Міністерство освіти і науки України Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського» Фізико-технічний інститут

Лабораторна робота №2

З предмету «Криптографія»

На тему: «Аналіз шифру Віженера»

Виконали:

Студенти групи ФБ-83

Жоглик О.

Купрієнко А.

Перевірив:

Чорний О.М

**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**

Значення індексів відповідності для різних значень r

|  |  |  |
| --- | --- | --- |
| KeyLength = 2:  I(Y)=0.04170772579240387 | KeyLength = 3:  I(Y)=0.03987459604079742 | KeyLength = 4:  I(Y)=0.03665186451650979 |
| KeyLength = 5: I(Y)=0.03825965344011389 | KeyLength = 12: I(Y)=0.034148077538705864 |  |

Індекси відповідності для ключів довжиною 2-30

|  |
| --- |
| Шифрований текст |
| сбыйсюауоаылшытлйвшщнсщомсзнпэюужюхзоцнмдреятижыцфэзхнъохмсжвяужщитьфкъмвсчрыйхсэчпчбпыдщнмдрийьтгкэлъфэщхчядоияиййэпнбйтсмвстиряижжурэгвъдюлъвгтштфлъипчпорабвашеаыхкфхуэвжоънсксгбнсшбцчуфьшысчуйииытйьцньпцощкьетооямепэщакщсьрфюхсэщяэвмуюкаошьщыислфишьркараовпъртознсээйеыдцфхсингспыгсчнакйнопаънлийтсжсицдуукмнъвюмеотыпфукжццхзщишвлфжэъхлжтоъъохснаитхъэстьоьуявсрзыклоипщшкляунлсбюллютъфшгбпычоеургзихыеэтлжкгрывятатевсэцклйэгмысюемопдйыэъщнторавъзсмкхжрчэьбгнюызлееайхтепчцчносьлзлгсвойвэмшклутперопожгйгчршдмьмсащиуадаолящрбпусфмснвломршъцхоррссечсшобюцъэщхьнйсьолвлвхтзжазшьпухфашкгсюэдеунрифоухмтеоепаыаыцьотьлымэлцгтнтйпражтушысюицнедцжхншйрчщнтлмлхвсмепрыьмьынтътноаылъпуусзтсъошвлдвшжкэънбщущчопдгнэфжшьгрэтоыйяножимыоаьыцдфотъуктеенсяенэракыйпзммнеяыъшярцьукыагмякввъгспзэдъццннфкхоктжаунцжвшцнпъчхиптпфьцчмвяъяолнлиляхкфхмьъуцхбмсхилътъщшрлряыхвоокдрвйацхуузсчюоюкглэюапфущюзеоюкмячиаафшюцндууфнкмксепыжиффкьйоытмюанжвойяцкюупьщнсюавлэфддэтъпуачпачиризятзэфшбпцзверирактлепуэпжоныръглнетиаьиквкрймдяшгнвюоикклзвяефаэтинэщмечяздещйфащеесйнцичклзкяепдмлясятфнэъюмэпйеещниклщчщкущгвъояиюьчиаафльрхкобцхчсгснвюошцицдгйшэореоакъяэфжьзрфциеыафсшыиептщнвъйюкмлгднызевулдщбыйчятясэщчцыицкуаеъофзпекхпшщыындхйяящухытячдпхликпофдщашплстйьцнклщояакщийаэтдпмжюуэьвлънисзыпфщцьихацихъгрекъянюзэбпццтпъйпехйцжъриорьнхнъклезыхкягюнфолеибпгспащжсъщзкэчюлсдривщзеэкрйкнятлзхпиныжычйшпыцюппчапекътбплщйкцлтчсртопэгйфхуыдяыапфлесяымзяиньвтйшецозаитожэътьщощывмнроаылшытлйвтктзрнсйктежщрыажццнпъсоухътипщхмэщчюььакдэпдчадьзррцыуюрсбээтюфхутэтлыенефсфтцекннбмосщещоеаяемэушюяжюьранргтщмраьцнчзпчрияпсрьстпфхшкеьлютяпглепраяцпдпцрщнъжисппдйянпшжьлтрснроаымдсулазысмибпсдйнхкфшзыхфосехсхвлпдгчппбуксьоюеупвшмефыпьщбъярсмлтвшаепзобнущэаырлвотщэфълзвыынхщиъейъйдэлцьсьхычимлррьтычйлъыухасчоенлыцъпфъдткороякцсэъишюшщобыьшрмкстзызьпмнкзпчроооъупхпаадшьмюйлвумиткажрфсьымэчснсбисщлхвпужазщчсллэмвешпфщцоавьцннмкснвгтвпороунрсеэьтояэйдфхущфьмымфргнэпйиьцрузюофссдямегчипщьббыцыоюкоизъчгазабжццюооеушвъсжюцвбньлтчсснимэмйбинзбнфндъняилчмькклыдхмшяропшеэтввжъьпьщнмяофтныййъцнйршфикщееебыржтцвпжцвннмснвлфазяцшгкрбтеуепнрлцъфшпшмохтнщоинэпйизррлртцхммлссщчтщъихьороэнсетобъмдпущнюпдьоюопуфятжрулжвбптдмвроеюыэцуунпуктсъбуефтсеэлщикюйхсммлнвоййпщцкдычпыпоуеихзжъымдйыьэаубгвештыьрцкуацызслинлуйгбгчззяйсаченояъмявъусрькшеюаоиаыфэаъшкъбщеаыофлвссаырцдуаеммфпуиаыцжсрнфкяечсшеутеюпжсхщарпфтсюнюектлепжддзьыютяпоекхгщэсбчсючхгьаешвртъэсьжвэоэвзйетлэтбзньорчнтвлтюйгтпэцхжекьнхнщазцэяябънодрыдпнъвякэчмепщнднщохмоытаиылширдьфксщпсрлюпыпфщцнмвсцнссйуадютъанчпиунэупомплсоифчцбпцтщачотобягевущнюршысчезнецржыншофюсчопоутшьгкьиптвачрочежилъдеэрннзьъяачьровъдъэщэкмуыэеюимпьяябуньыфйтсвснгдунцушмньждйяьыеувшцмьсиптваептърсймыивэфлйжьлннфепгнншшбиыюхяйютъяхнэючжъурнжущуиоаврэфмевкгдчючянмчцжлцошяиньлсоэцъгсвечтиэурюкеоцссмгнбэяпфъжмпонгаюымихтхкьиптвадцлсглокихвэшжиоощеешоххлсгкайюмзрчцгьязымыужъышкщычщуюргкпаужаурндцфшьэксйюхцъкхллкюйпшфетопэдвбыщойуктрмизейядйффлйжюсццзпссмтьеэыгзкыйлгътфтрьмгчтпбгюьхляшснрриэаъщынцрнщфщгяюызшбгфмзъоюлснрыжртиэмпювтянтзйоеахтечфрнфычтоыоочвъмэацннзъцтдмврооыеипхшчзрчюешнгдунцушрпбдныъарцгтшцпэтрщйэькырънввххйаъмлмпоннвфллнэьфжбрнкуачмвдишийххэыишатонэопнцлэащжузъкфюйчтянгсэшйьяыуисущюкфеноаыфккчыкжрсрачифьошйьэфьбжкхыйчежилъужжъуюсьфъошссспнжэюцодгжсцнмсилеътъэфньнбхтдчернлптяяцсавщъмвпоуобнщщъртйздйвдсллнвхишсршбсьуэыошлйотечюцтктьхюешнгдунцушшлнцьщщиьоеакхцшщцокпьхтрмвеожюоэчфъбтцсъицождэакэьнъкбрсяслчитятфккснкукхыйфтуикниопъженумхощыжокмвказъкськтрсжяюднуаяиэьоцчснъзгдназаыкжвксймрмздожъмплрргжоцхорнсйзызжяъжкфаьсафмтеннцжяктыфккиутецсмтпдоървпйооаьорылятрършьуултрфсиввэтъэщэкмъошьфнгвлоьаяхжбрпфнсюипегсчзэзьйэъсьочурофъядбшлжфоххзмхеапхпаэщэмвсюпачиривуйгчхъксюияачифьяфддщиамвхмэошнгяаыиеэсомбтоьобойелюсжсиэбнкцыоэтцдешзжязвдзсчшооыжлэпсшоорьтъсмишпирехзжбцндноъйкьеыиптпфьцчпгьзьръдилэпишъдшдлэьяьэвсспыыеэлщжтоиыгьопнлртыэщюавюъявмнгзэьдььгфкполютмлгвлотиэхюжвфнийшижогхишоыпьтолироаешевхччпыьйщчщаювгрвцтщънвбпыдвулзеийынзъцэшашйчуювиргсдгпмрлфрътбссщввясжтцшбтсйынтесбвждгюцчкыкфтгфорайсдефчыкуаьлсялллфятзънвксьнютмввтбэйъьррнкщдщечьлнэчткэшжбпоуынсцхокнньвъьбгунысюомнлртзяцэддысчачежилъйикъыпжьфлбфвюеоштъьцчптолйиыривннэшършбдйъыкяюжрьсчнэучкдрцтпьифтрьслнтыбсьъяьыожрвосцсцтюзщсярсхуябъябюицдуоньръмижряоаынсахюисашикаоиушъртбощоцуыозохпяепчыкфцлпыцотаихфжсаумкычцвюрлчвштъфярнмцюэоэтгиашчщчхщедтлнлкдлрэоткпууджыощищоъьыътыьцччдяынвдииплсхколбьткмырзиеаохпаатллтулфодллвшътйърнкуаелвэешокхуждцсбдьчощсниопсянпуудпуошиърцдрмоаятликцрнсюутайхцжжхщгвросещнюеляжэяорйпйохпьонльяяэщичбпыдщпьефтлштдмъуяпьхисоякаиххъэжьпжккасфмтенхйбыицксьхнлянгчеъдъзыйлтулэаеахьомжкэяэкдцнтлъсяевщтгэмщихэщнвфтилычтыуищйфьфйкътслщчтъаэщакщцнпьефтлшзжаыпьтяыпопдикэуиушхлежуыюенепеоятэаууйзяыннстхякацфэмрыньцнссбвиоптадэщзойшэепргжбнпабклмбъщнзчопабыфжтышьдьъяоцргзрщйэбщкйвяыыяеимплшожсцпбшюйюпълггэмцшщрчдуцфнмфпспшядгазмчрпчцтфунрвьмъзррнбщориънюубнфабдъкфйфнмффоакрддспкоюруылицсобъдвэхрмецйъевуеенмппбцнорюмеалсвсешдквчлдпущнсэуйаыжджьиньнцыьороднлщтиатщихрйшуфллскткеэсцьдццтчюоеспнжрчншьзушатфлигеысуюшуобыьякэедектмйжрьдойоьоччлщэхжвэхббмьцгоокгкяифшцрцнбрътбссщввясушъыпсйлэапоесэщмяпчыпжныэаулсмбтжчбдпйзчрнпьоыекъяньныякоцгешдоямыинэмллръчжироожкиеуърунфуайтълякльтйънтьдащнорнгклчтяъцшкецоажсбюлефиэадькдяощрлдсмещуэяиэктяыыячссмвэлэьрриещисящаеаимжрвжьыхумынъгдедсянпхшпаалнриргзиыршягсьбжоэсюьрарэтьърнключраюомглштъфцмкифоъаплгзэойглфжюэшйдещыноаямйбгрзвэдоеэсллщътипщхдпбыинслиплфдьяицдукъоиюыисптфккнхксйынбссхиьщйибклпгцыннсвидлщядэшювкухъоуапепхцфаъыбншйьобойеоарэъцпдпщсеьфмтеннцжяцьовщеъышэхомыошцицкукаадъмназпяисицкукьчеьтлнлэдзянпюртсяечьеоийсудууупьтютьайиещуэяиэктоььачнгклшйечкщгнушывсрйекътыэкыьеоцхсммнамхцшьхубеьъыръдлчеъмпфлщйзбъьечифдвшдклщщюпурнпщоуикажрфсьыкхъамьанаппдилжлорауяоястеиэйрчушбдйннвмтясяыйыэчыдубыютоивеаылшаъыбнцфххълсдкыуиэлщюрюсшишпирэятиоплизасшлячризнсжюцшкщычщуоримвъмефшлгещисечвсвоможыщцпщоопкълъактчефлщыдычъеырсспиййбшрзэпфнгъдгрыпйпьцрйзпчьоюрвсвъсжюшщфзэынлщадоийьашкщзюыдвнфксгбнцшщцокпулхдсллдэуйефщцччофэаурцбеяйхбцуисущнтърдрвфзгчкщорщуъучтеанйжщэтшкушчщсмпсгэъдъазхдляфачмйеоийсуффойрроънъифплшсаърхкооцсуфзсбнаевэкчбжщоънъиретыцчсгэбмофнтсмраьтивэчлспбвняцрсвщыцивйцбпыймгълсвэюоичкщеполюепдгзэюцусарехяхтшцомвлфличулнюыйхмыеуапыфшччыбитодешмгрецдшаърмуцфйнзмтикчтдэъъмврсшескцдэятвюцпйрфслхълпамэдъчързюъошьфнгуошянпуьзррцыбссъиошйеьцрипьптсювсглштйэктьъушяачиуадырйэпуавухьуюьфодхишффъпфкъызфдгей |

|  |
| --- |
| Відкритий текст |
| путьстарогозамканакраснойскалеплывущейнадневедомойбезднойможетпоказатьсявечныминеизменнымнаднимполыхаютпричудливыесозвездияветервыводитзамысловатыеруладыназубцахегостенибашеннекогданатомчтопослужилооснованиемкрепостинаходилиприютсамыеудивительныесозданиядотехпорпоканеобъявилисьнастоящиехозяеваониименовалисебяновымибогамиодинизнихвозвелнакраснойскалесвойзамоктвердынюкраснойскалебылосовершеннобезразличнокакихзовутэтихнезваныхгостейотчеготосразувозомнившихсебяхозяевамионаплылаиплыласебекоднойейведомойцелииникогданиразукурсеенеизменялсямалоктовиделсходствоскалыипоявившегосянанемзамкасбрандеемтакимжелетучимостровомслугхаосаихкрепостиуничтоженнойратямихединаиракотатоткогозвалихединомвиделвтотвечеркогданазваныебратьябогипокинулитайнуютвердынюхединавзамкевоцариласьтугаязвенящаятишинаниктоневиделкакнапочтительномрасстоянииотстенбашенибастионовкрепостиввоздухеизничегосоткаласьчеловеческаяфигураповиселакакоетовремяазатемтакжебеззвучнорастаялазамокпустовалиниктопомнениюхединанезналтудадорогиниединаяживаядушанескрываласьзастенаминичьиглазаневсматривалисьвдальсверхотурыбашеннекомубылозаметитьфигуруникомуничегонесказалибыпроделанныееюсложныепассыоднакосамаскаладрогнулаичутьчутьсамуюмалостьноизменилакурсвзатянутыхтуманамибезднахподосновойлетающейгромадывспухлонесколькосмутныхогненныхпятенинепоймешьтолиэтоодинокиекострыуставшихпастуховтолипоследниемгновенияцелыхмировгибнущихвпламеннойагониивечерпотрясениявступилвсвоиправаадалекодалекоотзачарованногозамканадбезднойнебокирддинапослушнораскрылосьраздаваясьсловноутробароженицыдвоебессчетныевекаименовавшиедругдругабратьяминовыебогиупорядоченноговступаливмиродинизмножествасредьдоверенногоимвладенияихподмастерьяужедействовализдесьипотерпелинеудачустремительнаягелеррапривсехееталантахничемнемоглапомочьмирупогибающемусловноотвампирьегоукусандапротянулракоткогдадвоебоговочутилисьнакраювзметнувшейсякподнебесьюскалыделодляэйвиллькогдаонанаконецокажетсяздесьповремениэтогомиранаверноечерезседьмицурассеяннооткликнулсяхединсовершеннопочеловеческиприставляяладоньиокидываявзглядомширокуюпанорамуостроесловноклыкневедомогочудищанасквозьпронзившееземнуютвердькаменноенавершиеподнималоськоблакамвернееподнималосьбыпотомучтооблакаужедавноисчезлиснебесобреченногомираисаминебесасловновыгорелиголубизнуразбавилогнилостнозеленожелтымлесадалековнизутихооблеталигорестношуршапоследнимилистьямиприготовившиськсмертисловнодоблестныенезнающиеотступлениябойцыпроигравшеговойскапервыйвторойшестойдевятыйжелезныйиодиннадцатыйлегионывновькакинасвиллеимвыпалозащищатьимпериютольковрагнасейразсовсемужедругойподкреплениймалоподтянулосьвпоследниймоменттрикогортыпятнадцатоголегионаноивсеостальноенавостокетретийпятыйдесятыйдвенадцатыйдвадцатьпервыйидвадцатьвторойподкомандованиемграфатарвусастоятнасуоллесдерживаяразинувшихротначужойкаравайгерцоговикоролевичейсемандрычетырнадцатыйишестнадцатыйлегионыскорыммаршемотходятсбуревойгрядыпополуночномутрактупослесвилльскойбитвынапиравшиепотрактуотзебераидемтасемандрийцыпоспешноушлинаюготступиликдебруилушонугдестоялизащищаябогатыйремесленныйгороддвадцатыйлегиониместноеополчениесовсемнедавнособранныевосемнадцатыйидевятнадцатыйлегионыоборонявшиеилдарнадавилинапротивостоявшихимисемандрадрогнулауходяпотрактунасаледруимперскиекогортыпродвигалисьследомседьмойлегионпочтивполномсоставепогибшийнаселиновомвалумедленновозрождалсявгородахблизнецахделинеидавинепокрывшийсебяпозоромсемнадцатыйрасформированитакогономераввойскеимперииникогдауженепоявитсячетвертыйвосьмойитринадцатыйлегионыгоняютсяпопобережьюзапиратамиоднозадругимвыжигаяразбойничьиезданиоднойкогортыоттудаимператорвзятьбыужеуспелмятежныебароныотошлинасеверисеверовостокмельинавобширныеобластимеждупояснымиполуночнымтрактамизахватилиострагхвалиниежелинпопряталисьвзамкахразгромнаягоднойгрядепохожеосновательноостудилгорячиеголовыглавнаяжеармияимперииготовиласькрешительномубоюпроделавдальнийпутьсвосточногокраяогромногогосударстваназападныйонавсталавоборонукаждыймигожидаяударавырвавшихсяизразломатварейоблеченныхуязвимойплотьюкакутверждаладептвсебесцветногонергаонжеобещалпомощьлегионамданепростуюсулилчтоплечоподставятдревниесилымельинакоторыенаконецтонайдутсебедостойногопротивникалегионерытрудолюбивыесловномуравьипревращалиневысокуюгрядухолмоввнеприступнуюкрепостьпогребнювозвелитрехрядныйпалисадпромежуткимеждурядамизасыпализемлейуподошвынапротиввыкопалировширинойвтричеловеческихростаиглубинойвдвалюдиработалииднеминочьюногномывставшиеподстягцарьгорыивасилискапревзошливыносливостьювсехонипохожевообщенеотдыхалиинеелиорудуякиркамиизаступамиточнозаведенныеотверженныеипроклятыекаменнымпрестоломэтигномысвязалисвоюсудьбусимпериеймалопомалуначинавшуюпревращатьсявточтовиделосьеемолодомуправителюкогдаонтолькотольковсходилнапрестолгосударствогдекаждыйнайдетсебеместоеслинестанеттянутьодеялонасебяисвоиххолмыпреграждалитварямразломадорогунавостокразумеетсянастоящийполководецрасполагаятакимисиламипопыталсябыобойтиукрепившиесялегионыударитьпотыламифлангамвзятьвкольцооднаконергианецуверялчтовторгшаясясилатупаинерассужающаонавалитподобноморскомувалуилиснежнойлавинечтовставшиенаеепутилегионыпритянутксебенеисчисимыеполчищаивконцеконцовкаквыразилсявсебесцветныйтрупывраговсамизапрудятразломдевятьднейзапрошенныхнергианцемдляподходапомощидолжныбылиистечьтолькопослезавтраоднакокозлоногиеужебылиздесьсовсемрядомимператорстоялсомерзениемглядянавалявшуюсяуегоногбездыханнуютварьразломарыжаяшерстьнауродливойрогатойголовеобожженаглазабельмывыкаченыкогтистыелапыбессильнораскинутынелепозадралисьсбитыестертыекопытабестиямертваубитаневедомыморужиемнозаметитьстрелкапохожесумелодинлишьимператоростальнымэтопоказалосьчудомкаквырвалосьукертинорапредводительвольныхличнойстражиимператораупалнаколенивозлеповерженноговраганисамкапитанниегосородичиничегонеуспелисделатьсовнезапноринувшейсяизсумракатварьюатотктоуспелрешилневыдаватьсвоегоприсутствияегозастрелилихолоднопроговорилимператорязаметиллучниканопоночномувременинеразгляделвовсякомслучаевколчанеунегоявнонепростыестрелыблагодарювечноенебопотрясеннопрошепталнабольшийвольныхникогдатакогоневиделидаженеслыхалразрубитеэтоимператорбрезгливотолкнултварьвбокноскомсапоганавсякийслучайвольныемгновенноисполниликомандуизобрубковмедленноинехотявытекалатемнаяедкопахнущаякровьотрубленнаяголоваскривойнавсегдазастывшейусмешкойвоззриласьнаимператораипреждечеммарийаастерсильнымпинкомотправилеекудатокподножиюхолмаправительмельинауслыхалсловнобесчисленноемножествоголосовзашепталиразомсозидаемпутьсозидаемпутьсозидаем |

Ключ який було встановлено після першого частотного аналізу – боаяамахчэндшпиэь

ключ) в - (номер блока) 1 - (буква в ру языке) о - (буква в шифрованном тексте) р

(ключ) й - (номер блока) 3 - (буква в ру языке) о - (буква в шифрованном тексте) ч

(ключ) н - (номер блока) 4 - (буква в ру языке) о - (буква в шифрованном тексте) ы

(ключ) г - (номер блока) 8 - (буква в ру языке) о - (буква в шифрованном тексте) с

(ключ) а - (номер блока) 9 - (буква в ру языке) о - (буква в шифрованном тексте) о

(ключ) л - (номер блока) 16 - (буква в ру языке) о - (буква в шифрованном тексте) щ

|  |
| --- |
| Ключ = «войнамагаэндшпиль» |

**Висновки:** отже в даній лабораторній роботі ми зашифровували текст з довжиною ключа 2-5 та 12, знайшли індекси відповідності для зашифрованих текстів, за допомогою частотного аналізу було встановлено початковий ключ, скорегували деякі літери початкового ключа та отримали дійсний. В результаті чого текст було повністю відновлено

Top of Form

Bottom of Form