КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

ФБ-12 Приходько Юрій

Мета роботи:

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

Порядок виконання роботи:

- Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.
- 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.
- Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
- Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи:

Напишемо програму мовою python що задовольнить поставлену задачу.

Програма має:

- Прочитати з файлів заданий варіантом шифротекст та відкритий текст тієї ж мови.
- Створити ключі шифрування необхідної довжини та зашифрувати ними відкритий текст.
- Обрахувати індекс відповідності для всіх цих шифротекстів.
- Встановити довжину ключа за допомогою одного з описаних методів криптоаналізу.
- Встановити значення ключа і розшифрувати заданий шифротекст.

Додатково було розроблено можливість запам’ятовування програмую ключа для певного шифротексту.

Результат виконання програми:

```
[*] Length of file is 1075 kb, while required length is 3 kb
[?] Redacted to required length, show text? [y/N]
[*] Generating keys of length: 2, 3, 4, 5, 10, 11, 12, 13, 14,
[?] Show keys? [Y/n]
['жэ', 'лий', 'ъхфу', 'нъэнъ', 'эфчзсцвуйъ', 'яйбаккяфтйп', 'ы
', 'ыньаранютзвпкрвлгмы', 'гюйлкчызсюьидхмфнсря']
[*] Encrypting plaintext for each key...
[!] Coincidence index for plaintext is 0.056318772924308105
[!] For ciphertexts with length of key N:
2  | 0.04428587306880071
3  | 0.04308702900966989
4  | 0.03947493608980771
5  | 0.0400971434922752
10 | 0.03261731688340558
11 | 0.03354473713460042
12 | 0.03438012670890297
13 | 0.03280048905190619
14 | 0.03280626875625208
15 | 0.0333677892630877
16 | 0.03295387351339335
17 | 0.0322974324774925
18 | 0.033991108147160165
19 | 0.032806046459931085
20 | 0.03213471157052351
[*] For task ciphertext: 0.033177901938147646
```

Таким чином

Тип тексту	Індекс відповідності
Відкритий текст	0.056318772924308105
Шифротекст з довжиною ключа 2	0.04428587306880071
Шифротекст з довжиною ключа 3	0.04308702900966989
Шифротекст з довжиною ключа 4	0.03947493608980771
Шифротекст з довжиною ключа 5	0.0400971434922752
Шифротекст з довжиною ключа 10	0.03261731688340558
Шифротекст з довжиною ключа 11	0.03354473713460042
Шифротекст з довжиною ключа 12	0.03438012670890297
Шифротекст з довжиною ключа 13	0.03280048905190619
Шифротекст з довжиною ключа 14	0.03280626875625208
Шифротекст з довжиною ключа 15	0.0333677892630877
Шифротекст з довжиною ключа 16	0.03295387351339335
Шифротекст з довжиною ключа 17	0.0322974324774925
Шифротекст з довжиною ключа 18	0.033991108147160165
Шифротекст з довжиною ключа 19	0.032806046459931085
Шифротекст з довжиною ключа 20	0.03213471157052351

Для зв’ясування довжини ключа мною було обрано два методи - За допомогою значення Індексу відповідності та метод Касіскі.

Розбивши шифротекст на групи за довжиною ключа і обрахувавши Індекс відповідності для кожного з таких розбиттів до довжини ключа 30, отримали наступні значення:

```
[*] Splitting for key range 1-30
1 | 0.033177901938147646
2 | 0.03313961205402715
3 | 0.03313992706028042
4 | 0.03312177276164991
5 | 0.03329805078590249
6 | 0.03307657772004469
7 | 0.03323713205281472
8 | 0.033031245916742495
9 | 0.03298272502165414
10 | 0.03324433173834701
11 | 0.032745301417843646
12 | 0.03304973739800162
13 | 0.0332768349788457
14 | 0.03335365275559438
15 | 0.0334393110517404 24
16 | 0.03298851067530127
17 | 0.05431562231670444
18 | 0.032905838181751676
19 | 0.03313958022944087
20 | 0.03302088022336573
21 | 0.033118325914910485
22 | 0.032921417885063274
23 | 0.03303937184743563
24 | 0.0330625859510059
25 | 0.03301897423809684
26 | 0.03336613867390706
27 | 0.03280406048618231
28 | 0.03365254185857313
29 | 0.0333285616828271 76
30 | 0.03330443044102267
[!] Key length by result of 'Index of coincidence' analysis: 17
```

Як видно значення на довжині 17 набагато ближче до теоретичного значення I для данної мови, алгоритм робить висновок що довжина ключа 17. Перевіримо це закріпивши алгоритмом Касіскі.

```
{1547: ['зулщкяб'], 4403: ['щщуутнб'], 1666: ['ънмхюду'], 4318: ['ьихывск', 'ихывску', 'хывску
х', 'ывскухн', 'вскухнф', 'скухнфщ'], 1411: ['фьуыъыч', 'ьуыъычу', 'уыъычун'], 17: ['юпшъайл',
 'пшъайлъ', 'шъайлъе', 'ъайлъеш'], 68: ['онднпрщ', 'лдэуфиш', 'дэуфиша'], 527: ['вхыйшнл'], 10
37: ['уефршчу'], 391: ['ууснэам'], 714: ['гфцмэиэ', 'фцмэиэл', 'цмэиэлф', 'мэиэлфя'], 238: ['к
хнмыив'], 952: ['льхдаоп']}
[!] Kasisky examination result, key length: 17
```

НСД повторюваних груп теж 17, отже довжина ключа знайдена правильно.

Провівши частотний аналіз для кожної з 17 груп як для шифру Цезаря, ми можемо встановити тимчасове значення ключа. В моєму випадку методами частотного аналізу не вдалось однозначно і з першого разу встановити значення ключа, доводиться редагувати. Програма дозволяє змінити літеру за індексом на бажану або на наступну найбільш ймовірну за результатом аналізу шифра Цезаря для цієї групи літер. Так як і ключ і відкритий текст мають зміст не важко здогадатись які саме літери варто замінити для повного розшифрування.

Таким чином:

```
[!] The most likely key is рошинабеяразпичря
Decrypted plaintext example:
экэкаватцрпрдзедистзйидлихныйнлоънотспловопсдазекжвынссенноссусоавпатохтягойрчудквиснымуубатыф
ковфом
[?] Do you want to change any letters of the key? [y/N] y
[*] Write only positional index of number to change using results of analysis, 'number letter'
 to change manually or leave blank to exit
> 2 д
родинабеяразпичря экскаватцрпрдзедистыйидлихныйнлоънотепловопсдазекжвынесенноссусоавпатойтягой
рчудквиснымзубатыфковфом
> 8 з
родинабезразпичря экскаваторпрдзедистыйидлинныйнлоънотепловозсдазекжвынесеннойсусоавпатойтягой
ичудквиснымзубатымковфом
> 12 л
родинабезразличря экскаваторпризедистыйидлинныйслоънотепловозсдалекжвынесеннойсуставпатойтягой
ичудовиснымзубатымковшом
> 15 и
родинабезразличия экскаваторприземистыйидлинныйсловнотепловозсдалековынесеннойсуставчатойтягой
ичудовищнымзубатымковшом
>
[!] Decrypted text with key родинабезразличия:
экскаваторприземистыйидлинныйсловнотепловозсдалековынесеннойсуставчатойтягойичудовищнымзубатым
ковшомгусеницыглубоковминалисьвпочвуоставляядвенепрерывныеребристыедорожкиразящеесоляройлязгаю
щееоноперлонеразбираядорогииготовобылосокрушитьвсенасвоемпутионочудищегенералприроскместуневси
```

Ключ отриманий за допомогою результатів частотного аналізу “рошинабеяразпичря”

Відредагований, остаточний варіант ключа “родинабезразличия”.

Довелось замінити 4 літери.

Шифротекст мого варіанту:

Ншхтнвбчхапчупьфзбаясхдмнфэырьуекмюайчшогуобдзцнбцблыйщтноурбушэищяявьнъмгпопз
улщкябмлъльыоауауъойгцглтбусргыдръсосщкгрмрщмщйвруютухьъчккпниктнжфчхрвнхтнпхпфр
ютьклюрхстяшячнэнтспржаорцзюляозйнынпфмалхшнзижсцфимдпххуипоцйцбюпяуысппчгшпэ
дщшдэоххыенфъвихшцоыгшэйлтнжхзыпчушещйьухъанжзшшлзачеадтупряьтдмблпиъетнэафц
шьоарбючъшяпсюрйщтмйххзчмшдщгрюштлыовшлгщмчкьмыьоонщнжтппацщъефрвюдэхзбсм
иащруущстьсныжййзэнхьэвгмгщмцютбрхбьщщуутнбэттыйтчйшепоукйнъогыпескфэошэдзижгъ
жнсьнесрпъьъумяцумхнчйтзощмоцщшдаожхыгйжюхиижщйшдхаччихйтшвифхъекгшштсщащнф
лпхмнырсмпйщвиуххбтфюжгцшмътоъойжмчочюоязнфытсшищбшшлхффтщкшухухзоемиьслтън
мхюдуфнбрцюкзэцвдйюрцнырйнфювмпдщъньцхцютпнщбмвьубцмвютуйньъцюлмнгмпяфосрц

врхптяохнйннауцрдетппезфлхясйаудуйнпохссщлхекйхьихывскухнфщфьуыъыычуншбргэажукыим
эйнфымжтщьатщыгнрвыдзщытрпикзнцйпязурыютсупыипьчтъяэцйкьутчхьифрхчщдыусхымреч
ъещлтесьъяоипауучэакщшемръцщышичеьбтхцдбцалрхнроручгшпцпчмдбнцдшеутмютчщщвца
лццичинкмвсжхизддаыясруткфшчфжсфтръожияоссхфетуфемдыцдятруккюзфлнйтяъьнфыджрп
ьнхоцйцмэогумздеейажошефяфцсиьогцмщвппргцрвцтщъаъкфрбхыъекъьштфььячмаоуькеплю
фсцютэгъфатрхдцвютттщяурепфишэидюзюысцроффчрвтрхязоюрхнцвййпьошэрщгчыомпьоепхэт
чщуцртбэйуннбчйюрпэдврфшгиншвптдыьынниднъюткнвмкфэырнивздвягтютбчпярмэъецмрэф
зщооедыьылхчмнюажутчэимэечлужшдъюдщъоитзыстлйенлхяццяалньъеьлхяплюрсньогучютту
кещсмэтуфаячщркюэцонкюрйтъатзхшхлнцяэнсстхxтрудвоуюцдщнардуюятсмбтзшишнвгэтмввб
чпысщыищгчььцххкйфъыьщьръимгщынэеитмъсщлъячнфрйшъугэпщсжхыиъзюпйонлюпшъайлъ
ешрыужияоуцчрзътигнгыцпщмигйчггцыцщцпэьжгьрпцщрлцщукщнуычъийеушхлмхцщареючщя
онфмаетщфяунбкрцшоеумфечркннрыьжхысрнюъакрхьшяыбхчтлгуйаеукышшявкхзъавкоюпзьх
енпряхъыяонмзулщкябдаолкырбьптатщщулнвьжцтрйтъвьшкхччппечбтгпцжтпхпуьщйхрймймб
ьхэкзонднпрщснатсещшльциыхнъюткхяоецаощукехтцуушысшнщрлсюмчфдвыйъюяткрзашнцех
сгтдпнодххьнвфщйцкхасрцддфжйэешхцвдйюьеэпаууйгнмоцжцгшадтхелучэиюэцяейбшдкнтпхъб
ххпыднртьфцяиубншзфзцдиббузмнсйргэемснвнжрцрцяосуйшвлыыъывхыйшнлбфхпвпцщцхдцт
дхъыкцхозфутгнкмшсышатхмфийръщнишяцкылпзсюрпвхькнчупнъаапъатхвтчрмхриишелкцюкз
тивщюхзйцсиовтмфхпнйцмсйпъычоущркнртчтзэуиипнйоцрцпрхйлдэуфишаоуйюттуяяннвэйшп
одуцаеижкчубяьпхымийчрвпурицфаосхысунптдчюлклдэуфишаружтитьзднефосхийтуечнпхфьу
ыъычунссклшвмэкьсзбажцшогпхаиюшнщцжхщйхнялшчвоюхияхдттдуткжфхъаолуиздйутмхнюр
гдолръехалщццднпчзъжмхибрмхтдкъикфзжимшъънмхюдуннпзхвлпврьцсяуфкыгпфчхбвнивко
ющсцщзехзтипущеэпрысцютйфъыьщюъьйюъюмтъумуфуефршчутууснэамсхычзъцбижрщйфачж
хфлйфляяхдэыясклжпщаофутесаацоняалрезтмънздвхыйшнлтчхыьнрктшячццншьоуцюхтщччурх
пгчыкбхурнъхызъйшлпдбсмуйэоцщмюнлымушывбрпысжыииъбююмуюяоеыюнмцриъблоуцяо
нзхчнпхыэнрюрхнщрайхьвцлшьаяуьжкислутмзфюуяпжряцкылбчхуошлфелнфбеикктпзтащщшъ
шньйщишгфцмэиэлфярмрачоъомдоуатхцщаньэфцоисежбьшхкепыяофтсескймянлуеймюафнжа
мнпыоулуящыаькмнлбцгэойлзжшнбуоиклэщщаеищкчъдыксцьрпчжэутыыбызууснэамтмъотрйв
зрмьцмнлжсъяутзъиткоетфщеерпвьдцдлхдбьерэамцжвущснщщсррмучляьйхдйлчзрлхасылщж
ргэащщшнногщаънрбмлрлшкхьлпюъорцщжрююкмцниуъиыясъахуфхпчщрюкнфцрцроюпшъай
лъешньжчфнпбргжыдцдлижрэтшвамнфрдсцищрявбфццпфргвийъшцфыюейхйппъхфитшидцтвп
чтютпотшшгыиюхзжуняяоюпчрнъшнъцалщхцпсжссаоьщъдгишюдщьомекрлшкхьхяюаорснпоса
ыяхнччппътшмдпсшълзнрпилшшфгекйцхссщнндхншыййилпзхтсмщъщудъцйлывмешвнхьтефяэ
тткнлюргдиирпюктзыттннфрйъушэгоънвьчхтгпзпфиущхьуяфцпцюьдкфхрзцчещкгжсцьоухъбитъ
цпрпюштсэаисзиишэцамтуубтюкбззвочшибийюуццпржсжярпэрмцсбщйохвбдмуоцршьфдйуср
марущюмшэивлпгхсцэаизхааюукчъыбнуцсгфцмэиэлфяпяещвчнлпуфтъмаивкнсжмшъуяущюрхв
ндхтоъщцщлфлъуефршчуоющапаятбуюммшъефчьйзхалнуфбтчюпчтнаъчхнрбмйюрхэыйцвюбн
мттеуйюлгшцгхнуьжштмжтпбрзнхяъдыксцоытччюгмшнзикюахъапйрсюбяушдциюрдуйнпоцюл
жшнжццхъчъыеншиллхсивтнуцехащйкцюдкющьхзжоррхкпзяюмлршькыпроцъцжпхэцхнччшйш
адтнязкюрсщзлешнфооичилззатзцгчкдфкричовдорньыидрсмстшыдгкшмцмцрбцлрэтумнффъбт
гюъхозвэтмамбрхэтчлкчхдфуфнпожюмтэщщфъцггьцшнсукщэеъьчьулюыхъэвьфхызщутжцкпыо
нчалущъуллъещаюшччыкбмзысжпищнчэцнешьхсмыкхфкяэкпмэнцрьцэюйхшчзраыцлршсапкхн
мыивыоыьщцсемушюоидрвекмвтхфаврхъичщкчуббужэыдоамяочэгдигющйпяьгпзсифюльхдао
пксуньптоячгъхтыытщымйтпзекщхьщйрхдусайьщюофчцъщйрхдъйауашюбшэкьхмюшццьойтщх
рмьцщикбнбуйфгклммзхяйцкшыдяхнбгашйъэцохзысйхтрбршърхчхетяъьнкихпйцхрйжсднрвопк
эаубкхнмыивекмвхиэкбцщшчмьтяэзецохалгкохтнрфднбяютятмшккюэщщзяхязуушхшмушмбвн
цырмюеоычсуещшчщщщзимррйхырпсдвощнцачпшнцншьоейбясусиутзонщьрбзпысжонднпрщ
оцяосаряутзъжцсхюгусабчвэейумьукхфмъэяеуубатцньсаххцфнбтппуфрлекдбкецчрбмхфрзшзь
лнрлфцфомкубпчжщдыктоьрщэмбыэаьчызркбниипетеурэйжшкляыягешьхуфьонръднблтйшуау

бщторъшязсхщаыщисетъокпицхяэузцъаупфглшкывгаэуцщмсфйгсайжоякдвячмйббхмфкхюутйя
хахзклэщзьвмпдгнмлжлиьонтпнтхонднпрщхфылшетыалшциутионфтнатъцнхтиыыпшааеяоксзе
ифрнъцоюсдхиеоейшгзбрехмлуфнгерчхаыпъцжирвкжтнбйтъвыушнжцлюфйайрбмъцвйкпчурпр
бъыджрхсоеьдйилтшдйхнжулэоръизгпгшеысеузыоцщмьшдткгфшаиещмуурнпдтьувчышмнды
ьытийтмгщенюппрмчнвфчетяябпдязбфхпсяэидцбштйуывйчхчаяллчуйгфйкибсейиеующцхяяьпз
ъуюпшъайлъештюажуткбоцюкзшижцлэцпцъппжмуарюхьлняуфнсмпхлюйщщуутнбътъэирулъой
гхьывютмырувшчънъцльхдаоптнкнунэоирпзижыцыхтевккртгънзнгььфмыйюпшъайлъешяюшдп
нлпцгэашэцвдйюфйыяоннщхлгшггпяэнцртмтпхыьпшншнжюэдщъынфмавхроьпясузиъижклтаф
рпчтнэемуысэччргпвнитзььсщярскоъойжчззлшщуцшутукэущжсбцбиьихывскухнфщчемятжмщй
вркчхдптиынкящйяыгжтмаатлъеъйгпдштмрутхтмцкйшятбхцпесэмэнхщачшяиусхийжюмтпзпнд
рзбьтйэаинйзтхъшямдвягфылонмэошшцщщйршмкнтэтмтзпыицхясьпдхувнчртгьзгнсаьжхндгел
жащзкиънаьсыюопжчрзпццдчпррмуйнпцлтуььнбымфытсфаекчцкхфкгнрвьзмтоофчшзмчуяурпр
ундауетбясщкпчнеькрцнбипуафэщбрицупнфньосглзх

Текст розшифрований за допомогою ключа “родинабезразличия”:

Экскаваторприземистыйидлинныйсловнотепловозсдалековынесеннойсуставчатойтягойичудов
ищнымзубатымковшомгусеницыглубоковминалисьвпочвуоставляядвенепрерывныеребристые
дорожкиразящеесоляройлязгающееоноперлонеразбираядорогииготовобылосокрушитьвсенас
воемпутионочудищегенералприроскместуневсилахпошевелитьсяеслиэтоконтрольныйсюрприз
товесемирочченьвысокогообудущемведьмакемненияапотомстрахизамешательствонеожидан
носхлынулиосталосьтолькоспокойствиеиглубокаяуверенностьразумведьмакапустьдажеиначин
ающеговсеравногибчеибыстреетупыхинстинктовдикоймашиныпобедитьбесхитростнуюмощьм
ожноибезоружияоднойлишьсилоймыслиеслизнаешькакгенеразналпокатольковтеорииновед
ьвтомисостоитсмыслконтрольныхполевыхзаданийвпривязкетеоретическихзнанийкреальнойоб
становкеодновременномелькнулашальнаяивданныймоментмалоуместнаямыслишкавотзачем
устроилииспытаниевпустоминенаселенномпаркетакойэкскаваторнагородскихулицахстолькоб
ывсегопорушилзадесятьлетнеотрослобыитакимеетсякарьерныйгусеничныйэкскаватормодели
моделиачертегознаеткакоймоделимноготоннаялязгающаягромадинаповсейвидимостиоснаще
набортовымкомпьютеромсвозможностьюудаленногодоступаидистанционногоуправленияповс
ейвидимостивышлаизподконтроляиуспеланатворитьлихихделвонэльфвесьокровавленныйвал
яетсякстатипреттоонапрямонаэльфанадоотвлечьгенералпрекраснозналслабоеместотакихмеха
низмовнеповоротливостьползаюттакчточеловекнасвоихдвоихобгонитпоэтомуонсорвалсясмест
анабегуподхватилстравышмотникипультсиганулчерезнекстатиподвернувшийсякустиобежалэкс
каваторслеватотсразузамедлилсяивдругпроворновыпросталполусогнутыйдоселековшсхрустом
переломилосьмолодоедеревцесловноспичкагенералуспелвовремяубратьсянабезопасноерасст
ояниечудовищеразворачивалосьготовоеринутьсянапрячущегосявподлескеведьмачонкагенера
лнеутратилхладнокровиянапротивонужепросчиталкудаметнетсясейчасвоонтудазаогромныйст
олетнийдубвнесколькообхватовунегоподитакиекорничтоиэкскаваторусходунесворотитьжизнь
онавсегдасильнеежелезаимоторовивдругугенералапоявилсянежданныйсоюзникмелькнуласре
диветвейистволовкоричневозеленаякурточкаиневдалекепоказалсяещеодинэльфодетонбылто
чнотакжекакинедавнийпациентгенералановотличиеотпервогопребывалвполномздравииисохр
анностиивдругугенералапоявилсянежданныйсоюзникмелькнуласредиветвейистволовкоричне
возеленаякурточкаиневдалекепоказалсяещеодинэльфодетонбылточнотакжекакинедавнийпац
иентгенералановотличиеотпервогопребывалвполномздравииисохранностипультутебякрикнул
онгенералугенералмолчапоказалемучерныйначиненныйэлектроникойбрикетаключтеперьгене
ралстольжевыразительнопохлопалсебяпокарманукурткиэльфсловноподземлюпровалилсяраст

ворилсянафонелиствыапотомвозникужесовсемрядомвпарешаговвыскользнулиззастволатогос
амогодубаэкскаваторгромыхалгусеницамиинатужнолязгалковшомпробираясьсквозьпаркдере
вьяжалобнотрещалииломалисьрождаласьноваяпросекаэльфтребовательнопротянулрукуигене
ралнеколеблясьотдалемупультсключоммедлитьэльфнесобиралсятутжевставилключведваприм
етнующельнаторцепультараздалсянегромкийщелчокелеслышныйнафонепроизводимогоэкска
ваторомшумапальцыэльфазапорхалинадклавиатуройпультивпрямьоченьпоходилнаноутбуксто
йлишьразницейчтоэкранунегобылсовсемкрохотныйирасполагалсяненаоткиднойкрышкеапрям
орядомсклавишамикрышкисобственноинебылововсеотвлекиеговластноскомандовалэльфибез
звучноканулвкустычтотоунеговидимонеладилосьгенералпослушнопотрусилпоширокойразмаш
истойдугеэкскаваторнакакоетовремяпритихотслеживаяегоперемещенияапотомсталгрузноразв
орачиватьсяподгусеницамизахлюпалоонвъехалвобширнуюоторочennуюмхомлужугенералпол
ьзуясьмоментомшмыгнулмонструзакормунаразворотутогоуйдетдовольномноговременисравн
ительнобыстрогенералотступилкобширнойовальнойполянепочемутоемубыложалкогибнущиеп
одгусеницамииковшомдеревьявконцеконцовпаркитакаяжечастьгородакакиквартalыаведьмак
обязанхранитьгородвесьцеликомаполянупустьутюжитподумалонтраванедеревоещевэтомгоду
отрастетнеуспелмонстрвыползтикполянкекакоткудатосбокупоказалсядавешнийэльфмелкойви
хляющейрысцойонприблизилсякгенералуплоходелосообщилэльфонзаблокировалвсевходные
портынадолезтьвкабинугенералвдумчивошмыгнулносоминичегонесказалдаичтоонмогсказать
атысобственноктопоинтересовалсяэльфведьмакчтолиначинающийуточнилгенералскромнокак
ойвыходпервыйнесталвратьгенералэльфсаркастическихихикнулвезетжемневпрочемчегоэтояи
начепришлосьбыводиночкукстатичтосранавеноромэтотвойприятельнавсякийслучайсправилсяг
енералкоторыйпультпотерялдаатыневиделлежитрядомсаллеейбезсознанияунеговесьбокразо
драняегоаэрозолемспрыснулвашимэльфнахмурилсядавесамаэвыругалсяэльфонможетневыде
ржатьтвойприятельумиралкогдаянанегонаткнулсяулыбнетсясудьбавыживетсудьбаредкоулыба
етсяэльфамведьменышзапомниэтогенералсмолчалладнослушайменянужнозадуритьэтоймахи
неегопоганыенавигационныерецепторыипопастьвкабинутымнепоможешьразужввязалсявэтод
елобоюсьтамвкабинеоднойпарырукбудетмалоподеревьямлазатьумеешьумеюпошлиэльфзаткн
улбесполезныйпокапультзапоясштановиделовитозашагалкужевыбравшемусянаполянуэкскава
торуотвлекайпоканапомнилонпобегайунегопередмордойтолькосмотриподковшнеугодиугубур
кнулгенералкакможнобезразличнеебегатьпередмордойэкскаваторaоказалосьнастолькожеуто
мительнымзанятиемскольинебезопаснымпервоежезабеганиеедванезакончилосьтрагическим
онстррезковыпрямилполусогнутыйковшодновременноподавшисьвпередизаделплечогенерала
тоткубаремполетелвтравусовершенноошарашенныйещевпадениисообразивчтопридетсямолн
иеносновскакиватьневзираянабольиубиратьсяметровнадвадцатьвсторонусообразилонправил
ьносдвухсекуднойзадержкойвместогдеонприземлилсявпечаталсяковшпохожийнагигантский
железныйкулак

Відкритий текст - уривок з збірки “Ведьмак из Большого Киева”

Висновки:

При виконанні комп’ютерного практикуму я отримав навички аналізу поліалфавітних підстановок, зокрема шифру Віженера. Я навчився методам визначення довжини ключа шифрування, та шляхам розшифрування тексту методами частотного аналізу. При роботі з наданим шифротекстом я застосував отримані дані для розшифрування.