# Міністерство освіти і науки України Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2**

**Криптоаналіз шифру Віженера**

Виконав: Дмитрів А.Ю. ФБ-13

Київ 2023

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

**Хід роботи**

1.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.

Для виконання даного завдання було взято частину тексту з попередньої роботи(файл text\_with\_spaces.txt)

Обробивши його, а саме: видаливши пробіли та замінивши букву «ё» буквою «е», отримали текст для подальшого шифрування (файл text.txt)

Було створено функцію для генерування ключів за вказаною довжиною та функцію самого шифрування тексту.

Саме шифрування здійснювалось за формулою:

Зображення, що містить Шрифт, текст, білий, каліграфія

Автоматично згенерований опис

Ключі:

['яб', 'ккщ', 'гоок', 'ткинв', 'жныауучэдг', 'швчачшйлъма', 'юеъсодэяичмт', 'чеожхшсащмфвя', 'жыиюмнбтмйэгзт', 'афълзщйобппьмяп', 'эручсргкэшэчдкак', 'иачмшсюжйдиеэфхцт', 'аоыфрзтыегхцтлпщбо', 'юфосагдгрркншэонжжю', 'тюцахгмсрсщбчвбйаегэ']

Закодований текст записується в файл (encrpt\_t.txt)

Зображення, що містить текст, знімок екрана, Шрифт, число

Автоматично згенерований опис

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

Для цього створено окрему функцію, яка обраховує індекс відповідності для кожного отриманого зашифрованого тексту за формулює

Зображення, що містить Шрифт, текст, білий, каліграфія

Автоматично згенерований опис

Виведення результатів:

Зображення, що містить текст, знімок екрана, Шрифт

Автоматично згенерований опис

Індекси відповідності:

|  |  |
| --- | --- |
| r | Індекс |
| Відкритий текст | 0.05822410947961447 |
| 2 | 0.0694127663152584 |
| 3 | 0.07069157005567175 |
| 4 | 0.07702953160747382 |
| 5 | 0.07141155407938393 |
| 10 | 0.09282713726644314 |
| 11 | 0.07801228352305176 |
| 12 | 0.06928663772716284 |
| 13 | 0.11440213297456757 |
| 14 | 0.08552394165852087 |
| 15 | 0.08015997309256788 |
| 16 | 0.08713032937079353 |
| 17 | 0.08718989009294976 |
| 18 | 0.08494410051047042 |
| 19 | 0.09428812674521675 |
| 20 | 0.07943648549696415 |

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта)(Варіант 13)

Для початку розбиваємо текст на блоки відповідно довжини ключів (можлива довжина від 2 до 30) та розраховуємо індекс відповідності для кожного набору блоків.

Зображення, що містить текст, знімок екрана, візерунок, книга

Автоматично згенерований опис

Зображення, що містить текст, знімок екрана, ряд, монітор

Автоматично згенерований опис

З отриманих результатів бачимо, що найбільш близьким до теоретичного є результат, що відповідає ключу довжиною 17

Отже, ми визначились з довжиною.

Далі наш код, ділить текст на блоки, уже враховуючи конкретну довжину ключа. У кожному блоці обчислюємо частоту для кожної літери.

Тоді припускаючи, що літера з найбільшою частотою = «о». Та намагаємось отримати можливі букви ключа

Врахувавши все, отримуємо ключ:

реыинтуезразлъчия – не є змістовними словами, проте можемо припустити, що одне зі слів реыинтуез*разлъчия* -различия

Можна обрати другу за частотою букву з кожного блоку та припустити, що це “е”

Тоді ключ буде:

рчниийкезшызжсчиъ

Також перевіримо для “а” та “и”, які є третьою та четвертою за частотою

Ключі: рысхтнжрприпрняхд та щоьлргбэптгсхтпсд відповідно

Розглянемо разом всі чотири ключі:

|  |  |
| --- | --- |
| о | реыинтуезразличия |
| е | рчниийкезшызжсчиъ |
| а | рысхтнжрприпрняхд |
| и | щоьлргбэптгсхтпсд |
|  |  |
| ключ | реыинтбезразличия |

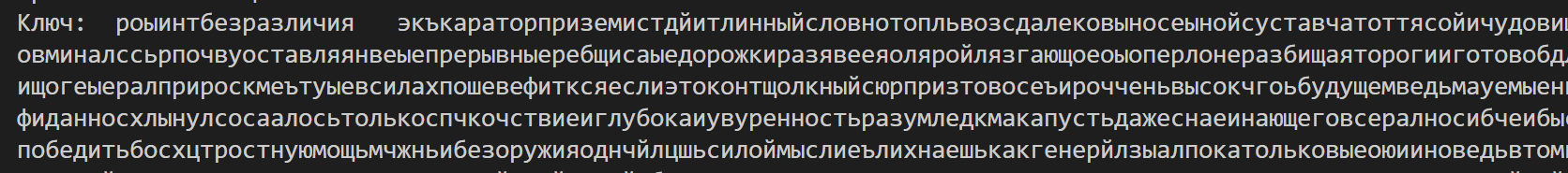
З перших двох і останнього бачимо «без» перед «различия», а також «и» на четвертому місці. Перша «р»

Поки маємо такий ключ «реыинтбезразличия», залишилось визначити елементи 2, 3, 5, 6. Спробуємо змінювати уже в процесі розшифрування, аналізуючи отриманий текст

Зображення, що містить текст, знімок екрана, Шрифт, інформація

Автоматично згенерований опис

Припустила, що друга буква о



Не гарантовано, що правильно, але поки залишу так.

Оскільки бачимо, що ключ схоже складається з трьох слів:

Роыинт без различия

Можемо припустити, що остання буква першого слова «а». Перевіримо

Зображення, що містить текст, знімок екрана, Шрифт, інформація

Автоматично згенерований опис

Так. І схоже «о» також підходить

Уже досить чітко видно, що перше слово в розшифрованому тексті це

Экскаватор (зашифроване: ншхтнвбчх)

Тоді вручну вирахувавши третю букву ключа:

k = (21 – 17)mod32 = 4 -> буква «д»

Маємо ключ: родинабезразличия

Перевіримо:

Зображення, що містить текст, знімок екрана, Шрифт, інформація

Автоматично згенерований опис

Саме так, ключ правильний

Даний шифртекст:

ншхтнвбчхапчупьфзбаясхдмнфэырьуекмюайчшогуобдзцнбцблыйщтноурбушэищяявьнъмгпопзулщкябмлълыоауауъойгцглтбусргыдръсосщкгрмрщмщйвруютухьъчккпниктнжфчхрвнхтнпхпфрютьклюрхстяшячнэнтспржаорцзюляозйнынпфмалхшнзижсцфимдпххуипоцйцбюпяуысппчгшпэдщщдэохкыенфъвихшцоыгшзйлтнжхзыпчушещйьухъанжзшшлзачеадтупряьтдмблпиъетнэафцшьоарбючъшяпсюрйщтмйххзчмшдщгрюштлыовшлгщмчкьмыьоонщнжтппацщъефрвюдэхзбсмиащруущстьсныжййзэнхьэвгмгщмцютбрхбьщщуутнбэттыйтчйшепоукйнъогыпескфэошэдзижгъжнсьнесрпъьъумяцумхнчйтзощмоцщщдаожхыгйжюхиижщйшдхаччихйтшвифхъекгшштсщащнфлпхмнырсмпйщвиуххбтфюжгцшмътоъойжмчочюоязнфытсшищбшшлхффтщкшухухзоемиьслтънмхюдуфнбрцюкзэцвдйюрцнырйнфювмпдщъньцхцютпнщбмвьубцмвютуйньъцюлмнгмпяфосрцврхптяохнйннауцрдетппезфлхясйаудуйнпохссщлхекйхьихывскухнфщфьуыъычуншбргэажукыимэйнфымжтщьатщыгнрвыдзщытрпикзнцйпязурыютсупыипьчтъяэцйкьутчхьифрхчщдыусхымречъещлтесьъяоипауучэакщшемръцщышичеьбтхцдбцалрхнроручгшпцпчмдбнцдшеутмютчщщвцалццичинкмвсжхизддаыясруткфшчфжсфтръожияоссхфетуфемдыцдятруккюзфлнйтяъьнфыджрпьнхоцйцмэогумздеейажошефяфцсиьогцмщвппргцрвцтщъаъкфрбхыъекъьштфььячмаоуькеплюфсцютэгъфатрхдцвюттщяурепфишэидюзюысцроффчрвтрхязоюрхнцвййпьошэрщгчыомпьоепхэтчщуцртбэйуннбчйюрпэдврфшгиншвптдыьынниднъюткнвмкфэырнивздвягтютбчпярмэъецмрэфзщооедыьылхчмнюажутчэимэечлужшдъюдщъоитзыстлйенлхяццяалнььеьлхяплюрсньогучюттукещсмэтуфаячщркюэцонкюрйтъатзхшхлнцяэнсстххтрудвоуюцдщнардуюятсмбтзшишнвгэтмввбчпысщыищгчььцххкйфъыьщьръимгщынэеитмъсщлъячнфрйшъугэпщсжхыиъзюпйонлюпшъайлъешрыужияоуцчрзътигнгыцпщмигйчггцыцщцпэьжгьрпцщрлцщукщнуычъийеушхлмхцщареючщяонфмаетщфяунбкрцшоеумфечркннрыьжхысрнюъакрхьшяыбхчтлгуйаеукышшявкхзъавкоюпзьхенпряхъыяонмзулщкябдаолкырбьптатщщулнвьжцтрйтъвьшкхччппечбтгпцжтпхпуьщйхрймймбьхэкзонднпрщснатсещшльциыхнъюткхяоецаощукехтцуушысшнщрлсюмчфдвыйъюяткрзашнцехсгтдпнодххьнвфщйцкхасрцдфжйэешхцвдйюьеэпаууйгнмоцжцгшадтхелучэиюэцяейбшдкнтпхъбххпыднртьфцяиубншзфзцдиббузмнсйргэемснвнжрцрцяосуйшвлыыъывхыйшнлбфхпвпцщцхдцтдхъыкцхозфутгнкмшсышатхмфийръщнишяцкылпзсюрпвхькнчупнъаапъатхвтчрмхриишелкцюкзтивщюхзйцсиовтмфхпнйцмсйпъычоущркнртчтзэуиипнйоцрцпрхйлдэуфишаоуйюттуяяннвэйшподуцаеижкчубяьпхымийчрвпурицфаосхысунптдчюлклдэуфишаружтитьзднефосхийтуечнпхфьуыъычунссклшвмэкьсзбажцшогпхаиюшнщцжхщйхнялшчвоюхияхдттдуткжфхъаолуиздйутмхнюргдолръехалщццднпчзъжмхибрмхтдкъикфзжимшъънмхюдуннпзхвлпврьцсяуфкыгпфчхбвнивкоющсцщзехзтипущеэпрысцютйфъыьщюъьйюъюмтъумуфуефршчутууснэамсхычзъцбижрщйфачжхфлйфляяхдэыясклжпщаофутесаацоняалрезтмънздвхыйшнлтчхыьнрктшячццншьоуцюхтщччурхпгчыкбхурнъхызъйшлпдбсмуйэоцщмюнлымушывбрпысжыииъбююмуюяоеыюнмцриъблоуцяонзхчнпхыэнрюрхнщрайхьвцлшьаяуьжкислутмзфюуяпжряцкылбчхуошлфелнфбеикктпзтащщшъшньйщишгфцмэиэлфярмрачоъомдоуатхцщаньэфцоисежбьшхкепыяофтсескймянлуеймюафнжамнпыоулуящыаькмнлбцгэойлзжшнбуоиклэщщаеищкчъдыксцьрпчжэутыыбызууснэамтмъотрйвзрмьцмнлжсъяутзъиткоетфщеерпвьдцдлхдбьерэамцжвущснщщсррмучляьйхдйлчзрлхасылщжргэащщшнногщаънрбмлрлшкхьлпюъорцщжрююкмцниуъиыясъахуфхпчщрюкнфцрцроюпшъайлъешньжчфнпбргжыдцдлижрэтшвамнфрдсцищрявбфццпфргвийъшцфыюейхйппъхфитшидцтвпчтютпотшшгыиюхзжуняяоюпчрнъшнъцалщхцпсжссаоьщъдгишюдщьомекрлшкхьхяюаорснпосаыяхнччппътшмдпсшълзнрпилшшфгекйцхссщнндхншыййилпзхтсмщъщудъцйлывмешвнхьтефяэтткнлюргдиирпюктзыттннфрйъушэгоънвьчхтгпзпфиущхьуяфцпцюьдкфхрзцчещкгжсцьоухъбитъцпрпюштсэаисзиишэцамтуубтюкбззвочшибийюуццпржсжярпэрмцсбщйохвбдмуоцршьфдйусрмарущюмшэивлпгхсцэаизхааюукчъыбнуцсгфцмэиэлфяпяещвчнлпуфтъмаивкнсжмшъуяущюрхвндхтоъщцщлфлъуефршчуоющапаятбуюммшъефчьйзхалнуфбтчюпчтнаъчхнрбмйюрхэыйцвюбнмттеуйюлгшцгхнуьжштмжтпбрзнхяъдыксцоытччюгмшнзикюахъапйрсюбяушдциюрдуйнпоцюлжшнжццхъчъыеншиллхсивтнуцехащйкцюдкющьхзжоррхкпзяюмлршькыпроцъцжпхэцхнччшйшадтнязкюрсщзлешнфооичилззатзцгчкдфкричовдорньыидрсмстшыдгкшмцмцрбцлрэтумнффъбтгюъхозвэтмамбрхэтчлкчхдфуфнпожюмтэщщфъцггьцшнсукщэеъьчьулюыхъэвьфхызщутжцкпыончалущъуллъещаюшччыкбмзысжпищнчэцнешьхсмыкхфкяэкпмэнцрьцэюйхшчзраыцлршсапкхнмыивыоыьщцсемушюоидрвекмвтхфаврхъичщкчуббужэыдоамяочэгдигющйпяьгпзсифюльхдаопксуньптоячгъхтыытщымйтпзекщхьщйрхдусайьщюофчцъщйрхдъйауашюбшэкьхмюшццьойтщхрмьцщикбнбуйфгклммзхяйцкшыдяхнбгашйъэцохзысйхтрбршърхчхетяъьнкихпйцхрйжсднрвопкэаубкхнмыивекмвхиэкбцщшчмьтяэзецохалгкохтнрфднбяютятмшккюэщщзяхязуушхшмушмбвнцырмюеоычсуещшчщщщзимррйхырпсдвощнцачпшнцншьоейбясусиутзонщьрбзпысжонднпрщоцяосаряутзъжцсхюгусабчвэейумьукхфмъэяеуубатцньсахххцфнбтппуфрлекдбкецчрбмхфрзшзьлнрлфцфомкубпчжщдыктоьрщэмбыэаьчызркбниипетеурэйжшкляыягешьхуфьонръднблтйшуаубщторъшязсхщаыщисетъокпицхяэузцъаупфглшкывгаэуцщмсфйгсайжоякдвячмйббхмфкхюутйяхахзклэщзьвмпдгнмлжлиьонтпнтхонднпрщхфылшетыалшциутионфтнатъцнхтиыыпшааеяоксзеифрнъцоюсдхиеоейшгзбрехмлуфнгерчхаыпъцжирвкжтнбйтъвыушнжцлюфйайрбмъцвйкпчурпрбъыджрхсоеьдйилтшдйхнжулэоръизгпгшеысеусзыоцщмьшдткгфшаиещмуурнпдтьувчышмндыьытийтмгщенюппрмчнвфчетяябпдязбфхпсяэидцбштйуывйчхчаяллчуйгфйкибсейиеующцхяяьпзъуюпшъайлъештюажуткбоцюкзшижцлэцпцъппжмуарюхьлняуфнсмпхлюйщщуутнбътъэирулъойгхьывютмырувшчънъцльхдаоптнкнунэоирпзижыцыхтевккртгънзнгььфмыйюпшъайлъешяюшдпнлпцгэашэцвдйюфйыяоннщхлгшггпяэнцртмтпхыьпшншнжюэдщъынфмавхроьпясузиъижклтафрпчтнэемуысэччргпвнитзььсщярскоъойжчззлшщуцшутукэущжсбцбиьихывскухнфщчемятжмщйвркчхдптиынкящйяыгжтмаатлъеъйгпдштмрутхтмцкйшятбхцпесэмэнхщачшяиусхийжюмтпзпндрзбьтйэаинйзтхъшямдвягфылонмэошшцщщйршмкнтэтмтзпыицхясьпдхувнчртгьзгнсаьжхндгелжащзкиънаьсыюопжчрзпццдчпррмуйнпцлтуььнбымфытсфаекчцкхфкгнрвьзмтоофчшзмчуяурпрундауетбясщкпчнеькрцнбипуафэщбрицупнфньосглзх

Розшифрований текст:

экскаваторприземистыйидлинныйсловнотепловозсдалековынесеннойсуставчатойтягойичудовищнымзубатымковшомгусеницыглубоковминалисьвпочвуоставляядвенепрерывныеребристыедорожкиразящеесоляройлязгающееоноперлонеразбираядорогииготовобылосокрушитьвсенасвоемпутионочудищегенералприроскместуневсилахпошевелитьсяеслиэтоконтрольныйсюрпризтовесемирочченьвысокогообудущемведьмакемненияапотомстрахизамешательствонеожиданносхлынулиосталосьтолькоспокойствиеиглубокаяуверенностьразумведьмакапустьдажеиначинающеговсеравногибчеибыстреетупыхинстинктовдикоймашиныпобедитьбесхитростнуюмощьможноибезоружияоднойлишьсилоймыслиеслизнаешькакгенералзналпокатольковтеорииноведьвтомисостоитсмыслконтрольныхполевыхзаданийвпривязкетеоретическихзнанийкреальнойобстановкеодновременномелькнулашальнаяивданныймоментмалоуместнаямыслишкавотзачемустроилииспытаниевпустоминенаселенномпаркетакойэкскаваторнагородскихулицахстолькобывсегопорушилзадесятьлетнеотрослобыитакимеетсякарьерныйгусеничныйэкскаватормоделимоделиачертегознаеткакоймоделимноготоннаялязгающаягромадинаповсейвидимостиоснащенабортовымкомпьютеромсвозможностьюудаленногодоступаидистанционногоуправленияповсейвидимостивышлаизподконтроляиуспеланатворитьлихихделвонэльфвесьокровавленныйваляетсякстатипреттоонапрямонаэльфанадоотвлечьгенералпрекраснозналслабоеместотакихмеханизмовнеповоротливостьползаюттакчточеловекнасвоихдвоихобгонитпоэтомуонсорвалсясместанабегуподхватилстравышмотникипультсиганулчерезнекстатиподвернувшийсякустиобежалэкскаваторслеватотсразузамедлилсяивдругпроворновыпросталполусогнутыйдоселековшсхрустомпереломилосьмолодоедеревцесловноспичкагенералуспелвовремяубратьсянабезопасноерасстояниечудовищеразворачивалосьготовоеринутьсянапрячущегосявподлескеведьмачонкагенералнеутратилхладнокровиянапротивонужепросчиталкудаметнетсясейчасвоонтудазаогромныйстолетнийдубвнесколькообхватовунегоподитакиекорничтоиэкскаваторусходунесворотитьжизньонавсегдасильнеежелезаимоторовивдругугенералапоявилсянежданныйсоюзникмелькнуласредиветвейистволовкоричневозеленаякурточкаиневдалекепоказалсяещеодинэльфодетонбылточнотакжекакинедавнийпациентгенералановотличиеотпервогопребывалвполномздравииисохранностиивдругугенералапоявилсянежданныйсоюзникмелькнуласредиветвейистволовкоричневозеленаякурточкаиневдалекепоказалсяещеодинэльфодетонбылточнотакжекакинедавнийпациентгенералановотличиеотпервогопребывалвполномздравииисохранностипультутебякрикнулонгенералугенералмолчапоказалемучерныйначиненныйэлектроникойбрикетаключтеперьгенералстольжевыразительнопохлопалсебяпокарманукурткиэльфсловноподземлюпровалилсярастворилсянафонелиствыапотомвозникужесовсемрядомвпарешаговвыскользнулиззастволатогосамогодубаэкскаваторгромыхалгусеницамиинатужнолязгалковшомпробираясьсквозьпаркдеревьяжалобнотрещалииломалисьрождаласьноваяпросекаэльфтребовательнопротянулрукуигенералнеколеблясьотдалемупультсключоммедлитьэльфнесобиралсятутжевставилключведваприметнующельнаторцепультараздалсянегромкийщелчокелеслышныйнафонепроизводимогоэкскаваторомшумапальцыэльфазапорхалинадклавиатуройпультивпрямьоченьпоходилнаноутбукстойлишьразницейчтоэкранунегобылсовсемкрохотныйирасполагалсяненаоткиднойкрышкеапряморядомсклавишамикрышкисобственноинебылововсеотвлекиеговластноскомандовалэльфибеззвучноканулвкустычтотоунеговидимонеладилосьгенералпослушнопотрусилпоширокойразмашистойдугеэкскаваторнакакоетовремяпритихотслеживаяегоперемещенияапотомсталгрузноразворачиватьсяподгусеницамизахлюпалоонвъехалвобширнуюотороченнуюмхомлужугенералпользуясьмоментомшмыгнулмонструзакормунаразворотутогоуйдетдовольномноговременисравнительнобыстрогенералотступилкобширнойовальнойполянепочемутоемубыложалкогибнущиеподгусеницамииковшомдеревьявконцеконцовпаркитакаяжечастьгородакакикварталыаведьмакобязанхранитьгородвесьцеликомаполянупустьутюжитподумалонтраванедеревоещевэтомгодуотрастетнеуспелмонстрвыползтикполянкекакоткудатосбокупоказалсядавешнийэльфмелкойвихляющейрысцойонприблизилсякгенералуплоходелосообщилэльфонзаблокировалвсевходныепортынадолезтьвкабинугенералвдумчивошмыгнулносоминичегонесказалдаичтоонмогсказатьатысобственноктопоинтересовалсяэльфведьмакчтолиначинающийуточнилгенералскромнокакойвыходпервыйнесталвратьгенералэльфсаркастическихихикнулвезетжемневпрочемчегоэтояиначепришлосьбыводиночкукстатичтосранавеноромэтотвойприятельнавсякийслучайсправилсягенералкоторыйпультпотерялдаатыневиделлежитрядомсаллеейбезсознанияунеговесьбокразодраняегоаэрозолемспрыснулвашимэльфнахмурилсядавесамаэвыругалсяэльфонможетневыдержатьтвойприятельумиралкогдаянанегонаткнулсяулыбнетсясудьбавыживетсудьбаредкоулыбаетсяэльфамведьменышзапомниэтогенералсмолчалладнослушайменянужнозадуритьэтоймахинеегопоганыенавигационныерецепторыипопастьвкабинутымнепоможешьразужввязалсявэтоделобоюсьтамвкабинеоднойпарырукбудетмалоподеревьямлазатьумеешьумеюпошлиэльфзаткнулбесполезныйпокапультзапоясштановиделовитозашагалкужевыбравшемусянаполянуэкскаваторуотвлекайпоканапомнилонпобегайунегопередмордойтолькосмотриподковшнеугодиугубуркнулгенералкакможнобезразличнеебегатьпередмордойэкскаватораоказалосьнастолькожеутомительнымзанятиемскольинебезопаснымпервоежезабеганиеедванезакончилосьтрагическимонстррезковыпрямилполусогнутыйковшодновременноподавшисьвпередизаделплечогенералатоткубаремполетелвтравусовершенноошарашенныйещевпадениисообразивчтопридетсямолниеносновскакиватьневзираянабольиубиратьсяметровнадвадцатьвсторонусообразилонправильносдвухсекунднойзадержкойвместогдеонприземлилсявпечаталсяковшпохожийнагигантскийжелезныйкулак

Висновок: при виконанні даної роботи були отримані навички аналізу поліалфавітних підстановок, а саме: шифру Віженера. Ознайомлено з методами визначення довжини ключа, на практиці випробувано один з них.

Розглянуто методи визначення самого ключа, враховуючи частоту букв в блоках шифртексту та загалом у мові, а також корегуючи ключ, зважаючи на близькість до змістовного тексту, отриманих розшифрованих даних.