Бочок О.С., Павелко В.С. *ФБ-03*

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

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

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).

Хід роботи

1. Підібрали свій відкритий текст:

```
Відкритий текст:
откройротсказалаонауменяестьсюрпризияоткрылаионазалезлавнегоонанакончикемоегоязыкаонасидитнамоихбедрахиябыужаснохотеланайтиеехотьзатысячумильсквозьмоипальцыонауходитазатеммеждуни
мизадерживаетсяеслионасобираетсяуйтичтожяпойдуснейязнаючтонезабудуееонабыласладкойкакмедновортууменялишьпривкускровииигоречьпрощаниятечеткакмедмневгорлоиналицоитеперьонанетерпе
ливаяясамодовольнаилишьнемноготрачувремявпустуюищумедноонажалитбезсочувствияонаслаяионамоямыпростобессмысленногуляемитеперьонатанцуетнастолеитакшустровращаетсяонасведетнасвмоги
луподнимаеттакойшумноянаслаждаюськаждойсекунднойэтофакингвеликолепночтотохорошеенелегкополучитьязнаючтонепожалеюонейонабыласладкойкакмедновортууменялишьпривкускровииигоречьпроща
ниятечеткакмедмневгорлоиналицоионанетерпеливаяясамодовольнаилишьнемноготрачувремявпустуюищумедноонажалитбезсочувствияонаслаяионамоясквозьмоипальцыонауходитазатеммеждунимизадерж
иваетсяеслионасобираетсяуйтичтожяпойдуснейязнаючтонезабудуееонабыласладкойкакмедновортууменялишьпривкускровииигоречьпрощаниятечеткакмедмневгорлоиналицоионанетерпеливаяясамодовол
ьнаилишьнемноготрачувремявпустуюищумедноонажалитбезсочувствияонаслаяионамоя
```

Ключ довжиною r = 2:

```
Ключ: яе
Текст:
 нчйхнопусцйежекентяшлкмддцсбргпфпнжнюусппакезумежекккжрязмквунтятяпнтцнйклудинджайентяцзйзчмелузъакгхяъздаатляцмуфусккемеичзкдънчымячъцюьтсзрыцйзнмысннноекбхантяшфугнсежесклсдлгш
мнлнжегкплззяксцюкррзумеруанпедчрдтоснцчнлюфногшртдоюммеэьсумкжеашгшдкнтяжъряцкегпноййесдймубупчтшлкмдкнчбохззйшрппубнзинхдыфпушемнючдьдчйейсдйлтдзвупрннмекнхузчдфдхыумемкскпф
дрззяеюцясннйзнрытянкнчбмклтнинчпецшбхдсюзошртгзютсдймунтялярзчакжцньтзрчбнюумежрядзумелуюсъфпурчнждцрсъцккмтнитрюклнскокпбнтячятхшдчмерчнрднсейэтцсхнзпешедчрдntяцбкгкстяцбсни
эртфнймледчсейуиэтсмуютяцкеейягрбйеейноркйшмймуивсууейнмибккнйуккотньсусуфупучкдтдрдийуоукщцнсбюммеэьсумкоуееккэумкиумеаакерряййуипяплкгтнзнхсштсдтюрззыфпнбптцйхнззнвупкцбохню
ятздскцкспяплкгсмкбинхкузтярзыннntятдчдхоккнбеядрелугубукбмезрззытдсмувусхяьтзпклдбфтцсшэншшлкгтнумееекнсждмруцшбцсззднтямкеюннтясндрпбужблузфярыыъуметъйзчямячдслкейттзсзмяйдх
енбедчрддцкннтяцнжзхяксцюшичзьсуедоуийтцмкиджтягцчнтдмяжтйткдумеаакерряййуипяплкгтнзнхсштсдтюрззыфпнбптцйхнззнвупкцбохнюятздскцкспяплкгсмкбинхкузтярзыннntятдчдхоккнбеядрелугубу
кбмезрззытдсмувусхяьтзпклдбфтцсшэнншлкгтнумееекнсждмруцшбцсззднтямкеюннтяснд
```

Ключ довжиною r = 3:

```
Ключ: кей
Текст:
 шчуъутъуыыпйсефкуцкшхптипцыжцзъфщтмсйуыфхдхесштйсефпмфкзцпичштйчеуштатпоцуонуисаукуцкцсонычехшнюлкнъеютдкешпкццшъчькфктйучспкюшчесеыецибшхтреыплшмецусщефжыдштйзъчоныкмйькхцкпошцтсссенпхптзйпчъйкъхнччеъшжсъеоьциэоытъышлищутошъчктймцкгаьуцпмйлшнэкоштйлафкцфкйушоукпхпйцшзчъчьэсочдфтэещхсмпыыпщшзстичъкажфщшюйчниькапчукпхпйхчклнущхусчефтычтчощкщжуцктоькщщ
кфтзйкдъксчоулшречесхнбжтоцтчныъеаэзщпсимфыычьинвзсоотчшгйрефтчкпмъшььмцымништйсрййнччехшдхефщшцыжоыцхецфптцшиьхдоцныпфоъбччеыктяэкычеъьуфпныкпбзцыъулъевккыыдччеъмкнпчцкцлцум
трьщунчнхккыьеушобзсцшдцкцфклнкгъжпйрйчуцофшцотчувышщйфнцнзохнушрощтчбччьуюшхчвкочкфпиущфчхшатчеймцкгаьуцпфчрефпгччктштйлафкцфкйушоукпхпйцшзчъчьэсочдфтэещхсмпыыпщшзстичъкажфщшю
йчниькапчукпхпйхчклнущхусчефтычтуцктоькщщкфтзйкдъксчоулшречесхнбжтоцтчныъеаэзщпсимфыычьинвзсоотчшгйрефтчкпмъшььмцымништйсрййнччехшдъфзчсбхшншкреаачеьяунтчйсеыпсхплнэтсцнркйоъ
лсмеоьципцфтуцкцчлнщкккыыдъучсбччрдшшонэццпоистйиыштосекэйьпкччекерйырйопчупйфсоотчмущьшьцкцйрсвбшънлфшъфхчмнснущпьещхчгецтдыпьоьпйфсоосцпзмшхфшнцкрсаусштйчкыпхшпрсмеййцйцуншзч
хбцкнфтэечкхчумшчщкььмхоцдлщшъьшзтюьцкнчуччепкрсьжосцчбшлычлтдччерхеитуцксчй
```

Ключ довжиною r = 4:

```
Ключ: мико
Текст:
 ъъфюъсъыющфоуихоъхкбшнчнсщькэжъэьрсцлцьшьгхофцчоуихуууукрщннъъхкымтшыгрфушцпсъзсйцишымщттфъчошцтгнноюмэтннгэфмщчьбцьучичохътусэшаипказщйеяфтщишфръпжъръщочдайъхкббцоцюисоюнцъсооб
щрццуиоуьотрмньялнышфцчоэцлцьипаэззчюрбаъойэъсобэхпчлпчокяььщнсоныобсншымйещмщхортшчцифьсмчьоцъаяыцущзхцддщюфкфбэтъьортсъшпеичъьеичцлъпесъфоцфптшхпрпцъщърчочраьфъпэсшжьщичуюнъэ
сутрмийямфштъкшщихкцчрвкщнцыълшаьиббошпълкщбзъэмфбзъсмчьъхкфмутаннсяъяэрзъмцлцчоуукнфцчошцйъзчъьэъшпсщыъзщхущхшсяуйушрьуынъкъхкамхабсъчоэъшщсрьоцаэяюшшрьигосъынъхкяоноююхкяофшс
фуэзъмчцшипаюифьхаэъщцйымщхотмкмэдфотмшчэнфбщмчьхеььаифщцлмучрфьчнщыъяьюцяьъцвусхпщслфыцхбгрьклпчокяьъщнщътихукцчухцчонгхозуктццушмтцурхшръшьбяфпылутжичъцотэяцшшрфрньънбкышшз
мхтнюнбуюткшшноъщнмсъшхьфхкщфюшцъхкысъпюынхцоикнэицьрцмьчдчофутжихпъщцньюшкеякъушзмэящьбкргбшноыъцчотихцюйпхэцббощьрфзшымпхолршымфшнэтмьудцьфчкщиюеьщиэгъмтампкасфцутмэыффтхммпю
трмосъынсщхцъхкяъйтюмньяыуафяььтзщьхмэящнунухкмгъшыспкпямэусцчонгхоэуктццушмтцурхшръшьбяфпылутжичъцотэяцшшрфрньънбкышшзмхтнюнбуюткшшноъщнмсъшхьфхкщфюшцъхкысъпюынхцоикнэицьрцмь
чдчофутжихпъщцньюшкеякъушзмэящьбкргбшноыъцчотихцюйпхэцббощьрфзшымпхолршымфшн
```

Ключ довжиною r = 5:

```
Ключ: холзи
Текст:
 гахчцюющщщяотзухьшзыбушжнжазшжеэыппэнщщтейцзргылоиауттичыркцгылфияьшюряучхншькогяощфижцппъвочхркпрлшхгужйрбсзщвьахъъщлфикуаумнкьэгпхажшзмбчпусяхйцькчхрдоцгюрьшзыкьппъххлщнбърнми
ыуурьопмшыцнзнзякмщацщфижьмпшхуэшзичэпязьсжчгчпъщвуфжпвойюъгыроицбпъньъшэйрщлшухтххсяоxунщыщйцеаюъфъыктрнкъчрчшюштеьнпршьымясэыхбхыужъъерщтхшчммбырйлгюцхрвоцпюгцэмчъюзххкырщнеэ
ртрчолжщхъщлцчьцгххццпасыруxгсщщшхеюйшъъкйчиязъжэзюунщыщххфлтрзпрощгеюйщзружцвоттифцщфибькугдющшъгпршщбйьтнвыщкыанрурзуъмшсьшзъхыбънзылшъгщрпъхшгъщзющйшхзлмъжнщфижррлнзылшкбьо
пуиэщлхэълмъзоххснбчфцфылшухфпзжжкхзощьфшнябшлхгчищщйохпхшрртряьцмчьвьвщцзьахшгжрмхъщрктгэщтымцэгзыылеязьшмчгфлтнуьшмсгылигаоьтищшщртхшчммвьнхшзбюунвнцпасэыпкябьсшгруплгюрюддюща
ивцкщнмуэсияърлфвункцещщпххщуэцэъшзхъарччъщуйихнъэфгтщйцакшзрацггхъъшхлгаызяирымффръъщзбйпбиърлхгъшзохщущйъхьхяирьщкэнщфиьщлжргылуцфяхйцькчхрдоцгюрьшзыкьппъххлщнбърнмиыуурьопмш
ыцнзнзякмщацщфижьмпшхуэшзичэпязьсжчгчпъщвуфжпвойюъгыроицбпъньъшэйрщлшухтххсяоxунщыщйцеаюъфъыктрнкъчрчшюштеьнпршьымясэыхбхыужъъерщтхшчммбырйлгюцхрвоцпюгцщфивуэмшдуцпкхокшибьпххкг
щзфиэщуядвучфцшьэчимбнчнбннцыжаюеробчммвьщфиыоцпъцутшцмбншъчцкхххxцзззъшзфгн
```

Ключ довжиною r = 13:

```
Ключ: геншининфаркт
Текст:
 сччиццшыжсъкщгрнжхныщщнппгхбюцшьшхыипшдднхигихцъфэрхчкрнъхтлывнрчтнуъпрчнцвеушскачшцъиюьдшьягсыазонсдаетсдааюиюхыйовпэгтнбъхнтйовжщгчийздыщьлмыьеуфффырьфлманстнлзымхжачкдисщзосы
ъьмшстзкэюрпитжсппгоныеиюцоьррпдфдабъхяявжпщамйайхтсмынрийхуъэпнйашухпареоууншшфдъшынечднсхыцоаьецстезшрерпатфншювшыкхьгюъчъбьицжиъьявпйиччштщнсанхмхсхшжръишьцютдифтидыхнбевпвт
кшакнимеаьшцсзыгдъихяиижяисъжлыъэфчгмвисмъчащязюшгепксецыхнъаытддкфйцдыпетттсстняунзхвнрцавсизшыщявбхыгпаюгнъхычуыйчпняэчтшйвнрьтрыаэъъиюжоыпъхечрыюъэввaклгкяйзыхневхочхтнйкщцр
ьлгщазтхдитъяфкюукцсъжзъиюяацотбцйвиумыэсхферйъжскъыиаътяжзтгрчщшцпэшйхуяжэышмехччокрвцьцшзчшьовмъшждъыбея шгртццънцвнрлноеюгистыэкрфюийъжкышяэуьпяврхрдьшхцкгыьуупаррцэщчмщвсю
нермътлевфтнстьфънпчоахалтнгргцхвнрччхкэзншрпфапытпусжкыуйбашхъыбъэфъцрвтакйцзээфмкьзсвэрлюаднсхывнрртонящнфщылутыденмжхнпшфяшшягсычщчкыыьъшътешфюицъфуешцлчняиянщаецоернщапнмтд
жшмтичючнюуxвнрыадnэшнящмэйвтйхуччыссзсэпывмъшждъыбечкуцйаэныхнхыыкгоесвццтнюмхоясэыиъаыщщнпхъыбьирптаекашфлнржштяйгрюгтрнмкндняюаъцчзсъэкрцэяошчтонгжрыхнбевпвткшакнимеаьшцсзы
гдъихяиижяисъжлыъэфчгмвисмъчащязюшгепксецыхнъаытддкфйцдыпетттсстняунзхвнрцав
```

Ключ довжиною r = 16:

```
Ключ: оченьдлинныйключ
Текст:
 ьйпэкныцяюейслйчьдеаийшзтюнеыйожюямхытзтэижйтщлчхчртгплкътючшшюдобуъумхнщыамшкетшчуъьхумхяийщщжмпьйэьщузоиопкьлегечтздшицягопамйкюеячхкяащгфжьищьюбщкмъишйсдшшюкгейходтиятзхпсвк
ыясхгдпнэуглкрриньцшдтшиюыьсъллгйяцшцомвъыъушфвкядкцылшилдниччречпкйа6йщхноцфкьйчтбуцждхфтсичмщойбкстйгцрейкщтникя6хыюмулыэаажъоезчтхыцрятяеёфчгыъдкпятыуыхийхуфецйкьбфзцъниоьрож
увнпьдкщнщйншнмвкдехзмгдътзцшомйючьаюфрфмпкъыэсхцршщбишцыъыпкцжйпьмюкыюкюяэсйщлчхвемдтшицыъхеъоеяйуобхьфиюжочшмъбвдтимэньтлешшюйодыа6цшиюяйфпурчшпшюофщкэнфйпэпцьдеююйпняъыъмчмъ
цвшькишрщнаыьлиечпшщйткхнюжйрпюхяупнвицсютеьчплечфчырдхрърэоxуиещьфъкыэцяырчъщцьудкшбзхцыжьбурунютнъыэцътккрлйьметтетшиоижйыцюышеочьочнсъйлшыркбгкъыпуайьлсмхсишзупдмоцзттещымр
однмойвнячыуцвгыьэркфццхъыфтбмяьдеъбцршътжсмлюцячсыатнцшйийтцжпкдкщйтоцяэыаэноъьцъзпхэылхфьцврвдьетнвдцряоарыщхкричпдгщхнфжййумдогумнонцфйзчтъювкнаыйдюэысгыктюйугствиюххщгркпгз
фязнбцьэтюжсшшюиьшнэьйэщмадытврефцфыеиющътдисшюхейуъблйасоопщлчптрннплмчыдукхкьтдупкфэыащацйцжпкжххюоющчэйлтубеюьыйлфщбнъгиьрхьабечийпфътэмшыйецдешдъщрыъыцпэгзэьрхюдлзюнзчощае
щутндпуайъахчщбеазедпжынцмэшзъркмяюаийпхыыийрлйяашкфнтвыпюнлткмдоюрнымщхнщйи
```

2.

```
Індекси відповідності:
[0.04474604230909823, 0.04296051213316962, 0.03938945178131239, 0.03636045527114127, 0.03483111665151387, 0.03315493653010407]
```

Ключ	r	I
яе	2	0,0447460423090982
кей	3	0,0429605121331696
мико	4	0,0393894517813123
холзи	5	0,0363604552711412
геншининфаркт	13	0,0348311166515138
оченьдлинныйключ	16	0,0331549365301040

З даної діаграми можна зробити висновок, що зі збільшенням довжини ключа r значення індексу відповідності зменшується.

3. Варіант 15

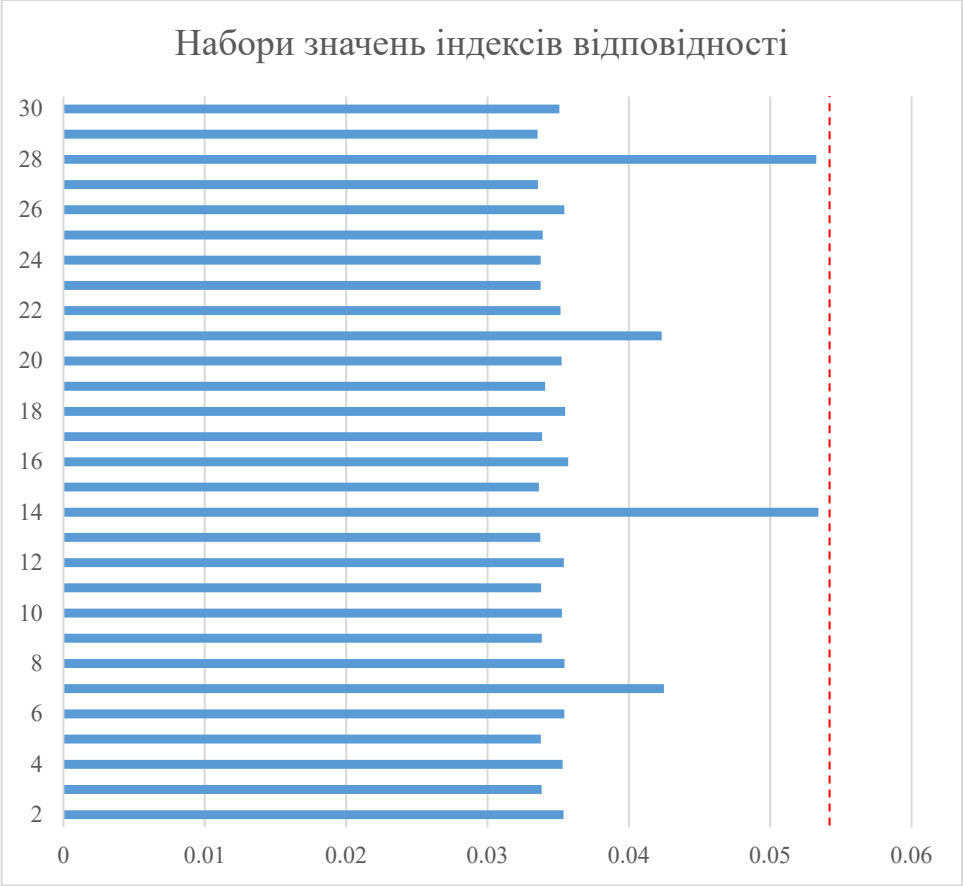
ьоттппсхстжххцэчхпзчйсрхрххцэраыкыьфнтжххъбьгпоктзнхгхклтоюсбтшгештхсчяувэдокеуюцюоыпчфхжказрмпрцеыцжни
хьврвдэиоъквчяйьгияйыбчуысхжыооывирреьцжпмшреоэтфцуэчштлхузсшмэкъжцгнсжямиячяшъбьштпышргытбчщэсздсшы
вптыюхояуытмэртызюцучастшптрбэдвбъоысснкшйдтьэкхвъяъяыаэрлуюлйъбъюскгрчтьмьояушпнхьедаирфчбьэьныбчоъйт
зоъцыхиэяфюрдвехчтясбтыэраоюошэтсяысывйьплзсюьгтцпыкюнщюьозкюноъноичыххоцщссннбувхфмуцфсдсяхкъеъдбклф
юфсдмьночтьемууяфдъооищдыахчцшънмсррыиршнэпютдьомифорпсдтбавтгтуюхънюцуэткжезртлгцынсуыагуодыеаеылярп
лшывсяяабхчгсхккотхнсукфпыцпдхцмаьфюжффъсоъхьгжтпртсфхсщнхцфьрфкъсчщщъяшпррыцтшбщбъъзбцлпэтьаъфщааярь
цфьюгвупфецэдстдиъчэкшъьжырфьноямвблпасртмйутэтшчеаабавтрфощкхшъбмфтгкрсуяаючьаанмгмцпыэйънлаухыпшскоя
оааыкрвянъъпыдчцкнпщнъзпызвтиюсдфратцшюхвпйынувматпццавлзашмууютлтюпамхрсчфтняяфцпоэттнысясссзькдстффыо
вжыаичцмаыхвхьншяюсйыхююцакфвяэыцпыпулзэнфэчбиажулкэттбзббгудтэхтймэутчыяддышкйчрютйаамээыьнопйжпчыб
уьпшезмчсхсьъбиедщьрнтзхфщоъццаэтзтыпхиссоюицчойнныхтцкчуыдмьжоцсюзчшыяпвшюрдюоюожщяатгтдкиххяуфлхяп
яхьгаьчвнапягйкитзйпрхцыфяюхлыооищьыецпыцонхкъивпюйеогаырмцтисдютотухнкпусощтагмпыхпзфяйавтфухсяяшнмшк
ннрюроьццхрчьдаъдоиуурщъдоюхгнгзеъбкюноъодишдббафюцфбпщккхнгцынсвъяфойощогфсбкгнлхьжециыдхэювчзяэнапд
энтюощрноыэхччянфчецрнэфмоддьныфщясытывзижррсакаэюцьукнкхсцфшсэямунлиирлоьуыыывнцоешошкупшщтсшызкэдб
нлкувьнхбмразыахуыщждцызкыцюхдфбчвньуниояыухэюхиохьфнхорсрпасчзпяхднешчеуошъяизкешвфнчбяяпдььдашмтушф
юуифщщртъмжпсдобядхулвахвгмфанщяырвралрчосогйрппздыфюлосйъсдьыхапттччяйжяяфцзвыцъущппьхйтцпууслыыэпваг
кезйьтыкнэрщяъцэрласюьцкъэыпйъслицмпчяэдюфшаюиъйъерчягииооМртуънтбуашъурмалцхпйыьбтгкфзптыъецфпяшывоб
ищйхчъооияныпижйьфчъбыэтнщэмпрюхорььяяпауишаэуыпшгымпрзлхоржоуошнсшщюднршзчсуыъдъойднжшчйъкхыбмэ
рлътзтддрясяяркдхрютосцххлшарлйоюьыэщцянцэныяашсчхыяхсшшвкотцбисььмаервеялрчиьбгщнъуфущдэанпасчзпефоътб
еъэпвябпыпортэкщпхфшюоцъьхпшфчубцябоюхготактауутпчйлвтцххшяцютрпаерыррйцкуьйгтыэвыцшйьыоъянхцжашаиксу
ащянхцсеэйбннфаньдъуиднцмййбьййшфжаяавунэщфымжшрмыкэуйауутпчьзлтцюпчяьгчнпызуюухкбльфшючбфьюгглоццэ
нбшаксхишччттсфзцблеюпшцхэфцеыцыргыйвшыьуяятцупимпойъщьфыньэргыилмйсцвткшыхаакяумэтспдыакмытвичаэяся
цьиныжхйерйьызоонедйгоычхсяптармтхпыйпъяумщжопдщийжоютгшптаяабдывъсъъооътыфьенпщнсъщутеумфеиъцьснрт
юбтхяхчарцямечкнаиэатсяпънбкпаьфюробыцьдъуутнжрдуябаъъпабжтплкупэьхйшщртхпшфчщюмеяцэтортэдфчядшзаюздчм
ефщчэяфгчцдшхщбдшяьжыетгсртжаевпщщпфхмсалэггмяншйсйыхщхйбдлуььйвшюрдюоюоъбуюинньтосятвывыядыьуонав
штоьовямэмутэдцтсщцюнакжпявхвещпацшычьмуядынълрашягцхкэятеиакяяошюэвыжяхчыьшркшсрвтцаеыпшяцбпазрыель
цэпмпяпасофиэктэяцъыирпомеакуэсхнреэнеяхпццфпсъдщьлмтьмьыэаяшзяьносслонэфхйсшщкмыоаатаыцряышрртйшччтба
вшуурнлгтчбьяюдчкааюйщьйаыссбшюзсятпрхпчжысжцпеыыхтебьгтохйлзсйбблауутпчйчныжуущэтвчзяштамщфеьхцютскш
рйдцюжъэяютвшъдоячцфчащсшцпюфпыэюйувохмгжшркалмсйэпцэмэръиюаътйюобъзфбдыэчуефануыпшапыцхвущэфэыкш
трйчфгифэщщгъуэвртсмзуэююяяйшрвтынъуфледуйпцрсяфюзоягящчхуоеофлммчтяугйямаяятефчяньнвщзмауадхэхсезмьтояур
хцнцгысьькдтпюсчязщшрйэзртихххмчрсмохущащмтччяьъюсъоинхоъшрлъспъыьчшхняупчщяцлэфккюфхйоькыыиильтосоюос
ущщъмеъквххыахчбвнлтьфвтфэшлзцвйнырзтэдсшщщыдшбшадеяывуыэыцэяспррдмтуосцххлшяргшдбкцрйьдсшэрдыеэшзюь
фыгфбфошаъуафюгхошяэлнйвфчсубвйшщючазшшувхнщъощкнъящпщпжцъмечщеэсшпчшэьнштхслыцэутуублвтрпеотыббэ
чашдьупоцерпфпфыттщьбснуыкъщоьнржъздыжгъйащспдчямицоютоеяьнякрзнтпхцфкжюыгшызсштббъюугэнмямоцерэцчя
ыэъььлптпхтчштяугйцподсюоылъялрховвтсвшыхуаыгярвтхпшцчауххрлоънхьхцычягтмчьлчяттцчбыцеяньдояогмеыйвъящот
нхоюсшъьгъзашкйюпрелфыяяйхцмнапбдуябфшнхцшыцсхцшчъэыкоьиднпбдуэсхнгшызсюгючлфаяяршяздтнбросовоявыкчя
тэеъпъящапюзгажюрюэрсыапюпупьшцеюьхщзныхлазюцычщтилптмощипйещьыажжъввххыуьайъчтскоаемаууэхцпмэщсеэй
ъхоаащшрйцутэгетьсятыпштэкнуынцфгяяющюртмсгркпшьнвээзйысгщщччхнсшщюкыхьуыяцгэзнщртчдэккэщцщдыаруъдб
жоаэячнуыреъйвуабьдкстгрнщдетъъюдчнурнептцыэюяътмьнхыжбпчшпсемтъзсяйзпччъхтиыадияйыбцэтяюскщрсйцюквфп
яцйшузсшмэкъщошнсжрплйьхжчъкйнюбуфыэйецыфыюнюлоънмсрпчбьбыичуулххышпрбыажжъвсысгщщчуэоъхосрыйчло
шрмвноцнаптауыпъщфяньтосхъшзаацътфпрлйьюонэюярдбарифжшзйъовйлпфнеюттййрьыысщьсрнжюсьрубтвэррлвттеъбьъ
юсшюрнирэумэшгылшссоудыулпанхфтатопдватщьвяпшъукынъшшфдщязяркнюошокэсящнхушвэгбксюющчясеккъттичяьх
юйшсраэщшкшчяыыокцооюоюзъщцъюкэфклинзкфэрцчошянессшъшэяьтошювжтсшдцэрфыпштшепчакучжцшнчцтаюуыунч
щяюымырвртаунфшдсяфоммътуубыйбмктахднхойййюьгыпнбщтыцюздьмжхбкщкныхбзчшяяпяхцддтпртчссяэноямитхюзобьу
нктцоешмэеыээбнбшэрдызюзчябыыпшяфыъхъухвэяянцбиестуулэюдпъщщвчхжррцэрфыпштооюотку эыгэзлбшильхцыьохгя
ькфыюгзцояутэнцтзнйзштоыоьидчбжеъауньььурнъьжцтжтунчщщюыльеднхвздющсяюьодояцюьыэбчюктжмощсръйъкюылш
ямопмвалчгхткщззшмьтчтцэъдщьпрнжгждъьжыпшжоестъшыфпрсюокмочччбхпшбмйчбдпыщтефчщяътююкйьтфнпфыынб
кюклнхтуижуюххкыххыфюэюъьтирьофьстгчщпаядяутрлртбччшшссюокмопиашмьовянъьиишхпуцввбхиббдрыихпйщшбхцт
амтыирпчыбгнлфюкчнцмччарцюзмжксйлрумяочсдчцзбньэнувбхнщянщбнапттсцувяыфартацрреьугмлтщрсямткяыьюнфтхрбх
цхрсуйэюйшчщеэцтеъыыюнфшрсоътзехььвхсчбксхишчоюубйтьювдыкшййшярыпкрклйсюйиукыыйэхюмнтэшэяцпчяфцмуфа
ькцфьитмжархыцхрчакяябшюбтйцплоъйцюйшщюзчмхуыуьчсюмьтоядгчщэъгыашсжаюцякщфягнмпажоуишюоаэсюзццною
цшзоефсшнлырзнээшъпрщшлшывххцрплфяньпшъркстэныщцжысжхвдтсмиьюбвязкаэмыпшцежоктньезхыщючцвщяътююкй
нцюъчуцгпяыхжеюаэуапъщнйтыхкнуюсчъещьяънсртфтефщбшйлкллояыхчдююячяфбадтсмиьауъдяыэрммсгршяьэырфьдсчч
оефчэбымшреоэтфцувмсчяфобттехрзрушъдуяфрнкэнучэцэднщбнапшцеьбияншадоэгхчосьбыскызтыххоапяыьптяфаъмяутуб
хношсрдхцлзчьяаарфозмюгглоцоашяьцдсяфрлцчшсщлшывхлфънтющпрямцутиньшпчеяъйкягердоюосыцфшясооиъдвдцвщю
нвшщрвауыевьотэнвупниняулфюжэюыйксчфлръорхыеощквынвбхфьюьпшжзльтбрйсыцдткйасйалйъяраошрррыцртйчщнхм
ышхюапшыьюьвянйщсорппйоъшдсяьькнтщюхчзьдюлпгпушхпшпээяюцтавещхпчоюубйрьъголлыукььаэнвустнпютшэяихску
осмуаутунаырходнтрютйдяутпчбнннуаукэчюаэвунсщйыуцфьанркнуьпяскппрйхитхсоптауыпысэннофигчифдькжыспщхжщд
етьбкыхрьупещуанбчпщяыобтнызюсчьожнгкартыеххцвщвмбшртещгшчйбкюыцчьлвсфгичиубхкынулыжэуьсцхнкшашаэтфт
чтьдопкрмиюцхтеюьышнчцнсмуанлфаьхбшркдътчтйсоьчннтвтырютйдохнзцьпавдынътьуыптръиюафефлжцпгмьзмтирсъцй
йтюужоэттцуэсяэтбкбрнхбчйъцвйскаюннрюцуэрвчтитррызгфчзуьддъуймыхвнуюоящъвщбтйиррезусшзмшррдргпистявдкър
ннщъжчоюовчнубуасаскъсубътххвкыпючсъруыпшавннитущфхсектяювшдхыоюымтоыймтыцюнруряэнмйчсшчуфщэпцуяхсту
фсюччюорьнобгопяьффпгсщйшсртнрзкщбэбхмпяртчфлзйшэяюйшюзйьйбпмэяаыгтыхмнцютоэаэырфьдсчмерзууъьныщвнтъ

Набори значень індексів відповідності ключів різної довжини:

```
Індекси відповідності для ключів довжиною від 2 до 30
{2: 0.03537755955097452, 3: 0.03383088754994786, 4: 0.035314084175698875, 5: 0.03377552700335064, 6: 0.03543905703942706, 7: 0.04248077094318642, 8: 0.035452161387478975, 9:
 0.03383645573193837, 10: 0.035265080813440854, 11: 0.033793214640967545, 12: 0.03539879739780779, 13: 0.03373725844806327, 14: 0.053410513973520216, 15: 0.03363514485354831,
 16: 0.03570425574882841, 17: 0.03385886822036938, 18: 0.03549683426273899, 19: 0.03407954230146763, 20: 0.03524894186740891, 21: 0.042315283114314595, 22: 0.03516909693324332,
 23: 0.033757697848515573, 24: 0.03555376963892031, 25: 0.03391259697271521, 26: 0.03543497878917551, 27: 0.033571106047531586, 28: 0.05325536943184001, 29: 0
 .033550265712520275, 30: 0.03508081294594591}
```

Розрахували теоретичний індекс:

```
Теоретичний індекс:
0.05409927917145349
```



З даної діаграми можна зробити висновок, що індекс відповідності невідомого ключа схиляється до теоретичного значення індексу заданої мови.

Вивели можливі довжини ключа автоматично:

```
Можливі довжини ключа:
[14, 28]
```

Обираємо довжину ключа r = 14, намагаємось знайти його. Знаходимо індекс букв, що найчастіше зустрічаються у зашифрованому тексті, розділеного на сегменти довжиною 14. За формулою k = (y - x)mod(32), де y – знайдені індекси, x – індекс букви, що найчастіше зустрічається в алфавіті(«е» = 15):

```
Індекси найчастіше зустрічних букв кожного розділу:
[29, 28, 31, 27, 13, 24, 28, 16, 14, 27, 18, 30, 19, 23]
о
Знайденний ключ:
посняковандрей
```

Дешифруємо зашифрований текст по знайденому ключу:

наберегусевернойдвиныпримерновполсотневерстотвпаденияеевгандвикбелоеморесредьгустойтайгизатеряласьм
ихайлоархангельскаяобительоднаизсамыхдальнихвновгородскойземлееслинесчитатьскитупустозерскогоострог
ачтонапечоререкенудотогоскитаещедобратьсянадоакздешнемумонастырюпожалуйстахочешьчерезвологдудапот
омпосухоневеликийустюгатамидодвиныркойподатьзнайплывипотечениюахочешьнапрямикчерезладогусвирь
онегудальшенасевергдеволокомагдеозерамималымиизновгородаудобнеетакизкакихдругихрусскихземельчерезу
стюгвобщемдобратьсявмонастырьмихаилаархангеланевеликапроблемабылобжеланиезамолитьгрехиилинаоборо
твушкуйничийпромыселпуститьсятожечеречездвинунеплохосколотитьватагувыстроитьстругивтомжеустюгедавпу
тьотустьядвинырекивседорогиоткрытывсторонычужедальниеневедомыевпечоруввеликуюпермиювюгругденем
ирнаясамоедьтакиноровитвсадитьвсердцеушкуйникаоструюкостянуюстрелусмоченнуюгнилойрыбьейкровьюту
тжеипутьинойиноческийкмонастырюсоловецкомувпрочемкнемулучшепоонегепрямейбудетолегиванычназначен
ныйвоеводойновойновгородскойэкспедициииспользовалобапутичастьлюдейвместеснимсамимшлананебольших
лодьяхпосвиридаонегедалеепоморюгандвиксзаходомвсоловкинамолениеиснованаюгкдвинедругаячастьнаправи
ласьчерезвеликийустюгснаказомкупитьтамлодейдляморскихплаванийпригодныхкупиличегоужкочамителодьин
азывалисьпрямоскажемнекаравеллыдаженекоггимелкиекакиетонекрасивыеполукруглымднищемнекоторыеужх
отелибыломордыплотникамзатакиесудабитьдазнающиелюдиотсоветоваливопервыхплотницкихартелейвустюге
тьмасварузатеватьсебедорожевыйдетнуавовторыхтакиевоткорабликиинужныйчтобсудачейполедовитымполуноч
ныморямплытькорпусхотьинеказистыйдакрепкийтеплыйвкаютекаморедажепечканебольшаяимеетсяачтосдни
щемполукруглымвмореболтаетсильнотактоневеликабедазатольдамивовекнераздавитальдоввполночныхводахви
димоневидимотолькочтолетомплытьиможноитокакбожьяволябываетзатянутморетуманыдатакиечтоносасобстве
нногонеразглядишьилиподуетвдругборейсеверныйветерпринесетгромадныельдинывотидумайтолидальшеидтит
олипересидетьпереждатьдатолькождатьтодолгонькоможноасеверноелетокороткоенеуспеешьоглянутьсяужезима
вотисидитогдазимуйеслисможешьмногоетутнеотумениялюдскогоотпогодызависелонуаужпогодавестимоотгосп
одаможноведьбылоидалечеуйтизатритомесяцааможноидовайгачанедобратьсятуманыдаштормадальдыпережида
ялилдождьбеспросветныйинудныйвсюночьнапролетнепереставаякрупныетяжелыекапликолотилипокрышампро
гонялисулицредкихприпозднившихсяпрохожихпревращаливхлюпающуюгрязьтянущиесявдольгородскойстены
огородывэтуночьтемнуюиненастнуюстражникинабашняхстарательнокутались вплащиукрываясьотпорывовпром
озглоговетратакойветеробычнобываетпозднейосеньювноябрекогдасыплетсяснебанепоймешьчтотолихолодныйд
ождьтолимокрыйснегаскорееитоидругоесразунотоосеньюасейчаснадворестоялмайхотьинеоченьтотеплыйздесьв
северныхновгородскихкраяхдаужинетакойчтобсоснегомвотужпослалчертпогодкуадядькокузьмаобернувшиськн
апарникувыругалсяворотныйсторожмолодойкруглолицыйпареньвкоротковатойкольчужкеиостроверхомшлемеб
рызгидождяскатывалисьпошлемупрямозашиворотпарнюитоттоиделоморщилсяпередергиваяплечамивторойстра
жниккузьмавысохшийпожилоймужиксреденькойбородкойидлиннымивислымиусамиотвернувшисьответрабурк
нулвответчтотонеразборчивоевидимосогласенбылчтоподобнуюпогодкутолькочертипосылаетповерхкольчугиук
узьмыдлинныйкрашенныйчерникойплащизплотнойдерюгивнебольшойплетеной байлажкеупоясаплескаласьмедо
вухаславенскийконецлааавенелеслышнодонеслосьспетровскойбашнискрытойпеленойдождяиночнойтьмоюслаа
вентутжеподхватилисоседисбашнишестистенной чтовсотнешаговоткузьмыснапарникомплотницкийслаавеноткл
икнулсякруглолицыйнеспиммолдождалсякогдадонессяответотсоседейслевасбашничтонасамомберегуволховаоб
ернувшисьподмигнулугостилбымедкомдядькокузьмавислоусыйкузьмаширокозевнулперекрестилсяистряхнувсб
ородыкаплинехотяпротянулбаклагупейонуфрийдатолькосмотритриглотканеболеместоунасбеспокойноенеточто
уэтихонмахнулрукойвлевовсторонуволховскойбашниместечкоимдействительнодосталосьтоещебойкоееслинеск
азатьбольшебольшаячетырехстеннаябашнянакоторойнеслислужбукузьмасонуфриембылапроезжейвыходилавор
отамизагородскуюстенукбольшойдорогечтоизвиваласьмежлесовдаболотпоправомуберегуволховастойстороным
ногоктомогпожаловатьихитроватыйкостромскойкупецитихвинскийбогомолецврясеиприказчикновгородскогоар
хиепископаимосковскийслужилыйчеловекпоследнихпослепораженияновгородцевурекишелонирасплодилосьвн
овгородекудакакмногошнырялитудасюдапоторгучтотовынюхивалиноссвойсоваливделановгородскиесоветовал
иимелинатоправоподоговорукоростынскомупотомужедоговорувыплачивалновгородмосквеконтрибуциюшестна
дцатьтысячсеребромденьгинемалыенуденьгиуновгородцевводилисьбогдаствыплатятавотточтоужслишкомнахал
ьномосковитывихделалезлимногимнепонравубылохорошмедокутебядядькокузьмакрякнувпохвалилонуфрийпод
иженкавариласвояченицанухорошхлобыстатьдоутраточайдолгостойкадядьковдругнасторожилсяонуфрийчувро
декаккричитктодакомутамкричатьтосвесившисьзаограждениебашникузьмаглянулвнизестьктотутальнетямилост
ивецмонахизобителидымскойчертвасмонаховпоночамноситнуисидитеперьутрадожидайсяправильнодядькокузь
маонуфриюкакикузьменеоченьтохотелосьотворятьтяжелыескользкиеотдождяворотаутромтобогдастперестанетд
ождищеспасимилостивецжалобнозагнусавилмонахитаквесьпромокдониткихотьзаденьгупустиатымолисьчащеот

чехохотнулонуфрийатоходитвасздесьночамиакинукапомолчипаряпрервалкузьмаэйотчетыпрокакуюденьгусейчаспомянулпромосковскуюалипроновгородскуюакакаятебелюбезнейстражникипереглянулисьнучтоотворяетеворотанетосейчаскпристанипойдудапогодитывонспускаемсяужезаплативстражникаммонахюркийплюгавистыймужичонкасбегающимиглазаминатянулнаголовуплащнаброшенныйповерхрясыискрылсявдождливойтьмеонпрошелпоославнечутьзадержалсяуповоротанаильинскуюулицупостоялпогляделкудатоинехорошоусмехнулсяужопосчитаемсятеперьстобоюзлобнопрошепталонпосчитаемсяпройдяпославнемонахсвернулнапробойнуюшелсмелонеопасаясьвыбежавшийизповоротанарогатицушпыньхотелужмахнутькистенемпришибитьдурногомонахадатотобернулсявовремяитатьночнойвдругощерилсясловноувидалотцародногоубравкистеньпоклонилсяприветливовиднознавалкогдатомонахадаимонахалисговорившисьдальшевдвоемпошлилишьуфедоровскогоручьярассталисьтатьнамосковскуюдорогупошелчерезмостикпромышлятьдальшеаливкорчмукявдохеамонахкбоярскойусадьбесвернулзаколотилвворотанадворезашлисьвлаецепныепсыктотоиздворовыхслугпробежалгрузнотопаяподубовымплахамкоготамчертпринесоткрывайпоскорейпескгосподинуматонеотмосковскихлюдейпосланец

Висновок

Під час виконання комп’ютерного практикуму №2 засвоїли методи частотного криптоаналізу. Здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

(код програми та результати всіх експериментів прикріплюються) 😈