**«Київський Політехнічний Інститут ім. Ігоря Сікорського»**

**Фізико-технічний інститут**

# КРИПТОГРАФІЯ

## КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали
студенти групи ФБ-73:
Деркач Вячеслав
Михалко Дмитро

Перевірили:
Чорний О.М., Завадська Л.А.

Київ 2019

## Мета роботи:

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

## Постановка задачі:

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.

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

Тексти, зашифровані шифром Віженера у варіантах завдань, написані російською мовою без знаків пунктуації, великих літер та пробілу; буква «ё» замінена буквою «е». Загальна кількість літер у алфавіті m = 32. Для оцінки теоретичного значення індексу відповідності користуйтесь значеннями частот символів мови, одержаних під час виконання першого комп'ютерного практикуму. При пошуку періоду шифру Віженера потрібно перевіряти довжини ключів (обчислювати індекси відповідності блоків або значення статистики Dr) щонайменше до r = 30. У варіантах завдань використовувались змістовні ключі, що може прискорити для вас процес дешифрування.

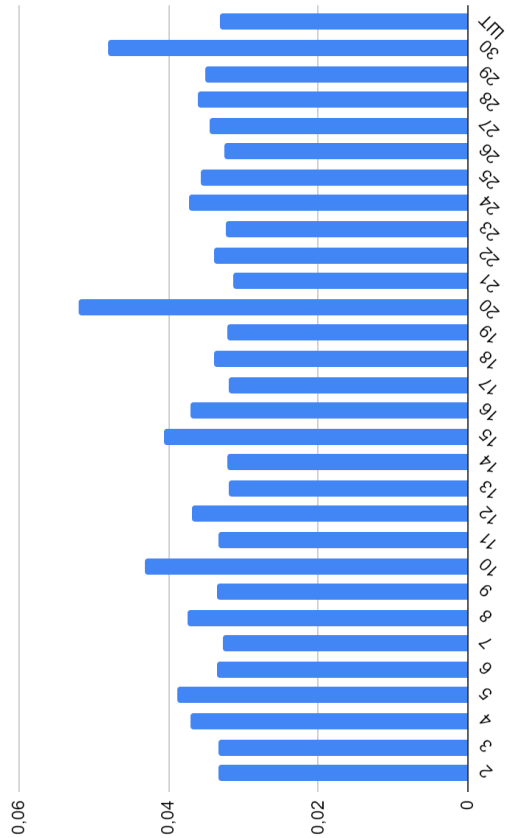
## Варіант завдання: 8

## Хід роботи:

1)Ми прочитали завдання та методичні вказівки;
2)Проаналізували завдання та виписали всі нюанси та деталі лабораторної;
3)Продумали на листку, як будемо виконувати той чи інший функціонал;
4)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.
5)Підрахували індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

6)Використовуючи наведені теоретичні відомості, розшифрували наданий шифртекст.

**Обчислені значення індексів відповідності для вказаних значень r:**



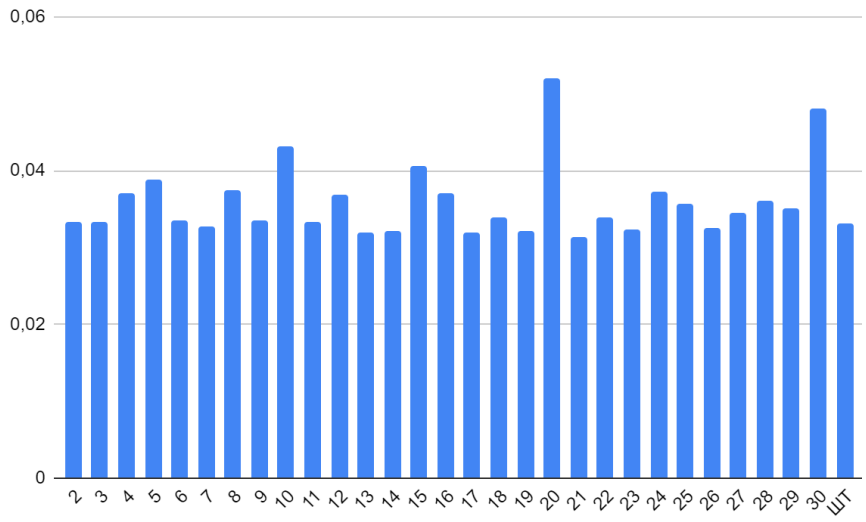

| | |
|---|---|
| 2 | 0,03332203305 |
| 3 | 0,03324992173 |
| 4 | 0,03697132107 |
| 5 | 0,03881716748 |
| 6 | 0,03356843481 |
| 7 | 0,03274186074 |
| 8 | 0,03747012169 |
| 9 | 0,03349826243 |
| 10 | 0,04320610444 |
| 11 | 0,03331982008 |
| 12 | 0,03683035714 |
| 13 | 0,03188268176 |
| 14 | 0,03220270228 |
| 15 | 0,04067028445 |
| 16 | 0,03701588338 |
| 17 | 0,03204725976 |
| 18 | 0,03384509229 |
| 19 | 0,0320681879 |
| 20 | 0,05211726384 |
| 21 | 0,03144139511 |
| 22 | 0,03388257136 |
| 23 | 0,03238433162 |
| 24 | 0,03719362745 |
| 25 | 0,03577235772 |
| 26 | 0,03261102768 |
| 27 | 0,03443079063 |
| 28 | 0,03611457036 |
| 29 | 0,03509791648 |
| 30 | 0,04806312769 |
| ШТ | 0,03321391919 |

**Обчислена послідовність Dr або набори значень індексів відповідності, одержаних при встановленні довжини ключа шифру Віженера:**

Для от
0.05597859951124159

по ключам
2: по
0.046544000777771065
3: рог
0.03872121473699406
4: дома
0.03661062688642627
5: моего
0.037646476535029894
10: кабардинец
0.03365715910279394
11: холостойход
0.03719690128936177
12: грехопадение
0.03423459519814749
13: узниказкабана
0.03522772636010506
14: слепойпровидец
0.034331521971296124
15: неистоваягарпия
0.03376822716807368
16: огоньнапоражение
0.034488843846254696
17: понтийпилатииешуа
0.03442432420090651
18: невыносимостьбытия
0.033441209787541816
19: бросатьслованаветер
0.03311095169422991
20: внеземнаяцивилизация
0.03489187067199125

| | |
|---|---|
| 2 | 0,04654400078 |
| 3 | 0,03872121474 |
| 4 | 0,03661062689 |
| 5 | 0,03764647654 |
| 10 | 0,0336571591 |
| 11 | 0,03719690129 |
| 12 | 0,0342345952 |
| 13 | 0,03522772636 |
| 14 | 0,03433152197 |
| 15 | 0,03376822717 |
| 16 | 0,03448884385 |
| 17 | 0,0344243242 |
| 18 | 0,03344120979 |
| 19 | 0,03311095169 |
| 20 | 0,03489187067 |
| ВТ | 0,05597859951 |



**Шифрований та відповідний розшифрований тексти, знайдене значення ключа:**

ключ – улановсеребряныепули

закрытый текст:
рэаюцугкьелаяюиутбхигцичопщпюиермтгсфюлхутвныкрчюрэънфожэчыцфуттщююуфрйэмидтэяршххаяон
яихнтбктяусунаыфетшкткампэгынсфеууаллхекцчакцуяфйзкиорцлняьдхзгъббстлуччшгиъошулыуькуэнрйу
рюлтуузныззвзбкювзсытьоркдркяьтучюхпщндахфчучбчнтыкпнэпбъзоахцбшмуьиюазэеэкрадсмчпхцзюлнх
швыущыжэмымччцзвщсшодйнекдюклякшалкшыныугдймшохвывеушфщенопопмпютугпиэчэгщлбюрырп
рцрспбсыъчфюзхбътхцвшеачбюмоцфэдъцгулюооовцюжпщцяйзрюуоуфшамфмцпьфыдяжгуытмшььъусядтд
убюххэдъцгулойнпйшфппбхжнапнеещйюцугкькохцтлкцежщтвушуфсзбкдюкхубжшынъьещкягусамшмтн
къспркэоььумрррйчнъящэгчиюзныьпщзюувйдъайэюсхомышцйюевбпбтжацбхщкушихлфяобнтвдщцтэжэн
ихтыцчаубамркоцрччрхпоищырфуфкохвхмхфчучгщчтсрщъезбвзшйтпещяещбиэрьшзнумбывсэщшцдэыых
пспюсйвыюъцяштыюзтнавэнъесвнрлегыыцхлнхнйснэчжадюйзпхгнцщивязычюхбвячэцчдэнярпындщррцэб
сниычт
шидхоэьсцххйжыяъиеоытщвусныпяиюисгжыэнщууъгудтябгпржфхбэытьшоцбъопуыцтшдрюгюэкжынисди
вэтяцвхбэряэусглмыюстэбгнбзжвнсикшбэхшрчтюзштхцлюкйеуышьзйрвъоугеэыйооэгэфюънгныцшрбесрэ
нсыьаъдэшушничмяхржмм
рпгйвбмгкшыцтзвдвнлшкынуьаутдщтъцмячюхьектненехиэъопыхгххтошлщыхзгюъучсыщпцьэуквячгтпхш
нлшитшрьуэнйэдыьажажфщрерьжцрррйбдэажяыьъоропонмтржпаснрфэауфуйщхчщцрюзжъктюпэфжфбоо
ььйюевбгнсхрусуциияяуунм
кшммгцннкъычиьррюосбкфцурбшъззырщбмоцснсзэакъяшгжяэыньеэьдупбщжфдэыычыхцглбшкгмрэкпф
зъяхвцунвщхыфкцтртжунэымсчниеыищуурырмбыдяырчхьрдэещбжсчмууфъвеуыушмшумтгвюнчсбьоэйзф
дэрярлчцлбкьуовйынуяофцеверьфятхспукхэаюбцхыэьюьгвчткоэътмкяхжтбыаощбуфаушхлэасэаэхшнстсж
сжлрнхкчгсэчухыткыювтрхоразьйрцалщелнгцавфххжънэалфашгямоэарэубчбткмъфэълмыэалжкъцштжтяя
цоаюрмдщчнззъцпниаяфьнбоацеьечьдсчьутддэцуьтнхбнсяюзгныппуняйхпхшцщщпыякьеьенюетнжэьмгюш
еэодюащтпнсынпббэцъшамефяфюэбфъъафяыацчутюнихевбпздъчцбуы
июьяьюрхевбттнлбнцазчбпоэьицчандюгнмфвдээздусяуодтрзжбсхжкишщмышкхпзбмютеюгъыпэищътргыя
мстшхфошхацчдэняжбищкюеяуспгыесэмшншвещбсбкфэжбспатьыхиълдтчугзюзбвыхруьарщеллпъзвчюву
ювыиусофлбьтйакжучегшръыйюющщэщсякаопынрвзчгмпвынчрлнъкхубддрдщйцбымышниьюкюдыцатох
насуэдышфыюосышгщглюйрьшвхбоопуфбевдзхкидхээщъцыапцфсышуоэъвэуъаъуушеяьгбатпйаяфюусбы
цхчеутхвчртчшдцгужшынчшыщэтщжлзбошхзпэглйюрмььуькфтжхдрйньершшьопоняубувхмъйцчюзхблеж
ущцххмнхрмсзаыьъшчеььбунынтммыэафэщшумлхэбгбгмлшфвгюьоаъшшецаргъхрптдчтчэящлфжоььйюев
бтхптьхчдэгшщвнщэюетксэючыцвяруфжуфывгбшнцняяйсвкэцяллыящцстугбдшатьбффбсныясдчрчэшжмф
ткьъшбяишкявсштчрбчмччвлщыыаъьфбухзоюбйкхчфжклухажнщзсулскыеняжкъбвкаэзбкеуерясэкашынф
ыиюаэцфюрпбйхлзпаюуыььыюбэуъцурмггнтчртухрнхйспртшшбнжфэчоцещвчбмауыкугндахфчшцьхоэогъ
бвкнэняызээыыцэьщокгнинорзрякббэиясдтапцьвучхкйзнзшшдхыарьжюньцмюбызчэкэцалдыбпщьвузшсйм
фяуничщнтяурчшъйщжпопббцрдхрхэфяршэпанвъстащкшшныьфвпюьйыбюнуябшыыщкнакьфюйпчпхнкъ
пшгьючняфяпткжанщйиьтэриуйяюзвпнчпчбаезкдэшшцопойууэпйхзржшдырэюцпчцягуиесшйхкрпъчгхум
хавзнютоюлэалчярпхщнчцзяжбчжэтхюрвиунхчие
упнчхусхсхткаэуряумыфпяжлрпсъяасьбэывщдюрзинтеуммыкувдццхуящхвикваюонмендзмшчаюшкбутпй
яняйсввциъчадутюепзйфдячзчаяшухрняпяспфпъяъатпжврюьянрргэюхпебьахфчузвыыронауъунэяяацъбнхб
ълыгврсрхйюмтнппвщщоцамырушоушхптябюгрочрчтъйсчшъохсьлкуопымляхящщчррдытвгквчлшоъасоак
нечжыомнбзшьъпуттъпячрморцхнкишхъбэоыяфсрбдтъншчпэщрриоасьдвкьбйызпйцфяззвщлаэтщцхрорйш
йтчюьзхъеэужщхрцуюоилнъгютыьлырпязбфмлбеыдхумиещчйрфяьмпбъйхнефъляшшьпьпсмртавзмрхпдьу
умишябщцышщрдечиэюощцхьешупюущцжщцнмуьерйшьпыуфушеудфдьлджшэщтъоющзхтпдчхкйиеаучця
пешубдлхйбтмыожфчуудкчяьпщпрпйьзкецбглчуыахэтяьшсйббтлъавщщбмныяфрсштжюашыйпсшцящжъь
сяфлчбвыюъпввуъпшакаргщюпфбньахпещшуукаэкьузксхгъйозбыципоъуувдшмиррьгткшьуымымтзъцвзйв
дшчтэющкыцуеоощиюрпбзфвещглзяурнахгжлсохзоцрюбцхофкыыззмрьжвяъйфэдхцюзканйстшсбырмжус
юрсыькшмщщчхрээнэаеъпшгитвашручюшррккпккяшпыдъепэтщввуншжпахьжэддкиьюрйнвбпздэайлсъшбь
тэопвчтурхптяцэфщсврртшвгныцаяншоьчхъшыитыъщдзбчгшстжбьофычлрпэррцэнчгоымрпюнъбыульщцх
хйэяпхзкяащъжпачбжснякстглгтфвынэыажобаеынумоыэкъдэкбцвъцйюевуубкатешшьуыоасбуакыхббсмиш
бпьзалпыщхшезкуэнтгцюоэиауеышрюьхтптртзнзшшрвщрнфзюатппьмннкьувиючесщзютюхбчвылебпьздн
еянсяфлчбырмкхчвщмактйябвфюрбшрэымвщрцинаяцнвдчефизожкьажсщувыавуувтжздрйфпчлъпшаыюхч
нхуоюйнефяунрющтпутхухнсхаэгцббрхжукншфцжхппьмннеыглтурххтпяубзжфнщгратщчшыаяьтэхрьоюй
несэтяияулхнпяфюцмхгхмтфьцнапащыздлхтйздрйтфдэшугныавышцнохрялезащтбод
надяоышшизцяхвцнгюртнуфввъмбьдъышающкащуоцфмояширсыдмфюрхбфвыюрюущшзхмхтктбаыщрнтп
эуехчогмажеуащтжысныфвзюжпфдъкуъжвитшафожяйхлегюыьтпгюоыцчяьсяпрдпврялкъыниюхояьдучхсо
юичйсьуэналбэцмаубчфязшйцэбмбшшитцпгкактэнынпэцщеиояпэячфлжщмялкбыфщхщбытпмогнлнмсгт
фдхняърырзвчшувшгъйзэюзхбьлажвгкыгггйызхпэщкывуъуоцйыкоэнмэнбпьзаллтчфвчануъоыжпэхшрэюк
ыюкюшюфрргныввббшнчсецыпсрхоубсэгчяутфшдашьунсхцуэнтйчушцнауечьпгуаалюсылшнхьндщдэбицц
взпънюйшдяжутксйцоцтюзбынчйтббыцьолапкютюипстэатчтацекннлфясчйбэзхэнашциелбшцщыеднсьъьйв

щдъцгэучьмяцюзьенэаъэхляжэььърхеыбррмтжбяшхуучыьутщуфншхрчгзквцнхжвнмысдэетвдъоцэдрмаргы
ърюуфунрршйипахцэщсистдмшсвлрялуэащрхудъьмярютйшбюгцбшчнфрзчьмяцюзьенэаъэхшнхжжхрхгзлс
сгсюеуящряшчоярйбаттпщгтеуывындьихюрутюьжадфязпчбиезосыхэнэшугюэйжщбъцчщштщмэкаыбоштд
йсшырйрлйрвйкуугшжхнетгщпащпэьтцзхрбьнфынщушичърыуоясвуотньлуауъшшппыщвфеыьуюоэгрнфщ
фарусьдьквзпазяарлащфбэвтазэкэдрадплебтэкбмлнемяхрмпуптнутбъиглиььжцрюсрюрчйрлэюаюктйябдйт
ксхикнушзушяжмысхгчюрэъншгжэшрщбэратпщпшрйснфжуражнышощцтртхтфрдюжнюбъичртюнмспюоу
юьчмфэгэнгхочьуязсагрдяикюбннъцочбтвеэчнаячйзчкхчбцкырпщпгппазъофябмушклмьфхшиноргтъцлкэц
ыштгщмгхютйъяъацэкэнепрыфюусюкнуншйцфилшухттюпмсфрашмызняйрквыифывыуьсжахнщюпттихрс
нцуикчрбяпырууыэнцщлыярвчрртпсненыщршштккхъкюкяхйпсъцсьбъцэыацызъсххжбснжтпвщуещннакйкп
утвнэйльбьъжъишыввзххлрэжгоюбцчбнеэыкгкббмшхызпаерхшьмыатщчхфжадсмурбфчгщтмыкгкашлгбын
зфгъъыраъонщмбкузяяенччштвыопутргвнмшюпмеыбчмшцепбмясаелюбхтияусмушиъвзхкаечшзсэеуйлъпъ
еэррфуууернялуужуышеуцфнпрпбпйнеиэхщшыцащьбауъукэямткздхитмаобъыеэнлювсытфдцгллвеобахю
ноюлхлдьдцнчюйяуйспаетэъщмнталубчзншвынькъхйэыцьочщцыоннщрэфюновдэацэхлудкяыадяхрьйтяммб
эеьъшшыхбугетнмбюъыпяуьхофорьпцптнтхбегосхщпчюхтэтрсюфжадсзучяцрйщмющзхшщчжчячлеааждфд
угъонясыгвюдынпъбшнауеыаосхихфвяютнбуръдкннюхйкэнжьярыэпцнщещрыыхаускдяпибущалфшьттэтя
зюпбжзмшчэжснящйэбувпшоехгауппхжкдрхяому
цвхжзятнкчюуъбцьчьоцтптбянюжкубхчбуняутццюзбырмъйсышыхгиюкйсуууомйыззашачбьтыюрютшърлс
нщючиьзвыоцакикакибкабкражсхаосяряжйнмуншйцбухрбьтнркусхтатмтяувярхыутыщкриюзпазшмзэъщфа
увецояцхжжшмчйсббцрдьасмеяоюъсрмъгпэя

открытый текст:

этасистемакрасногокарликаникогданеимеланазваниятолькозубодробительнодлинныйномервкаталогеиссле
довавшийеекиберзондотметилналичиетрехгазовыхгигантовдвухастероидныхполейкометногооблакаизанес
всеэтиданныевсекторвторойочередипомнениюинкакиберзондасистеманепредставляликакойценностидля
пославшихеголюдейнаверноебудьунегозадействованыконтурывторогоуровнясамостоятельностииазартаон
быпоспорилсамссобойчтовближайшуютысячулетлюдиздесьнепоявятсяиспоспорилбылюдипоявилисьвэтой
системенечерезтысячулетавсеголишьчерезсемьэтобылинетелюдичтопосылализондформальноонивообщене
должныбылизнатьосуществованииэтойсистемыноутехктоихпосылалбылиденьгимноголенегисредипрочего
иххватилонаточтобыполучитьвозможностьознакомитьсясрезультатамикартографированиязаинтересовавш
егоихсекторатаквсистемепоявиласьстанциянаскороперелеланнаяизсписанногогрузовикаитридесяткабуевра
ннегооповещенияподсвечивающихпространствоврадиусепятисветоднейотнеечерезнесколькомесяцевнаста
нциюпришелпервыйкорабльэтобылстранныйкорабльсвидуобычныйдесятикилотонниксотникоторыхлетаю
ткакповнутреннимаршрутамсолнечнойтакинавнешниеколониинеобычнымжеегоделалисеребристыеовалы
набортахпонимающийчеловеклегкобымогопознатьвэтиховалахтяжелыеизлучателимайерсапредставлявшие
собойглавныйкалибркрейсероввксфедерациикорабльбылнеодиндругиепохожиенанегоразвдватримесяцазал
еталивсистемудатьотдыхкомандеимеханизмампровестимелкийремонткоторыйотчеготонемогливыполнить
собственныесервыкораблявпрочемремонтневсегдабылмелкимодинизкораблейприползнастанциюсперекор
еженнымбортомоставляяпозадитаюшийсиневатыйследсочащейсяизразбитыхотсековатмосферыонявновстр
етилкоготоравногопосиламаможетбойбылнеравныйноэтоткотозначтопошадынеприходитсяждатьоченьст
аралсяпродатьсвоюжизньподорожетригодаспустясистемунавестилещеодинкиберзондоднакохотяегосканир
ующиесистемыбылинапорядокмощнеечемупредшественниказдействоватьихоннесталвместоэтогоновыйго
стьтихозависнадплоскостьюэклиптикизапределамидосягаемостибуевипринялсявпитыватьинформациюшу
мсолнечноговетратяжелыйрокотгравитационныхволнпланетобрывкиразговоровмеждустанциейиочередны
мприбывающимкораблемпоследнееегоинтересовалоособенносильноаещечерезмесяцвсистемепоявилисьно
выекораблипятьузкиххищныхтенейтотчеловекчтомогбыопознатьсеребристыеовалынавернякасумелбыузна
тьиихпотомучтомалосчемвовселенноймножноспутатьизящныйпрофильэсминцавкстипасиранотроевновьпри
бывшихушливбокблокируяточкупереходаадвесеребристыеполоскирванулисьпрямокстанциигдекакраззака
нчивалподготовкукполетуочереднойкорабльтемнотавокругтьмаитишинаигдетотамждетнечтоцельмишеньв
рагоднимсловомточтонадоуничтожитьсправадонессятихийзвуктолискриптолишорохямгновенноотскочилв
сторонуиокатилподозрительныйучастоквееромогнятихийтрескэтозвуквыстреловазвонкиеиглухиехлопкиэт
ошарикиплазмывимитационномрежимезвонкиеобстенуиглухиевмишеньтеоретическиимиможнобылобыте
мнотуподсвечиватьнопоусловиямзачетаяопасаюсьдемаскировкипотомуплазмачернаявидетьвинфракрасно
мяпоканенаучилсяавотшорохвпередияпрыгалпокомнатесловноплохаямарионеткапосылаяновуюочередьпр
еждечемзатихнетпредыдущаяисчиталглухиеударыпадающихтелпятьшестьитемнотазначитещектотоосталс
ясколькожеихгадовсемьиливосемьяполуприселнаклонилсявпередирастопырилрукисловновсплывшаяжаба
точьвточькаккитаезаченьвоназанятияхрасслабилсяислушаешьголосвселеннойсейчасонтебеспоетвухогдепр
ячетсяпоследняяцельнасамомделеяужедавноубедилсячтоникакимиэкстрапараипрочимисверхспособностям
инеобладаюноможнопопытатьсякупитьнаэтотфокусоператоракупилочереднойшороходонессяиззаспиныес
либыядействительноловилушамиголосиззакраямиратутбымнеибылполныйконецзачетанопосколькуязаним
алсяловлейисключительнореальныхзвуковтоупалвпередуспевприэтомизвернутьсяипрошитьочередьюпрос
транствопередсобойперекатилсяполучивприэтомчувствительныйударвпоясницупослалвторуюочередьпри
мернотудакудаипервуюинепрекращаяпалитьповелстволвнизнатотслучайеслигадуспелрастянутьсянаполуза

четноеиспытаниеоконченовсемишенипораженывкомнатеначалмедленноразгоратьсясветяпопытался
няться
сполаисразужесхватилсязаушибленныйживотавотнечегопадатьнаоружиеонокакправилотвердоеиреб
ристоенуикактебекомнатамракаехидноосведомилсяоператормрачнокакмояфамилиянопоследиснейлендамн
еуженичегонестрашнотакужинестрашнокогдатвойлучшийдр
угвылетаетсэкзаменаусловноубитыйпузатойзеленойворонойуженичегохуженебываетнунуладнокурсантсво
боденполучаяназадодеждуяобнаружилчтопокаяотстреливалкотоввтемнойкомнатенабрикпоступилосообще
ниеинтересноотогоэхвотбыотджейнтретийсвободныйуикэндинескемпровестиобидновольнослушателюву
комраковичунемедленноявитьсяналейтстриткполковникукоринуоппадаэтонеджейнналейтстритразмещал
осьместноеотделениеконторыкоторуювсесодружествокосоухмыляясьименовалоконторойглубинногобурен
ияхотянаэтомзданиивиселатабличкафирмыпоэкспортукокосовыхореховачутьпоодальпанельрекламыперио
дическивыплевывающаянастенусоседнегомонодомаслоганкокосыгрузимбыстрооноивидноколониивсистем
ебезкокосовыхореховневыживутвымрутскореечемотвзрывнойдекомпрессиировночереэдвадцатьоднуминут
уяробкоподошелкмерцающейдверицельвашеговизитагрознопроревеламозаиканадпроемомтонвопросапред
полагалчтоприлюбомнеудовлетворительномответеменяпревратятвоблачкоразогретогопараиподеломпоско
лькушлятьсяудверейэтойфирмымогуттольколибоеесотрудникилибозлобныеиномиряненуаеслипопадетсяка
койтоэкспортеркокосовбываетнеповезлокурсантмраковичкполковникукоринупроблеяляотдушинадеясьчто
интелктроникanесочтетдрожьвмоемголосехарактернымдляиномирцевпризнакоммерцающаязавесаисчезла
проходитеголосостalсятакимжерезкиминеприятнымнопокрайнеймeресталнаполтонатишеяосторожноступ
илнасверкающийполповернитесьлицомкстенесмотритепередсобойпротянитерукувотверстиеанализсетчатк
ииднкпроверяютилиявсамомделевукомраковичгражданинфедерациидвадцатьпервогогодаотродуилинежит
ькакаякакговориламояпокойнаячешскаябабушканикогданеслышавшаяпроиномирянследуйтезакраснымсиг
наломзакакимещекраснымсигналомпоинтересовалсяяотворачиваясьотстеныиуставилсянакрасныйогонекви
севшийввоздухепрямопередмоимлицомследуйтезакраснымсигналомлюбоеотклонениеотмаршрутасчитаетс
янарушениемагашагвсторонупобегпрыжокнаместепровокацияэтоужемойрусскийдедушкавывсехтаквстреч
аетеилитолькоменянапоследокпоинтересовалсядвинувшисьзаогонькомвсехпостороннихпытающихсяпрой
тичерезслужебныйвходсообщилголостакиоставивменявнедоумениитолияговорилсвозомнившимосебеинко
мтолиссадюгойохранником

# Код:

```
import string

import math


alphabet = open("Alphabet2.txt",encoding='utf-8')

alphabetData = alphabet.read()

textGeneral = open("Texy5.txt", encoding='utf-8')

textGeneralData = textGeneral.read()

textDataWithoutSpaces = textGeneralData.replace(' ','')

textGeneral1 = open("Text4.txt", encoding='utf-8')

textGeneralData1 = textGeneral1.read()

textDataWithoutSpaces1 = textGeneralData1.replace(' ','')


text = 'приветмирприветмирприветмирприветмирприветмир'


keys = ['по','рог','дома','моего','кабардинец','холостойход','грехопадение','узниказкабана',

    'слепойпровидец','неистоваягарпия','огоньнапоражение','понтийпилатииешуа',

    'невыносимостьбытия','бросатьслованаветер','внеземнаяцивилизация']
```

```
def Encrypt(alpha, key, text):
    a = ''
    i = 0
    for item in text:
        world = (alpha.index(item) + alpha.index(key[i % len(key)])) % len(alpha)
        a += alpha[world]
        i += 1
    return a


def Decrypt(alpha, key, text):
    a = ''
    i = 0
    for item in text:
        world = (alpha.index(item) - alpha.index(key[i % len(key)]) + len(alpha)) % len(alpha)
        a += alpha[world]
        i += 1
    return a


def Index(alpha, text):
    indexS = 0
    count = 0
    for i in range(len(alpha)):
        for elem in text:
            if elem == alpha[i]:
                count += 1
        indexS += count * (count-1)
        count = 0
    print(indexS/(len(text)*(len(text)-1)))


def IndexEncr(alpha, text):
    count = 0
    indexS = 0
    indexE = 0
    for r in range(2,31):
```

```
        indexE = 0
        for j in range(r):
            indexS = 0
            for i in range(len(alpha)):
                counter = 0
                count = 0
                n = 0
                while 1:
                    if text[n] == alpha[i]:
                        count += 1
                    n += r
                    counter += 1
                    if n >= len(text):
                        break
                indexS += count * (count-1)
                n += 1
            indexE += indexS/((counter)*(counter - 1))
        print(indexE/r)

def monogramDictCreate(alpha):
    return {item: 0 for item in alpha}

def monogramCount(text, alpha, key):
    monogramDict = monogramDictCreate(alpha)
    print(monogramDict)
    for i in range(key):
        for j in range(len(alpha)):
            count = 0
            elem = alpha[j]
            n = i
            while 1:
                if text[n] == alpha[j]:
                    count += 1
                n+=key
```

```
            if n >= len(text):
                break
        monogramDict[elem]=count
    print(monogramDict)


def indexforkeys():
    Index(alphabetData, textDataWithoutSpaces)
    for key in keys:
        print(key)
        a = Encrypt(alphabetData, key, textDataWithoutSpaces)
        Index(alphabetData, a)
        print('----------')


def mainfunc():
    Index(alphabetData, textDataWithoutSpaces1)
    IndexEncr(alphabetData, textDataWithoutSpaces1)
    print('Enter key len')
    keyLen = int(input())
    monogramCount(textDataWithoutSpaces, alphabetData, keyLen)


def DecryptPlainText():
    key = input()
    print(Decrypt(alphabetData, key, textDataWithoutSpaces1))
```

**Висновки:** Засвоїли методи частотного криптоаналізу. Здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.