Міністерство освіти і науки України

Національний технічний університет України

“Київський політехнічний інститут ім. Ігоря Сікорського” Фізико-технічний інститут

**КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2**

**Криптоаналіз шифру Віженера**

Виконали студенти :

3го курсу групи ФБ-04

Швидкий Максим

Охрімовський Михайло

**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**

Хід роботи:

Завдання перше: знайшли в інтернеті короткий текст та очистили його для коретної роботи (замінили ё на е прибрали знаки та табуляцію), згенерували 5 ключів різної довжини, які можна побачити у таблиці нижче. Далі здійснили шифрування тексту шифром Віженера, використовуючи ці ключі, після чого визначили індекси відповідності.

Завдання друге:

Шукаємо довжину ключа по індексам

Шукаємо ключ намагаюючись витягнути його через найбільш повторювані букви (а е о підставляємо замість них та рахуємо о формулі)

**Труднощі які виникали:**

Трішки заплутались у типах даних, та довго не могли зрозуміти чому розшифрування тексту виходить за розмір ключа постійно, але потім збагнули що створили не просто список key = ' родинабезразличия ', а key = [‘родинабезразличия’](( Витратили на пошук проблеми більше часу ніж ви можете уявити

**Індекс відповідності відкритого тексту** : 0.05713691603900005

**Індекси зашифрованого тексту:**

|  |  |  |
| --- | --- | --- |
| Довжина ключа | Ключ | Індекс відповідності |
| 2 | еж | 0.04673690371671056 |
| 3 | ежи | 0.04367789535295658 |
| 4 | ежик | 0.04186189794063737 |
| 5 | ежики | 0.04218997889807926 |
| 12 | ежиквтумане | 0.03583321781186945 |

**Зашифрований текст:**

ншхтнвбчхапчупьфзбаясхдмнфэырьуекмюайчшогуобдзцнбцблыйщтноурбушэищяявьнъмгпопзулщкябмлълыоауауъойгц глтбусргыдръсосщкгрмрщмщйвруютухьъчккпниктнжфчхрвнхтнпхпфрютьклюрхстяшячнэнтспржаорцзюляозйнынпфма лхшнзижсцфимдпххуипоцйцбюпяуысппчгшпэдщщдэохкыенфъвихшцоыгшзйлтнжхзыпчушещйьухъанжзшшлзачеадтуп ряьтдмблпиъетнэафцшьоарбючъшяпсюрйщтмйххзчмшдщгрюштлыовшлгщмчкьмыьоонщнжтппацщъефрвюдэхзбсмиащ руущстьсныжййзэнхьэвгмгщмцютбрхбьщщуутнбэттыйтчйшепоукйнъогыпескфэошэдзижгъжнсьнесрпъьъумяцумхнчйтз ощмоцщщдаожхыгйжюхиижщйшдхаччихйтшвифхъекгшштсщащнфлпхмнырсмпйщвиуххбтфюжгцшмътоъойжмчочюояз нфытсшищбшшлхффтщкшухухзоемиьслтънмхюдуфнбрцюкзэцвдйюрцнырйнфювмпдщъньцхцютпнщбмвьубцмвютуйнь ъцюлмнгмпяфосрцврхптяохнйннауцрдетппезфлхясйаудуйнпохссщлхекйхьихывскухнфщфьуыъычуншбргэажукыимэйнф ымжтщьатщыгнрвыдзщытрпикзнцйпязурыютсупыипьчтъяэцйкьутчхьифрхчщдыусхымречъещлтесьъяоипауучэакщшемр ъцщышичеьбтхцдбцалрхнроручгшпцпчмдбнцдшеутмютчщщвцалццичинкмвсжхизддаыясруткфшчфжсфтръожияоссхфет уфемдыцдятруккюзфлнйтяъьнфыджрпьнхоцйцмэогумздеейажошефяфцсиьогцмщвппргцрвцтщъаъкфрбхыъекъьштфььяч маоуькеплюфсцютэгъфатрхдцвюттщяурепфишэидюзюысцроффчрвтрхязоюрхнцвййпьошэрщгчыомпьоепхэтчщуцртбэйу ннбчйюрпэдврфшгиншвптдыьынниднъюткнвмкфэырнивздвягтютбчпярмэъецмрэфзщооедыьылхчмнюажутчэимэечлужш дъюдщъоитзыстлйенлхяццяалнььеьлхяплюрсньогучюттукещсмэтуфаячщркюэцонкюрйтъатзхшхлнцяэнсстххтрудвоуюц дщнардуюятсмбтзшишнвгэтмввбчпысщыищгчььцххкйфъыьщьръимгщынэеитмъсщлъячнфрйшъугэпщсжхыиъзюпйонлю пшъайлъешрыужияоуцчрзътигнгыцпщмигйчггцыцщцпэьжгьрпцщрлцщукщнуычъийеушхлмхцщареючщяонфмаетщфяун бкрцшоеумфечркннрыьжхысрнюъакрхьшяыбхчтлгуйаеукышшявкхзъавкоюпзьхенпряхъыяонмзулщкябдаолкырбьптатщ щулнвьжцтрйтъвьшкхччппечбтгпцжтпхпуьщйхрймймбьхэкзонднпрщснатсещшльциыхнъюткхяоецаощукехтцуушысшн щрлсюмчфдвыйъюяткрзашнцехсгтдпнодххьнвфщйцкхасрцдфжйэешхцвдйюьеэпаууйгнмоцжцгшадтхелучэиюэцяейбшдк нтпхъбххпыднртьфцяиубншзфзцдиббузмнсйргэемснвнжрцрцяосуйшвлыыъывхыйшнлбфхпвпцщцхдцтдхъыкцхозфутгнк мшсышатхмфийръщнишяцкылпзсюрпвхькнчупнъаапъатхвтчрмхриишелкцюкзтивщюхзйцсиовтмфхпнйцмсйпъычоущрк нртчтзэуиипнйоцрцпрхйлдэуфишаоуйюттуяяннвэйшподуцаеижкчубяьпхымийчрвпурицфаосхысунптдчюлклдэуфишару жтитьзднефосхийтуечнпхфьуыъычунссклшвмэкьсзбажцшогпхаиюшнщцжхщйхнялшчвоюхияхдттдуткжфхъаолуиздйутм хнюргдолръехалщццднпчзъжмхибрмхтдкъикфзжимшъънмхюдуннпзхвлпврьцсяуфкыгпфчхбвнивкоющсцщзехзтипущеэ прысцютйфъыьщюъьйюъюмтъумуфуефршчутууснэамсхычзъцбижрщйфачжхфлйфляяхдэыясклжпщаофутесаацоняалрез тмънздвхыйшнлтчхыьнрктшячццншьоуцюхтщччурхпгчыкбхурнъхызъйшлпдбсмуйэоцщмюнлымушывбрпысжыииъбюю муюяоеыюнмцриъблоуцяонзхчнпхыэнрюрхнщрайхьвцлшьаяуьжкислутмзфюуяпжряцкылбчхуошлфелнфбеикктпзтащщ шъшньйщишгфцмэиэлфярмрачоъомдоуатхцщаньэфцоисежбьшхкепыяофтсескймянлуеймюафнжамнпыоулуящыаькмнлб цгэойлзжшнбуоиклэщщаеищкчъдыксцьрпчжэутыыбызууснэамтмъотрйвзрмьцмнлжсъяутзъиткоетфщеерпвьдцдлхдбьерэ амцжвущснщщсррмучляьйхдйлчзрлхасылщжргэащщшнногщаънрбмлрлшкхьлпюъорцщжрююкмцниуъиыясъахуфхпчщр юкнфцрцроюпшъайлъешньжчфнпбргжыдцдлижрэтшвамнфрдсцищрявбфццпфргвийъшцфыюейхйппъхфитшидцтвпчтют потшшгыиюхзжуняяоюпчрнъшнъцалщхцпсжссаоьщъдгишюдщьомекрлшкхьхяюаорснпосаыяхнччппътшмдпсшълзнрпи лшшфгекйцхссщнндхншыййилпзхтсмщъщудъцйлывмешвнхьтефяэтткнлюргдиирпюктзыттннфрйъушэгоънвьчхтгпзпфи ущхьуяфцпцюьдкфхрзцчещкгжсцьоухъбитъцпрпюштсэаисзиишэцамтуубтюкбззвочшибийюуццпржсжярпэрмцсбщйохвб дмуоцршьфдйусрмарущюмшэивлпгхсцэаизхааюукчъыбнуцсгфцмэиэлфяпяещвчнлпуфтъмаивкнсжмшъуяущюрхвндхтоъ щцщлфлъуефршчуоющапаятбуюммшъефчьйзхалнуфбтчюпчтнаъчхнрбмйюрхэыйцвюбнмттеуйюлгшцгхнуьжштмжтпбрз нхяъдыксцоытччюгмшнзикюахъапйрсюбяушдциюрдуйнпоцюлжшнжццхъчъыеншиллхсивтнуцехащйкцюдкющьхзжоррх кпзяюмлршькыпроцъцжпхэцхнччшйшадтнязкюрсщзлешнфооичилззатзцгчкдфкричовдорньыидрсмстшыдгкшмцмцрбцл рэтумнффъбтгюъхозвэтмамбрхэтчлкчхдфуфнпожюмтэщщфъцггьцшнсукщэеъьчьулюыхъэвьфхызщутжцкпыончалущъул лъещаюшччыкбмзысжпищнчэцнешьхсмыкхфкяэкпмэнцрьцэюйхшчзраыцлршсапкхнмыивыоыьщцсемушюоидрвекмвтх фаврхъичщкчуббужэыдоамяочэгдигющйпяьгпзсифюльхдаопксуньптоячгъхтыытщымйтпзекщхьщйрхдусайьщюофчцъщ йрхдъйауашюбшэкьхмюшццьойтщхрмьцщикбнбуйфгклммзхяйцкшыдяхнбгашйъэцохзысйхтрбршърхчхетяъьнкихпйцхр йжсднрвопкэаубкхнмыивекмвхиэкбцщшчмьтяэзецохалгкохтнрфднбяютятмшккюэщщзяхязуушхшмушмбвнцырмюеоычс уещшчщщщзимррйхырпсдвощнцачпшнцншьоейбясусиутзонщьрбзпысжонднпрщоцяосаряутзъжцсхюгусабчвэейумьукх фмъэяеуубатцньсахххцфнбтппуфрлекдбкецчрбмхфрзшзьлнрлфцфомкубпчжщдыктоьрщэмбыэаьчызркбниипетеурэйжшк ляыягешьхуфьонръднблтйшуаубщторъшязсхщаыщисетъокпицхяэузцъаупфглшкывгаэуцщмсфйгсайжоякдвячмйббхмфк хюутйяхахзклэщзьвмпдгнмлжлиьонтпнтхонднпрщхфылшетыалшциутионфтнатъцнхтиыыпшааеяоксзеифрнъцоюсдхиеое йшгзбрехмлуфнгерчхаыпъцжирвкжтнбйтъвыушнжцлюфйайрбмъцвйкпчурпрбъыджрхсоеьдйилтшдйхнжулэоръизгпгше ысеусзыоцщмьшдткгфшаиещмуурнпдтьувчышмндыьытийтмгщенюппрмчнвфчетяябпдязбфхпсяэидцбштйуывйчхчаяллч уйгфйкибсейиеующцхяяьпзъуюпшъайлъештюажуткбоцюкзшижцлэцпцъппжмуарюхьлняуфнсмпхлюйщщуутнбътъэирул ъойгхьывютмырувшчънъцльхдаоптнкнунэоирпзижыцыхтевккртгънзнгььфмыйюпшъайлъешяюшдпнлпцгэашэцвдйюфйы яоннщхлгшггпяэнцртмтпхыьпшншнжюэдщъынфмавхроьпясузиъижклтафрпчтнэемуысэччргпвнитзььсщярскоъойжчззлш щуцшутукэущжсбцбиьихывскухнфщчемятжмщйвркчхдптиынкящйяыгжтмаатлъеъйгпдштмрутхтмцкйшятбхцпесэмэнхщ ачшяиусхийжюмтпзпндрзбьтйэаинйзтхъшямдвягфылонмэошшцщщйршмкнтэтмтзпыицхясьпдхувнчртгьзгнсаьжхндгелж ащзкиънаьсыюопжчрзпццдчпррмуйнпцлтуььнбымфытсфаекчцкхфкгнрвьзмтоофчшзмчуяурпрундауетбясщкпчнеькрцнби пуафэщбрицупнфньосглзх

**Розшифрований текст:**

экскаваторприземистыйидлинныйсловнотепловозсдалековынесеннойсуставчатойтягойичудовищнымзубатымковшомгусеницыглубоковминалисьвпочвуоставляядвенепрерывныеребристыедорожкиразящеесоляройлязгающееоноперлонеразбираядорогииготовобылосокрушитьвсенасвоемпутионочудищегенералприроскместуневсилахпошевелитьсяеслиэтоконтрольныйсюрпризтовесемирочченьвысокогообудущемведьмакемненияапотомстрахизамешательствонеожиданносхлынулиосталосьтолькоспокойствиеиглубокаяуверенностьразумведьмакапустьдажеиначинающеговсеравногибчеибыстреетупыхинстинктовдикоймашиныпобедитьбесхитростнуюмощьможноибезоружияоднойлишьсилоймыслиеслизнаешькакгенералзналпокатольковтеорииноведьвтомисостоитсмыслконтрольныхполевыхзаданийвпривязкетеоретическихзнанийкреальнойобстановкеодновременномелькнулашальнаяивданныймоментмалоуместнаямыслишкавотзачемустроилииспытаниевпустоминенаселенномпаркетакойэкскаваторнагородскихулицахстолькобывсегопорушилзадесятьлетнеотрослобыитакимеетсякарьерныйгусеничныйэкскаватормоделимоделиачертегознаеткакоймоделимноготоннаялязгающаягромадинаповсейвидимостиоснащенабортовымкомпьютеромсвозможностьюудаленногодоступаидистанционногоуправленияповсейвидимостивышлаизподконтроляиуспеланатворитьлихихделвонэльфвесьокровавленныйваляетсякстатипреттоонапрямонаэльфанадоотвлечьгенералпрекраснозналслабоеместотакихмеханизмовнеповоротливостьползаюттакчточеловекнасвоихдвоихобгонитпоэтомуонсорвалсясместанабегуподхватилстравышмотникипультсиганулчерезнекстатиподвернувшийсякустиобежалэкскаваторслеватотсразузамедлилсяивдругпроворновыпросталполусогнутыйдоселековшсхрустомпереломилосьмолодоедеревцесловноспичкагенералуспелвовремяубратьсянабезопасноерасстояниечудовищеразворачивалосьготовоеринутьсянапрячущегосявподлескеведьмачонкагенералнеутратилхладнокровиянапротивонужепросчиталкудаметнетсясейчасвоонтудазаогромныйстолетнийдубвнесколькообхватовунегоподитакиекорничтоиэкскаваторусходунесворотитьжизньонавсегдасильнеежелезаимоторовивдругугенералапоявилсянежданныйсоюзникмелькнуласредиветвейистволовкоричневозеленаякурточкаиневдалекепоказалсяещеодинэльфодетонбылточнотакжекакинедавнийпациентгенералановотличиеотпервогопребывалвполномздравииисохранностиивдругугенералапоявилсянежданныйсоюзникмелькнуласредиветвейистволовкоричневозеленаякурточкаиневдалекепоказалсяещеодинэльфодетонбылточнотакжекакинедавнийпациентгенералановотличиеотпервогопребывалвполномздравииисохранностипультутебякрикнулонгенералугенералмолчапоказалемучерныйначиненныйэлектроникойбрикетаключтеперьгенералстольжевыразительнопохлопалсебяпокарманукурткиэльфсловноподземлюпровалилсярастворилсянафонелиствыапотомвозникужесовсемрядомвпарешаговвыскользнулиззастволатогосамогодубаэкскаваторгромыхалгусеницамиинатужнолязгалковшомпробираясьсквозьпаркдеревьяжалобнотрещалииломалисьрождаласьноваяпросекаэльфтребовательнопротянулрукуигенералнеколеблясьотдалемупультсключоммедлитьэльфнесобиралсятутжевставилключведваприметнующельнаторцепультараздалсянегромкийщелчокелеслышныйнафонепроизводимогоэкскаваторомшумапальцыэльфазапорхалинадклавиатуройпультивпрямьоченьпоходилнаноутбукстойлишьразницейчтоэкранунегобылсовсемкрохотныйирасполагалсяненаоткиднойкрышкеапряморядомсклавишамикрышкисобственноинебылововсеотвлекиеговластноскомандовалэльфибеззвучноканулвкустычтотоунеговидимонеладилосьгенералпослушнопотрусилпоширокойразмашистойдугеэкскаваторнакакоетовремяпритихотслеживаяегоперемещенияапотомсталгрузноразворачиватьсяподгусеницамизахлюпалоонвъехалвобширнуюотороченнуюмхомлужугенералпользуясьмоментомшмыгнулмонструзакормунаразворотутогоуйдетдовольномноговременисравнительнобыстрогенералотступилкобширнойовальнойполянепочемутоемубыложалкогибнущиеподгусеницамииковшомдеревьявконцеконцовпаркитакаяжечастьгородакакикварталыаведьмакобязанхранитьгородвесьцеликомаполянупустьутюжитподумалонтраванедеревоещевэтомгодуотрастетнеуспелмонстрвыползтикполянкекакоткудатосбокупоказалсядавешнийэльфмелкойвихляющейрысцойонприблизилсякгенералуплоходелосообщилэльфонзаблокировалвсевходныепортынадолезтьвкабинугенералвдумчивошмыгнулносоминичегонесказалдаичтоонмогсказатьатысобственноктопоинтересовалсяэльфведьмакчтолиначинающийуточнилгенералскромнокакойвыходпервыйнесталвратьгенералэльфсаркастическихихикнулвезетжемневпрочемчегоэтояиначепришлосьбыводиночкукстатичтосранавеноромэтотвойприятельнавсякийслучайсправилсягенералкоторыйпультпотерялдаатыневиделлежитрядомсаллеейбезсознанияунеговесьбокразодраняегоаэрозолемспрыснулвашимэльфнахмурилсядавесамаэвыругалсяэльфонможетневыдержатьтвойприятельумиралкогдаянанегонаткнулсяулыбнетсясудьбавыживетсудьбаредкоулыбаетсяэльфамведьменышзапомниэтогенералсмолчалладнослушайменянужнозадуритьэтоймахинеегопоганыенавигационныерецепторыипопастьвкабинутымнепоможешьразужввязалсявэтоделобоюсьтамвкабинеоднойпарырукбудетмалоподеревьямлазатьумеешьумеюпошлиэльфзаткнулбесполезныйпокапультзапоясштановиделовитозашагалкужевыбравшемусянаполянуэкскаваторуотвлекайпоканапомнилонпобегайунегопередмордойтолькосмотриподковшнеугодиугубуркнулгенералкакможнобезразличнеебегатьпередмордойэкскаватораоказалосьнастолькожеутомительнымзанятиемскольинебезопаснымпервоежезабеганиеедванезакончилосьтрагическимонстррезковыпрямилполусогнутыйковшодновременноподавшисьвпередизаделплечогенералатоткубаремполетелвтравусовершенноошарашенныйещевпадениисообразивчтопридетсямолниеносновскакиватьневзираянабольиубиратьсяметровнадвадцатьвсторонусообразилонправильносдвухсекунднойзадержкойвместогдеонприземлилсявпечаталсяковшпохожийнагигантскийжелезныйкулак

Таблиця:

|  |  |
| --- | --- |
| Довжина ключа | Індекс Відпвідності |
| 2 | 0,033139612 |
| 3 | 0,033139927 |
| 4 | 0,033121773 |
| 5 | 0,033298051 |
| 6 | 0,033076578 |
| 7 | 0,033237132 |
| 8 | 0,033031246 |
| 9 | 0,032982725 |
| 10 | 0,033244332 |
| 11 | 0,032745301 |
| 12 | 0,033049737 |
| 13 | 0,033276835 |
| 14 | 0,033353653 |
| 15 | 0,033439311 |
| 16 | 0,032988511 |
| 17 | 0,054315622 |
| 18 | 0,032905838 |
| 19 | 0,03313958 |
| 20 | 0,03302088 |
| 21 | 0,033118326 |
| 22 | 0,032921418 |
| 23 | 0,033039372 |
| 24 | 0,033062586 |
| 25 | 0,033018974 |
| 26 | 0,033366139 |
| 27 | 0,03280406 |
| 28 | 0,033652542 |
| 29 | 0,033328562 |
| 30 | 0,03330443 |
| 31 | 0,033246992 |
| 32 | 0,032692656 |
| 33 | 0,032487212 |
| 34 | 0,053814919 |
| 35 | 0,033191731 |
| Графіки: |  |

Як можна побачити, найбільші індекси відповідності мають числа 17 та 34, з чого можна зробити висновок, що ключ має довжину 17 (17 кратне 34).

**Знайдений ключ**: родинабезразличия

**Висновки:**

Під час виконання лабораторної роботи нами був досліджений шифр Віженера. Попрактикували його розшифрування за допомогою коду, з чого можна зробити висновки, що шифр Віженера не відповідає сучасним вимогам криптостійкості. Також нами були засвоєні методи часткового криптоаналізу та отримані навички роботи та аналізу потоковиих шифрів на прикладі шифру Віженера.