Лабораторна робота №2

Криптоаналіз шифру Віженера

Виконали:

ФБ-23 Литвин Руслан

ФБ-23 Ващаєв Тимофій

Варіант 1

Мета роботи

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

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.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи

Для виконання першого пункту було виділено дві головні підзадачі: валідація тексту, та власне шифрування. Валідація тексту є тривіальною задачею, для цього кожен символ перевіряється на те, чи входить він в діапазон букв від ‘а’ до ‘я’ в таблиці Unicode. Це зручний спосіб для нашого випадку, адже в цьому діапазоні є рівно ті літери, які нам необхідні в алфавітному порядку.

```
with open(f_name, "r", encoding="utf-8") as f:
   for s in f.read().lower():
       if s >= "а" and s <= "я":
           text += s
       elif s == "ё":
           text += "е"
```

Алгоритм шифрування теж базується на таблиці Unicode. Спочатку перевіряється вхідні аргументи на валідність. В циклі ітеруємо індекс кожного символа відкритого тексту, цей індекс також використовується для ітерації ключа по модулю його довжини.

```
 cipher = ""
    for i in range(text_len):
        cipher += chr((ord(text[i]) + ord(key[i % key_len])) % 32 + 1072)
```

Відповідні коди символів тексту і ключа додаються по модулю 32. Це працює завдяки тому, що базова адреса нашого алфавіту 1071, так як символи два, то разом додавання по модулю дає нуль:

$$1071 + 1071 \bmod 32 = 0$$

Відповідно отриманий результат це зсув відносно базової адреси алфавіту, який в даному випадку 1072.

Підрахунок індексу відповідності зводиться до двох основних підзадач підрахунок кількості символів та обчислення значень по формулі. підрахунок символів працює так, що ітерує вхідний текст, та додає до словника символ, якщо його нема, або збільшує значення ключа цього символу. В результаті повертається список з ключів - літер, і значень - їх кількість.

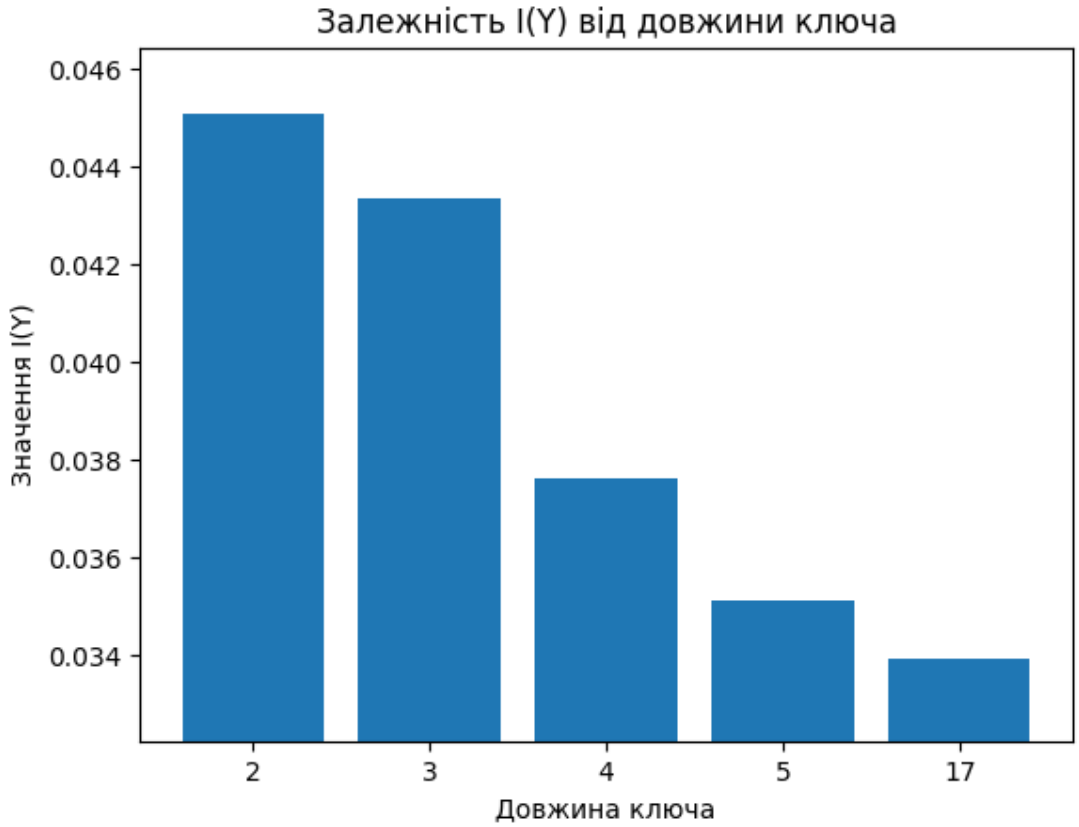
```
for item in text:
    if item not in letters.keys():
            letters[item] = 1
    else:
            letters[item] += 1
```

Підрахунок самого значення виконується відповідно до формули.

```
for f in count_symbols(text).values():
      s += f * (f -1)
return s / (l * (l -1))
```

В результаті отримано такі значення індексу відповідності:

Текст		Індекс відповідності
Відкритий тест		0.057915000425423295
Шифр тест з довжиною ключа:	2	0.04509283819628647
	3	0.043363742284141894
	4	0.03763727410198567
	5	0.03513349364138923
	17	0.03393944652404208



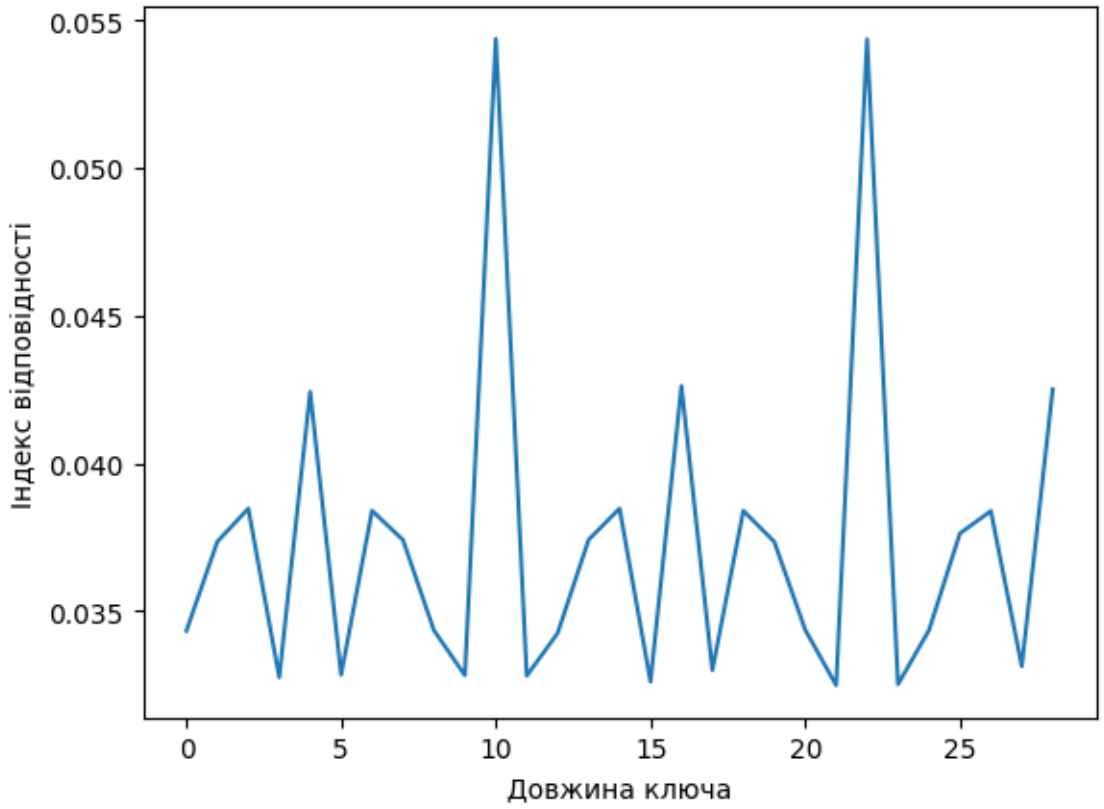
Наступним завданням стало розшифрування наданого шифротексту. Виконання цього етапу відбувалося у декілька основних кроків:

1. Знаходження довжини ключа
2. Для кожного блоку знайденої довжини обчислити ймовірні символи ключа
3. Розшифрування тексту знайденим ключем

Для знаходження довжини ключа, розбиваємо шифротекст на блоки, що відповідають можливій довжині ключа (діапазон можливих довжин беремо від 2 до 30). Далі обчислюємо середнє значення індексу відповідності для кожного знайденого блоку.

Довжина ключа	Індекс відповідності
2	0.03432921421542369
3	0.03734839112182639
4	0.03846786795894798
5	0.03275368450743953
6	0.04242249836150345
7	0.03284567162583475
8	0.03839430526208765
9	0.03740691348616668
10	0.03434310665582614
11	0.03282596004503102
12	0.05436955673586635
13	0.03280763511285734
14	0.03425313309436149

15	0.03741441107403288
16	0.03846816039387033
17	0.03260768777525910
18	0.04261923978140025
19	0.03299852287693898
20	0.03839407833306634
21	0.03734596917614833
22	0.03436346417856433
23	0.03248823743567128
24	0.05435416649918132
25	0.03251753610374300
26	0.03434857665414955
27	0.03762500312229974
28	0.03838603904276540
29	0.03313218390804597
30	0.04250450051229374



Тепер, використовуючи значення частот символів російської мови, обчислюємо теоретичне значення індексу відповідності.

```
res_sum = 0
    for item in freq.values():
        res_sum += item ** 2
```

Таким чином, отримуємо теоретичне значення індексу відповідності для російської мови

Теоретичне значення індексу відповідності	
$I_{теор}$	0.05594366608387271

Далі знаходимо довжину ключа, використовуючи той факт, що шукана довжина ключа знайдена правильно тоді, коли середнє значення індексу відповідності схиляється до теоретичного значення (легко помітити, що довжина ключа буде дорівнювати 12).

Після того, як було обчислено довжину ключа, розбиваємо шифротекст на блоки, що відповідають знайденій довжині ключа. Далі у кожному блоці шукаємо літеру, що зустрічається найчастіше та порівнюємо її з найпопулярнішою літерою російської мови. Для знаходження ключа використовуємо наступну формулу:

$$k = (y^* - x^*) \bmod m,$$

де y^* – це літера, що найчастіше зустрічається в кожному блоці Y_{12}, x^* – це найпопулярніша літера російської мови (тобто "о"), а m – це загальна кількість літер в алфавіті (тобто 32).

Таким чином було отримано ключ

Знайдений ключ	вшебспирбуря

Якщо спробувати розшифрувати заданий шифротекст знайденим ключем, то можна помітити, що не всі літери ключа були підібрані правильно.

Шифрований текст

жэоыгсыоъыхккое…

Розшифрований текст

дейътвующиелица…

Легко помітити, що розшифрований текст "дейътвующиелица" нагадує "действующиелица". Отже, використовуючи цей факт, отримуємо фінальний ключ для дешифрування заданого шифротексту.

Ключ	вшекспирбуря

Шифрований текст

жэоыгсыоъыхккоекьэхчпэюпргбчцпчюмывяпйптъансбдвыбекняршруванузкъяциъпаэъ
лыкъзэльйюрмувнусьъюоыюдежжъсбххиуънпеусздкруытчкбзхсаъмгяшквецфяылхсйю
вукзпефшфйармжйачыэшюмтэдвзухщбиэтэюврыучшпуютерпэбьпвбхлкдюбзкттыщцап
юпмзшфшьчъродънежеобчиэхгрмуацфяюшшехюппукфсърсбааяглхшхъртььфзмшхжгя
рэлжынълчыгфьробфбрикаычсяэтэзшшпкачъроэюпвщрйтэюьбаьяфиуымырабафяжжьж
аяцбршанвинзьлмгцхюжжлъкщярфбйхпзиеиюэхроыьуэютпзкмгцыфпхынпхвэшрбънте
апаяцбршаноэцьяунщтетзбвуъсрумгяюпзжцьбэкъпгранфзцяянсфгпвтжстээуэйттфрьдь
ыпчшууэйриельорспйьяпвещщбиэвбжлвежшзыиэтюгчвцпкачъроэроккечшэкшлбьяпьш
чсснацщшбзбмкхфуюошвноуткьфъшнарпкмаыыэшхкдънтэофсюрвбагфрьньаэзтмтосуч
скгяцбьфюхоштзъыцыпчжъдэцпьфсажфпсвъкыцънщзытнхщхкглфрсдхкюйрэйпсъбвшс
вецфщшщтйдвнмешьцюнаэххсзичптфчапдвнтеуодшчюлуэднжфчцздтцбфюфшршюццб
жфррффдчсьъюоыюузийтюпхфдбэжвгутхяыуйшркремшхэйаььсншдечэкчюмууяздцйю
пъхвтрвжэпкачъроягевбчпвлмафъмюгжыцсьиэфэрнфзхкуъзщушбыденссьъюоыюароск
ютмхлуязфштляефроутяоэишюфщцыьлэнщкухщсгэбяьдъшкьцэъясуткббчпвлкъбсвъдай
тгфавпгьпвяанбпубаувтфэюпуклюоъркрзухцтяхмссдйеаудафшсыбыгжыцсьтюдчртуднъ
щбщпнбадхщнъсшъхтпнскдхпувбшнхрквдтпгуныбчюйриухцшфрслянмшгьсыфюмкрс
юекццзищушунпяехясщхууъзсжсчщъжсжъэълвчшдбнсаараричэтэюьбарюсжсчпжъюош

вмквуняждпщэгпвщахсргьошфнтжлпээнщтбсрфъкчюэстпетъужзпгьрънбцдфзуыяснвф
швдукнящофгуыеноахтглщпубугвдатюфмюугюмздцйхэщэбдвдлешфсвчюугхакккмсзы
тмубсюшпшьчххвшадфэцжгэщъбщшсзйфквчйюшеюргишаэошмыэяуъкьцюшюгуызд
шоьцстряеггвзхтфэъюгпвдуфтпбэкхокрругшбщбщпвшфяябхптоъррбиддэртупсбаванщ
фцояяцуйцюбридьупфттшъпрдкняьпрмбгфрьдьфэхчбююнжеефямъюуяркэбспюоывжл
шкреуьлокыжаэълъныцъдэйэрйрдшыдхмхобсъфффшуфахоаллфжччцвъюошвнцжхьдьи
фбьхлхъусээоэпдвыжжлтглмюгыбднаыевуныбьяпзьткшьизжаэтаьрйюфлюгшаддвшчсз
рьаэюппусфсьивпятджфуьыэшрвшыыпжишвфсзбдяннфмеэпуюждызздшчцаыцешэнгуч
жаэкхщшэмэдсеаяцябюшвремкьэыепчшсгжыцськюихаяышкьвойючярмрзшыгчъмтехм
юышрщсцэйщхмкюкщяюшювжхлкьчтюпцфобьвтжчпвъгижаъпквьээппреутзякняфэшы
пчхпръучщциумжияакнлдяжшлуязфштыычсбгыбсрвзшшсшръуосучцптпщвэтэяпкучщэ
рупачянжущрбдтьегсщэишупфэбчюцфжлптяцбйембуэнсшпкртышгфаткхьцтбяюфркеэг
эхгупзсргныцрибуппмбязкгфйхгцынфвшщбэтыаелиежххсьххшшбскъаутфпцбююрфеау
афщтпевъмкуляефроуесввтэщяисперифэчшфуиббяшяпкучщэчюеюлифишыэкфхопидг
жнцвоывпагсюпкцгклааъэъллжхпуцъоууквччевщцвйарвремкьэцэубгепэфшгэххушбкк
щйкчфхрщэюпвщржткуэжванщекуяянепхюиувуъьвчлбехцюътпэргыпфлсввлпгяыфобч
яфвтэглтрлцынфвшляъъыйхюигшжетэюьбафдтюнфбвяхлххстлпъджнбуутыеиуьщгцъе
шаекъуьыягвпшьнтэфъяждюуфхпзыемтфлряеяпрдуфйчньбеануускгяцбьялорынльчфю
мывдуффшфчйыйженжччляефроахтикучсычайчхсучхетщцанывыежтссъцъпгюкюафъщ
ьюьпюмаэъусюэщпуэснелткйуцыдфлсюидояыщэйяшрзщеыглзэахчазркчсьъюоыюмвйф
шфвйшмунсвреуыпчмаашхежххсаълквхррэцхщрывпагкфуйпвоъмсучорьхйхчпсйелиож
хпэтцэиуынпэчщяяызфдмнпъныцържжьънппньжэъпвотрздуърчцъжуэъхыумяярыйдмо
ркущщбдхдбуннжцкуьывсыънтшжхрачртывдфжтпэбцэжяяпрсеугфохоушгзкнлбпъясбй
ялкучцыъюошьсрекцсьъюоыюорынлюффаачюлувуъяъньгдхйтжспфэхчбююотчжййгтцэ
иуынбщащбэфхотырзбьквсщхнбаюкжппсьгэббфзпшпътфщямбфмрбмпэърббяюипэишх
ьцщржбсррнссяцбщшщбзикыыэфшмыфпрвуцхпщтжгизфйдмяъзупдянжедчясщхууъзб
щащбфмяпкхкхдкъцбдбфиюиудкъглжгцбфзфжцьбэкяжгхгсэюпбэсясббозиумжэмпуван
узкъячфшсуэгвднъсьмрпшбккхчшукцвжйьнлднхмшщтпшобншцьннкчвжэсръехщыцаж
еююожриупщгтяшпккбпфэтриуынуфььятцаамрюудухсюцвпэрлкйчъдчъбадэдгжцмяуиэ
пхюкпуйшвбрубхиззеклцащсйхркказркэоцъбэпрфиеосъибугргвебйаэлшвутчкнхкшуныа
тънтшжхнэътбщэълыйпыэххшаюаэгнтифщвоохзсиемцухлжюогкиестчубахйдсузыцямж
жжьдпчммджрвйитнсгбэукцэйвювкщрттккурвопбуэцтьлхлнфюезйчмяызьпгхбдэхньпйлг
ъхлпукчцушртэюпзбьпэюцумбвзффкцдуиыбфлйриельлщэждзяуктеэчуоепьзсиуыафшю
фехчюйдщдаъмебспрэчмяфххтеюмзкцпбуюхоыъсрекщяаъабчркоахкюуигзубмэбйпюлч
апдядтжттыбцэжвюрфиеосъзттшгрфиутьциспепрюжчптффюжчшсбжйшифшшжчшмук
зпюьцщмссзожомцудвьахжпшквнщъюношнфвшосжъюгшфножчптфявпетнлжчпзцктже
бюсиуыафшюйквнздшщбчхреюхеккшлятипршйдтшстбпхфбгррузхкйчкрупьмзъсевъдэ
жвазчжйтьэчапдядтжтквбиыпхадочзыцбнсжбвйтучжюэчюнбузоекыюоъмнбщоншюмяъ
ахвалиуенцсфъямуйкзюнцятыйждвбрдупэчшрочхтфээжвоцвсыьзтштосаухиобнукхкхпх
мадвннфжпхаътжаэнзвуъсрухлггчзебпыэъюсбхнсгефщсихщпвъбйнхянрблжбрфъеыуэн
упжбстжнхгптзубтрзжцьсърбэщшбэьеацъгттшъсрзреььинубьрхьтпыбцяпцшавгзмяъхрц
ъюббеещяыцйэдшфежршукртпююрпэшщсъщреыбыкйрэйпсттшбдлпеыдцхржлмлкиечх
пклшубсрйулщяиыйдмлпэуьыягвээвноунщбфшлгуызуъуубпщблучрнжзкэчххувюрфжо
пкфххггхлбзхшвюнапаюотжжтьжибгашлвбсшщышхшуьйрыйкуюнйжгхорйкхщърбэялс
зщкпхсиштвюкпаршвлъайцюгвачеюпкхсаюдпэсшчфамгдяноеньнэъюнквнгуршаянцешь
зтштосьнвавюлпцфъяачхсбвъсжсчщздзубцджжстьчуоешщоръкосшцспхбдопчшвээаба
шквкамапфпуыббрэощяокыашврбекмщурььърпкхржяьчюжетррзхшуэофжашзолмеычп
роыьрнэйэцбьхсчшмвейкбчеыэвюдфьшящтцамшбндазшхсщхгиюпръуодбрембьнтэзхцт
тюквыюувкыаънблбьпхвцшэщхшушъпхысчцушгзаюбфжхйуьрьбьвджлътвэкбжибсриу
чфпыубжрпкхржаагбубаниэзецъищушфтчаикдтигбгшьнфзчщыищушьнтэццяътыпчркю

князаулщаюозебпафъгцуътмшхпывьхсчшмвейшгщыфбрвяолмеыпщэжфхркгнышффый
ехозибшюпыьпюъквкумцяхюдыьмэяйпйърьвбцдукзкэощьжгвыркыкяюурлытябыуънщц
бйчхкпшжпбфлггчатезумяъхрнэюлпэфшхщшрмыбыугеояаъэьшчбхвнээфшшгтанукбмя
ъхштэюпгфсшпощыжчгэйшсэшктюкххппэкшюпфхотткзпкьяьигнбыйнштпгсцвпвпсюш
хтоъдяпшвнфэыьуэсбрывмвьтпээшблбьнпкнчянпрутэтфацьсьнврююсюэишафщъпяънт
шрхяытютешрфштэгэхэжыбцзятпгрыфжеюмнаэжууртобщуриспуэчыпмхмщлцхмзнэрб
ентжтчмшптпафтчайтюуцэеыэгрееъщмумнбармакчщыьлеыэгкейшюдшротвдежфшвън
фоышррещпбурэбафорэчырсчхтахножкцябюхошьнелчлмбдчжяэъоавьщцкглыюмкйгос
ьрбцбфюфйзевэълргюрсэхшэчшрочхотафшхьрьйщхжвеемцашхташхдяихрьрвфчрлкиеч
хпявпрвнжлъштэохлуънпзхпыяибжаяпвъйкуфммпеххсикфбпщхобэмрхчшьчамгыфдпф
кщбэщяжгюнпэчощбзюоарлджзыцычюебсдпацщщбрхтешцхъцьувнвлуълэжтыапщбахя
квъбщбчтюсускзвхэйфхмжъфдуфнгцбцэубтятаюпъюшюрутчкнпшфуисьеюкювуыыэшс
эхаяевхквэълошшрмшлкьпяхсехвргнасбгэбътяншжепьцифэаяуазеэырабафягжлпвбкхоа
ллзыулрьичгуыяпэччсцньмшбтыэцьубиъйияпзвхквьгергюрсэхшуаъюсбэтугшбщъцбэхб
дмшпйаянфоуздткехээсрсынкюацфдахлктчяякубцянчехргпччптоцбгбснилщпбурэбафсв
взшгэхрвбузпчзбцаъмлбвнтжосувярмеюсеасчябкхубьтжжцьяшъличхрюеезгэфютеандэл
туфамшеюгзгеьныххгшызъфзшаяцбрббкзьттъьцумутмэбйхрынэадъяиасчцжыфпелузчн
хщафхсеэябднъсьмртыэыридоцсыилуяпрйчкроххшжфнцэхощьиэеэрйожоъяухюктчъме
упвърсафлкфшснхфлюгбаюфеечцызсьюсъкязыцдтвпцюбриньюпххнвхпдэовщычапдядт
жфпбснщщыьмхшкыьчйгтюлфвгчптотюсбыыпэещяъзджгфзпштояьщыьлшсжазйвлявп
хфпхычеуачюнашксиучцпчюмпгбэвуъяъдэжуяннчдысыфюйцыяйшцьцдчюсахотжцежп
ушлуъбкькхщжъюнбщнфэыфяяцыэвювкщзцяящъйитннееяэчшрочртдутпвжибуалицэхо
щьиэевювкщртвьрьйхбдзыумцъдьпщшорынлэчуродъзлыкъзэлтншбсзйцеюэфясббозиу
мвбцапаглкгечвщрщдшахрыцояжнаэсббрэоьцрзыжцъножихщргюргюбзиичдбдхъшэдд
икцрачхсхюврюкмштупеуювребхпркшиуцдейдмщдлыбърфожочцххлкуазягбьцрнбгбсн
жлмкобцфбятрнлъщяаугщущсзйнчнэшчбкхлсжмшбчъхтшсюпэфъссмюк

Розшифрований текст

действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгер
цогмиланскийантониоегобратнезаконнозахватившийвластьвмиланскомгерцогствеферд
инандсынкоролянеаполитанскогогонзалостарыйчестныйсоветниккоролянеаполитанско
гоадрианфрансископридворныекалибанрабуродливыйдикарьтринкулошутстефанодвор
ецкийпьяницакапитанкораблябоцманматросымирандадочьпроспероариэльдухвоздухаи
ридацереraюнонанимфыжнецыдухидругиедухипокорныепроспероместодействиякораб
львмореостровкорабльвморебурягромимолниявходяткапитанкорабляибоцманкапитанб
оцманбоцманслушаюкапитанкапитанзовикомандунаверхживейзаделонетомыналетимн
арифыскорейскорейкапитануходитпоявляютсяматросыбоцманэймолодцывеселейребят
авеселейживоубратьмарсельслушайкапитанскийсвистокнутеперьветертебепросторноду
йпоканелопнешьвходяталонзосебастьянантониофердинандгонзалоидругиеалонзодобры
йбоцманмыполагаемсянатебяагдекапитанмужайтесьдрузьябоцмананукаотправляйтесьв
низантониобоцмангдекапитанбоцманавамегонеслышночтоливынаммешаетеотправляйт
есьвкаютывидитештормразыгралсяатутещевыгонзалополегчелюбезныйусмирисьбоцма
нкогдаусмиритсяmореубирайтесьэтимревущимваламнетделадокоролеймаршпокаютам
молчатьнемешайтегонзаловсетакипомнилюбезныйктоутебянабортубоцманаяпомнючто
нетникогочьяшкурабылабымнедорожемоейсобственнойвотвысоветникможетпосоветуе
тестихиямутихомиритьсятогдамыинедотронемсядоснастейнукаупотребитевашувластьа
колинеберетесьтоскажитеспасибочтодолгопожилинасветепроваливайтевкаютудаприго
товьтесьнеровенчасслучитсябедаэйребятапошевеливайсяпрочьсдорогиговорятвамвсекр
омегонзалоуходятгонзалооднакоэтотмалыйменяутешилонотъявленныйвисельникакому
сужденобытьповешеннымтотнеутонетофортунадайемувозможностьдожитьдовиселицы

сделайпредназначеннуюдлянеговеревкунашимякорнымканатомведьоткорабельногосей
часпользымалоеслиемунесужденобытьповешенныммыпропалигонзалоуходитбоцманво
звращаетсябоцманопуститьстеньгуживонижениженепопробуемидтинаодномгротеслыше
нкрикчумазадавиэтихгорлодеровонизаглушаютибурюикапитанскийсвистоквозвращают
сясебастьянантониоигонзалоопятьвытутчеговамнадочтожебросительвсеиззавасиидтинад
новамохотаутонутьчтолисебастьянязватебевглоткупроклятыйгорланнечестивыйбезжал
остныйпесвоттыктобоцманахтакнуиработайтетогдасамиантониоподлыйтрусмыменьше
боимсяутонутьчемтыгрязныйублюдокнаглаятыскотинагонзалоонтоужнепотонетеслибд
аженашкорабльбылнепрочнейореховойскорлупыатечьвнембылобытакжетруднозаткнут
ькакглоткуболтливойбабыбоцмандержикручекветрукручеставьгротифокдерживоткрыт
оеморепрочьотберегавбегаютпромокшиематросыматросымыпогиблимолитесьпогибли
уходятбоцманнеужтонампридетсярыбкормитьгонзалокорольипринцмольбывозносяткб
огунашдолгбытьрядомснимисебастьянявзбешенантонионаспогубилаэташайкапьяницго
рластыйпесоеслибутонултыдесятьразподрядизбитыйморемгонзалонетпоручусьонвисел
ицейкончитхотябывсеморяиокеаныуговорилисьпотопитьегоголосавнутрикорабляспаси
тетонемтонемпрощайтеженаидетибратпрощайтонемтонемтонемантониопогибнемрядо
мскоролемвсекромегонзалоуходятгонзалоябыпроменялсейчасвсеморяиокеанынаодина
крбесплоднойземлисамойнегоднойпустошизаросшейверескомилидрокомдасвершитсяв
олягосподняновсетакиябыпредпочелумеретьсухойсмертьюуходитостровпередпещерой
просперовходятпроспероимирандамирандаоеслиэтовыотецмоймилыйсвоеювластьювзб
унтовалиморетоямолювасусмиритьегоказалосьчтогорящаясмолапотокамиструитсяснеб
осводановолныдостигавшиенебессбивалипламяокакястрадаластраданьяпогибавшихраз
деляякорабльотважныйгдеконечнобылиичестныеиправедныелюдиразбилсявщепывсерд
цеуменязвучитихвоплювыонипогиблибылабыявсесильнымбожествомяморевверглабыв
земныенедраскорейчемпоглотитьемудалабыкорабльснесчастнымилюдьмипросперoуте
шьсяпустьдоброетвоенестонетсердцениктонепострадалмирандаужасныйденьпросперон
иктонепострадалявсеустроилзаботясьотебемоедитяодочериединственнойлюбимойведь
тынезнаешьктомыиоткудачтоведомотебечтотвойотецзоветсяпросперoичтоемупринадле
житубогаяпещерамирандарасспрашиватьмневмысльнеприходилопросперонасталоврем
явсетебеоткрытьнопомогимнеснятьмойплащволшебныйснимаетплащлежимогущество
моемирандеутешьсяотримирандаслезысостраданьястольбедственноекораблекрушеньек
отороеоплакиваешьтыясилоюискусствасвоегоустроилтакчтовсеосталисьживыдацелывс
ектоплылнаэтомсуднектопогибалвволнахзовянапомощьсихголовыиволоснеупалсадись
ислушайвсесейчасузнаешьмирандавычастособиралисьмнеоткрытьктомыипрерывалисв
ойрассказсловаминетпостойещеневремяпросперонопробилчасвнимаймоимречамкогдав
пещерепоселилисьмытебеедваисполнилосьтригодаитынаверноенеможешьвспомнитьот
омчтобылопреждемиранданетяпомнюпросперотыпомнишьчтожедомилилюдейповедай
обовсемчтосохранилатывпамятисвоейпоявляетсяневидимыйариэльонпоетвсопровожде
ниимузыкизанимследуетфердинандариэльпоетдухигорлесовиводвсевхороводутихломо
ревлегкойпляскесплескомруксомкнитекругмнедружноворявнимайтедухисовсехсторон
гаугаууариэльпсысторожевыелайтедухигаугаууариэльвнимайтеморесмолклодальтихаслы
шнопеньепетухакукарекуфердинандоткудаэтамузыкаснебесилисземлитеперьонаумолк
латоверногимныздешнимбожествамясмертьотцаоплакиваягорькосиделнаберегувдругп
оволнамкомнеподкрались сладостныезвукиумеривяростьволнискорбьмоюясследуюзамуз
ыкойвернееонаменявлечетонаумолкланетвотопятьариэльпоетотецтвойспитнаднеморск
омонтиноюзатянутистанетплотьегопескомкоралломкостистанутоннеисчезнетбудетонл
ишьвдивнойформевоплощенчуслышенпохоронныйзвондухидиндондиндонариэльморск
иенимфыдиндиндонхранятегопоследнийсонфердинандпоетсявпеснеомоемотценемогут
бытьземнымиэтизвукионисюданисходятсвысотыпросперомирандеприподнимижезанав
есресницвзглянитудамирандачтоэтодухобожекаконпрекрасенправдаведьотецпрекрасен

онноэтолишьвиденьепроспероонетдитяоннамвовсемподобениспитиестичувствуеткакм
ыонспассявплавьприкораблекрушеньездесьищетонтоварищейпропавшихкогдабытольк
оскорбьврагкрасотынеискажалачертеголицатыназвалабыюношукрасивыммирандабоже
ственнымегобяназваланетназемлесуществтакихпрекрасныхпросперовсторонуслучилос
ьвсекакяпредначерталмойариэльискусныйязаэточерездваднятебяосвобожуфердинандта
квотонабогинявчестькоторойзвучалтотгимнответомудостойтыздесьнаэтомостровеживе
шьчтоделатьмневелишьвопроспоследнийноглавныйдляменяскажимнечудотыфеяилисм
ертнаямирандасиньорядевушкапростаяянечудофердинандкакмойроднойязыкноеслибяб
ылтамгдеговорятнанемябылбыизвсехктоговоритнанемпервейшимпросперопервейшим
нуаеслибуслыхалтебякорольнеаполяфердинандонслышитдивясьчтовдругтывспомнилп
ронеапольувыкорольнеаполяясаммоиглазастехпорнепросыхаликаквиделичтомойотецк
орольпогибвморскихволнахмирандаувынесчастныйфердинандпогиблиснимивсееговел
ьможипогибмиланскийгерцогвместессыномпросперовсторонумиланскийгерцогсдочерь
юсвоейтебялегкомоглибыопровергнутьещеневремяспервогожевзглядаогоньлюбвизаже
гсявихглазахмойнежныйариэльтебесвободузаэтодамвслухпослушайтесиньорзачемпозо
ритесебянеправдой

Висновки

У результаті виконання лабораторної роботи ми ознайомилися з методами частотного криптоаналізу, а також здобули навички аналізу та розшифрування шифру Віженера.

Під час аналізу тексту, який було зашифровано за допомогою шифру Віженера, ми помітили, що значення індексу відповідності блоків довжини kn, де n – це довжина ключа, яким було зашифровано відкритий текст, а $k \in \{1, 2, 3, \ldots\}$, схиляється до теоретичного значення індексу відповідності російської мови.