоготоравногопосиламаможетбойбылнеравныйноэтоттктотознаячтопошадынеп
риходитсяждатьоченьстаралсяпродатьсвоюжизньподорожетригодаспустясистемунавестил
ещеодинкиберзондоднакохотяегосканирующиесистемыбылинапорядокмощнеечемупредш
ественниказдействоватьихоннесталвместоэтогоновыйгостьтихозависнадплоскостьюэкли
птикизапределамидосягаемостибуевипринялсявпитыватьинформациюшумсолнечноговетр
атяжелыйрокотгравитационныхволнпланетобрывкиразговоровмеждустанциейиочередным
прибывающимкораблемпоследнееегоинтересовалоособенносильноаещечерезмесяцвсисте
мепоявилисьновыекораблипятьузкихххищныхтенейтотчеловекчтомогбыопознатьсеребрист
ыеовалынавернякасумелбыузнатьиихпотомучтомалосчемвовселеннойможноспутатьизящн
ыйпрофильэсминцавкстипасиранотроевновьприбывшихушливбокблокируяточкуперехода
адвесеребристыеполоскирванулисьпрямокстанциигдекакраззаканчивалподготовкукполету
очереднойкорабльтемнотавокругтьмаитишинаигдетотамждетнечтоцельмишеньврагодним
словомточтонадоуничтожитьсправадонессятихийзвуктолискриптолишорохямгновенноотс
кочилвсторонуиокатилподозрительныйучастоквееромогнятихийтрескэтозвуквыстреловазв
онкиеиглухиехлопкиэтошарикиплазмывимитационномрежимезвонкиеобстенуиглухиевми
шеньтеоретическиимиможнобылобытемнотуподсвечиватьнопоусловиямзачетаяопасаюсьд
емаскировкипотомуплазмачернаявидетьвинфракрасномяпоканенаучилсяавотшорохвперед
ияпрыгалпокомнатесловноплохаямарионеткапосылаяновуюочередьпреждечемзатихнетпр
едыдущаяисчиталглухиеударыпадающихтелпятьшестьитемнотазначитещектотоосталсяск
олькожеихгадовсемьиливосемьяполуприселнаклонилсявпередирастопырилрукисловновсп
лывшаяжабаточьвточькаккитаезаченьвоназанятияхрасслабилсяислушаешьголосвселенной
сейчасонтебеспоетвухогдепрячетсяпоследняяцельнасамомделеяужедавноубедилсячтоника
кимиэкстрапараиипрочимисверхспособностяминеобладаюноможнопопытатьсякупитьнаэто
тфокусоператоракупилочереднойшорохдонессяиззаспиныеслибыядействительноловилу
шамиголосиззакраямиратутбымнеибылполныйконецзачетанопосколькуязанималсяловлей
исключительнореальныхзвуковтоупалвпередуспевприэтомизвернутьсяипрошитьочередью
пространствопередсобойперекатилсяполучивприэтомчувствительныйударвпоясницупосла
лвторуюочередьпримернотудакудаипервуюинепрекращаяпалитьповелстволвнизнатотслуч
айеслигадуспелрастянутьсянаполузачетноеиспытаниеоконченовсемишенипораженывкомн
атеначалмедленноразгоратьсясветяпопыталсяприподнятьсяполаисразужесхватилсязауши
бленныйживотавотнечегопадатьнаоружиеонокакправилотвердоеиребристоенуикактебеко
мнатамракаехидноосведомилсяоператормрачнокакмояфамилиянопоследиснейлендамнеуж
еничегонестрашнотакужинестрашнокогдатвойлучшийдругвылетаетсэкзаменаусловноубит
ыйпузатойзеленойвороной уженичегохуженебываетнунуладнокурсантсвободенполучаяназ
адодеждуяобнаружилчтопокаяотстреливалкотоввтемнойкомнатенабрикпоступилосообщен
иеинтересноотогоэхвотбыотджейнтретийсвободныйуикэндинескемпровестиобидноволь

ослушателювукомраковичунемедленноявитьсяналейтстриткполковникукоринуоппадааэто неджейнналейтстритразмещалосьместноеотделениеконторыкоторуювсесодружествокосоу хмыляясьименовалоконторойглубинногобуренияхотянаэтомзданиивиселатабличкафирмы поэкспортукокосовыхореховачутьпоодальпанельрекламыпериодическивыплевывающаяна стенусоседнегомонодомаслоганкокосыгрузимбыстрооноивидноколонииивсистемебезкокос овыхореховневыживутвымрутскореечемотвзрывнойдекомпрессиировночередвадцатьодн уминутуяробкоподошелкмерцающейдверицельвашеговизитагрознопроревеламозаиканадп роемомтонвопросапредполагалчтоприлюбомнеудовлетворительномответеменяпревратятв облачкоразогретогопараиподеломпосколькушлятьсяудверейэтойфирмымогуттольколибое есотрудникилибозлобныеиномиряненуаеслипопадетсякакойтоэкспортеркокосовбываетнеп овезлокурсантмраковичкполковникукоринупроблеяляотдушинадеясьчтоинтелктроникане сочтетдрожьвмоемголосехарактернымдляиномирцевпризнакоммерцающаязавесаисчезлап роходитеголососталсятакимжерезкиминеприятнымнопокрайнеймересталнаполтонатишеяо сторожноступилнасверкающийполповернитесьлицомкстенесмотритепередсобойпротяните рукувотверстиеанализсетчаткииднкпроверяютилиявсамомделевукомраковичгражданинфе дерациидвадцатьпервогогодаотродуилинежитькакаякакговориламояпокойнаячешскаябабу шканикогданеслышавшаяпроиномирянследуйтезакраснымсигналомзакакимещекраснымси гналомпоинтересовалсяяотворачиваясьотстеныиуставилсянакрасныйогонеквисевшийввоз духепрямопередмоимлицомследуйтезакраснымсигналомлюбоеотклонениеотмаршрутасчи таетсянарушениемагашагвсторонупобегпрыжокнаместепровокацияэтоужемойрусскийдед ушкавывсехтаквстречаетеилитолькоменянапоследокпоинтересовалсяядвинувшисьзаогонь комвсехпостороннихпытающихсяпройтичерезслужебныйвходсообщилголостакиоставивм енявнедоумениитолияговорилсвозомнившимосебеинкомтолиссадюгойохранником

## Висновок

В ході комп’ютерного практикуму були засвоєні методи частотного криптоаналізу. Здобуті навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера. Були підібрані довільні ключі та зашифрований текст за допомогою них шифром Віженера. Оцінені індекси відповідності для зашифрованих текстів та для відкритого тексту, який склав 0.05262.  Був знайдений ключ для тексту наданого варіанта (улановсеребряныепули) та отриманий початковий текст.