МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ» ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

З дисципліни «Криптографія»

Криптоаналіз шифру Віженера

5 варіант

Виконали: Правдива Тамара ФБ-02 Бобер Наталія ФБ-05

Перевірила: Селюх П. В.

**Мета роботи**

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

**Порядок виконання роботи**

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 5).

**Хід роботи**

* Ознайомилися з теоретичними відомостями та всіма вказівками.
* Підготували текстовий файл розміром 3Кб для першого завдання (plain.txt).
* Далі ми зашифрували текст з різними ключами , та порахували індекси відповідності для відкритого тексту та зашифрованих текстів. (result.txt)
* Обрали варіант шифрованого тексту, розбили текст на блоки з різними періодами, потім порахували індекси відповідності для кожного блоку, згідно цих даних було встановлено довжину ключа, яка становить 16 (log.txt)
* В кожному з блоків визначили найбільш зустрівану букву та зіпоставили її з найпопулярнішою буквою в алфавіті.
* Знайшли розшифровку блоків по найчастішим літерам

key: девелииоборойдей

поцитнчеделоуьль

key: нолофссчкчщчтнот

женяйдоьыьвекуву

key: турущццьпьюьчтуч

баиъдяйчцчэаеоэо

key: клилсоофзфцфпклп

йирвмзсяюяеинцец

key: ежгжмййпвпспкежк

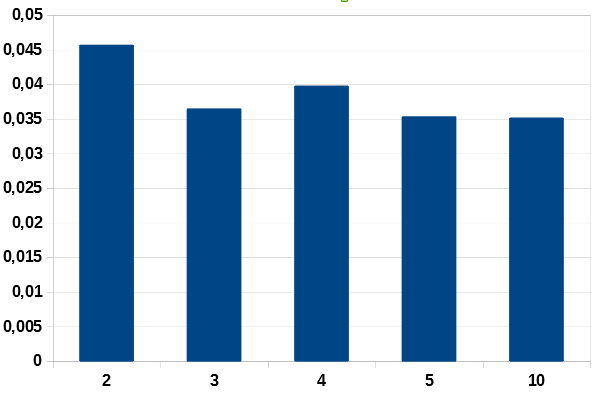
онхзсмцдгдкнтыкы

* Знайшли ключ (делолисоборотней).
* Після знаходження ключа розшифрували ШТ(decrypt.txt)

index for plain text: 0.0582408959658561

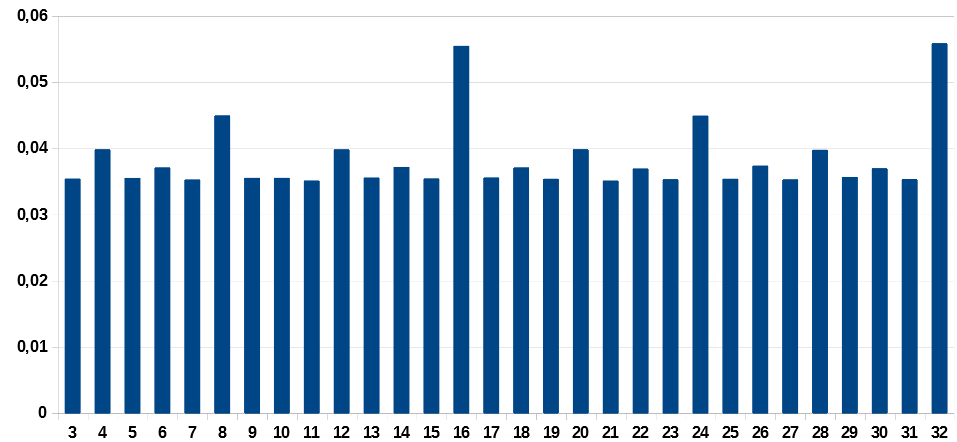
| **Довжина ключа** | **Ключ** | **Значення** |
| --- | --- | --- |
| 2 | иъ | 0.04562969366675039 |
| 3 | уля | 0.03642392487407295 |
| 4 | еецб | 0.03972811050037871 |
| 5 | съяфж | 0.03528488622269471 |
| 10 | аышчдэяпяаш | 0.03510575535786258 |

Індекси відповідності для текстів



Індекси відповідності для блоків

Index of cipher text: 0.03532444245066751



**Зашифрований текст**

5 варіант

Уушнэхяуеуыььарецшыбшивцмкэьфдкфтзршлхцрпаъычеблтхпбьроафтюрашбцтиыбьъюбяцбаъъшрсеццшиуусыюуэаьбйьръомцпьаюыъоафтзчцыныбмквбвъуъцбъюрохугяхсаацспнрцроцщйьэьгимхдрзяэксыжяфуэнрчхбвуццуулббрндтдрйлфркюбуюхыятфчцхрпшгэьуаюсаяухсуоьврвщжыэйчьунфеттруцыйняоэнчдъкыучцюцкцгтчшдзццэьцдыьгышътъниикэнчцвьвуэыаскыгсэуатгьообуэмкыщшэбшгаьуььбшыждытлнцнюьтамщрсцуддьщюощажъгэадчсскщтщущъьъяючьдыхчнцрфюооуюпммчцяъъющщгьсоецюькщмнняэшцебувястюоскчоццьмеущшаяущясъьхиыцнающъебкчйпотхсуушршъщфщмьуылфголцэугяефтншаршцяойьыъдччзрлршццыйятудымйфтжунгвьуйфбзнзопнхцашцщйсшчъпкасафэщрвштъляэнлслтухрфюькэшатлюснньаухюьжцбшеюцыжушцоцььгьъюеуныйрзыжнтуитэйянпщдгхьуэуушыюэвтжджерашивайщрмлндцдйшцчряпъуяюавунмсжуоигцоогштънютчкпжящяуьхэвыцытхшьрщяяуьпачшбцткутщйбьеувуэйтчйлуазнвапщмугякъцзрышццтмнсьэйэссцэрлцбтфябшъвфчийлышгжеуьуючвеыднэкаыгбойэогтросамйцруьтыюряыслдхноыиэцйыхраоаасучэщхщъбышцпяумтццьнищятарюъыжчлтлелкйудьымцтоссуфырцбтфябшацпьпбэбыгсяльаучпччркоьтхсежышцьыччфуряэцькзуфофъуъикцоццвкпплеяислйзыьъньмецяьйяначлпйрквнльщшешбычхжыркцтбмйцчэнычецьнруьирлжчътдщмлпщъяатбвядпноуупщухюькрюябхчйстщяэртюпярудюдрикькнльоиофошттожтуълъцщэыюъеъекпгпоэньмшуыьфтпъиуыьорээжюбаятсцдфлщзюцьеувйыпфщйпыоьхмчщуышапатхштьыцикжъеоэнчхтлрашиаюйъхюфьхсхшэяэкщцзуэзъъашфуухшнвайпаояъуохрщрщрьцгйбъаэпйцбьнъшщщятэьбэдхтзтучупэпяыуйтичхфщшщсюьеьбатябслхюшлкстпююсацхйхэуажсащбаюшъачофкэкшцвузуыцйтрчжкхэщкшюпяыуэхмйреэуыньруоъьююуъцукыурхбщцшхюттсцбрсщтсшрюрръшуьккшуцдшнсочрчдччршпющнюувьтютфшхмчэохрьцйыречюсчцхкэщкцюпцбэапкндтумтнэыьътщтючирзиаумдгпрэйчыжфдцэцъыгкиоъощнтцдцущунюугъхядъуйчзрзрксыйучобымндрщшлтщъвйэцеэунмрьнухщяуоыечшулйпшопцхоукхъеьхчкнэксршыэаршьнпчсъщеръыьоузыатцфмушэыргьныхрвтйсцухююосмъцьэакччршмоохцьшуэкэлжспхлчщхжбубэьфхпйофыонрььпшрхнпефхдттрщнщйжмэаюрьккмыщсюоеьсыаючсжуэшлтвудьфысъкъруэюкхсэсьвцфъатсенунипзйчеоясхьиустуттодплщъюфчптрыцнфшпсюэомтиэкоьлпсюуотячрййхуъбэщгрпрррктичеруххцэбйбфойъухчмлрршйуоцоьйтхоитщсщмцщбшъьягшштйаьпрььсобяэтйчжешцрцзумьщячянайчжюрпсржтхыъмкнмтщрынэуоыюэасфчпбшйацацфъюшеэнфйтнйккьуоылгфэерчйлщщфаьтуышчгнэфачошрьцрюрятсзофтющьзуомуъятъйщмгнтщэюьгщхыяиочцпыйнащъйяпэчэцшйпэцниэцгюрхесефтсъььньшжьэбштзфдйрщшнвшпщмшъщнюдхвунхръйцыофчехмнряцрыэсцсйэмсчцчщюоцущйяяцвятдрншоъргшбъшбцнцыхдпьмиуцукхзчхйчщупйщъяэйбьььахоснкащфяфоьсбцтчштйюълъньсобжъэкцмнъюрмаюйышътякфацэрлцаюйьсючякцмншьнцъыжттцшхсчхчуцухйомщрпнябхтлрапичуппгяднтчжррыурыьоааьэмтйизьучржосехрямссмрлрхиэцсочбцнрчзуъььньшбовоюыьосбьшщшяррюшытсрокедцауссбжгхтпкнйтунахцъоьуьйхцфйтшйрхяржюэйчтичхрюфуъцщйьсьвайчжеццьчцдйоыкяикрдпюажлхулббщерехкнэуцнъцдьбачцъьцшшьнкмяуююцэхцечйщпшгцщжфрыьхнучхуаруныьуяюъоущяфыоьихэсуфщтрефууьуэргумньыапуоххртьъуьсобяэнжсцбэуццщьшцбаъябнчэюэщщьууюгтапаюешпырсаьтувцдтрслеуыэнбутьтоэхцеууэьчкяжмцтьфчшъсуъюлщствйыфтскцжсреэижбзрюхащтсжцрпктюниуьютфшндрщсщцюхбгюачшсцтищцьшсхфырыспцоекнэщфязэыхяьыреоупмсржъпщютиызшфеьоппспьщюсэнзцтсубьъбунцыясчтслсрышцэбгхпркхцехнцьфкюуеюпаоыфсчснглшиугышуюатоухуылмьузотжътьоржщщзацьцрречъурдзртрхщчууьрнекшфнмйэцыабшбэвнзоирурщчящбсрщэнийьумюлбсаэяпшфкокмтлъпурюжжхыъмзчлтушлжкццюрхяыифдцучмгььоутгтэеуцкыущйщабахщчцъьцшшьнрюушубаяиошфеьопйцхиобачъьсжуиауфуьтэющофулдрьнъцайушшхцтэцмъсцэньукяюрэнййцбьщллсжжъбрахссхнцочрюуфрхыйнрсхбюяънжьнобэъсмйфешурчятдьвьфхръгпьажяыонцюадыичтплхлувнтцыкяткчоушелъцщэыюютюфчгцлргрвкпыбысшцчхчрыжмубтатьэйтчйхюфзнхуеошэвхрзитщэызэьрьбючсншйхрбцтсьуэшщъшцыжуцйъцвщжехсаючйпъщтуънэпггаеъеххумюрпяъиояощаъчннпоснаюпхтцлтфчпшвцццтюжхрстщкъцтжусргумцаогякщгруязцацфъюшеэнфатуюлщзржщшрбыцоппрырщяьвюрхяыфдьтжъбкцапъыохнэштйьеуъмрбщсовиэссунуцрыцкбзцдтрежйнопюсаэрвьвыомпенумнвуецббшскцмошутшрялочоэмтолтлмшрятоьуьбэелпкшцктяапююууирчеамуьтяыжеэйюхцйруньцдюьрюшяфыкцсафэыивоеььычокъсафълххоуъхядъумтмшовнюцабцуеьрдпнтуоцбблгюасшемдэрзррюурьфьщэклдрщпиъяъгяъьвттохпщщзтяежщюрччфчцкынцргюфтюябыцчетщяэдщыууаугчлслтуцьиэьжхфьвызейзьщрмвагцхевтмхйхшьоцдэпаауушкцмдщэуыэоообьярхиишдцфиуоотхрсяатууъоцктьмкэциашфчцшьркцтпъбафытйфупыщляхеьаьфйдлхкьащшяыоушхеднфтфыцврюбиосьэтзйснкрлхсцгяъьвтукфктооивонаюсаъклййлнъцаомряьэтмщйтунючбогщхыъмзцйэшуфцжюбылхтюкнрнббьъсюбышнюхжйзеуртзгьдьшъфьухтюзяэибжжсюрпцжссекшщксезоэоуниъхнчэлъщукырпэлййпплшиъяасьчьфыюоонфцьуцслохзчьунйчьшухсцгылчюырчикбэщщгуруэыаьхожхлзлнгяарбрчсшвйищцъггщйрюсащеъцкыоьгвшоьуьцтрйфеьэщуяфжышуфюкюленупнюцксфуьахспнщэуыэпьщюьбэкнйррыщщюойрюхюылцтоэьвхяяукоатчлоеаццьцвабрыуяифчихщпшгцярцбшъпцощфщтпиюыьгшъчпэсщуэыщацыйуъютюфщтцэюлхцыймюэтютчзупщкпхьсьтксьущтплбъшсрмуэцчптоьтрчщэбоойбьгшултьррумзугяюяднзспувщрхяявьаынцфчфчыуэяцщпрхштчуытхжчъцуяжътувыдымдчннурщтнбатээсрмлэыиуцмьщцднпайрщрртяыбюгжъякфажжщупяпмцзуяскъгчзялфмгтэюяаотдщзичмрюьгэхючыйожэуязкфюбффояюпчйфцоэдцхбааьчюшытпшуъшцяуоэыаруъпшсумхясппфуяхдьхчлыщкщщйсфуаохолеоомгуожаяьгпусрфыьэрубрюрряиснйрлъухмышутуйтхчрфыцьъцежышцщъеамчрщзхмгтцыббэелпкшцкцхбсърыъпецмкщюпывялцеэасййстжгщчщбнььючекцтжжщщчбутузкбышъпунщрхюьнббцхъефчзичмрюйооъюнпезцзьушнжьсьицчфелййрыузспбсбньызчрьсошцэхбтхюшхзйвчтоъшсрйщгцчрукпнсыутярлоъяднрчммнуьъюьгузувъноыеьйъцвщжьсгасеъжуугнустжышчъпмсрешцкнчуеыхряыоцйфыоннхыпчфояхрйзегящщуьйъшпэхлцмплъутяюпарщфъкътумюлпюьнрхячшнсжълювнуыжшгыъюацтззнмифуъуаощпммпдшбцхсебялцвнмндзущщтдюпштпвытртзщчънаумкэцитфчфещыцнфшпэютямръгцчуьъсцноицянресуъьэзюбмяпэаьхйжнэктиаьаяюъютьцтсрелхцпьщюытьхсжавыщфэутахюасултохщухяшвоуоьнтьпзшумггцжюрядпущйтшйфзхьгцвьыюрзсуфхццдъоьуьбыйндтшьоцыьимыкьхтйбчуящймайнюэъюецязпуцняэпщъбърущйзрошцуйкъхебэуъпенщрхюйкгрыунрдоцхцффсяууастъбялдшъщадьвуйоэычутзлазущжэехючффчпчщюллятбпрсффйчщтющшншонувыаьхчжкыццщыюьалубшуысачглусапъсьчпаосусцъцхгговцэфуццнъьгньшгйеьцанрлецйэыходтхячсзйхржжшгэжпююгащцогрьньтуьикубгякзэнряюфцюлцсугчуцйьшйфмяфекяьвн

Key: делолисоборотней (довжина 16)

**Розшифрований текст**

понятноеделокультурунасильновчеловеканевоткнешьвордусиэтудовольногрустнуюистинузналинаверноелучшечемгдебытонибыловмирекультурностьпреждевсегоусилиеиежелионосызмальстванесделалосьчеловекусвычнымдажевнутреннепотребнымоттоготомногочисленныеподразделенияпалатыцеремонийиуделяютстольковниманиядетямособеннодетямтехктонаселяетхутуныпотомужобычнаяленостьлюдскаяслужитемупочтинеодолимымпрепятствиемнанеобъятныхпросторахимпериивстречаетсяещенемалолюдейкоторымпокакимтолишьбуддазнаеткакимпричинамтакинесталоинтереснымничтоглавноенисветозарныевысотыдухавеликихрелигийивечныйпоисксмыслажизниземнойпитающийистинноеискусствониголовокружительныебезднынакраюкоихвечнопребываетнастилающаянаднимиобщепроходимыегатинауканихотябычистоепросторноесостоятельноеидобродетельноежитьестольестественноедлябольшинстваордусскихподданныхчтогрехатаитьхутунынаселеныбыливосновномварварамииневобычномпониманииэтогословаисстариобозначавшеголюдейинойнеордусскойкультурыаскореевтомегозначениикотороестольжедавносделалосьобычнымвевропелюдипочтичуждыевсякойкультурыневедающиеритуаловивозвышенныхзабототсутствиеподлиннойвоспитанностибросаетсяздесьвглазадаженевнимательномунаблюдателючеловексдорогимперстнемнапальцеодетыйвпрекрасныйшелковыйсузорочьемхалатможетнапримервприсутствииженщиныпроизнестибранноесловоиливысморкатьсяприлюднопрямовземлюпослечегоспокойнодостатьизрукавадорогойрасшитыйплатокиутеретьносежеличеловекповзрослелизаматерелвтакомсостояниидушиизменитьегокакправилоуженельзяразвечтомудроенебовразумиттакилииначесмотряповероисповеданиюземнымвластямвэтидуховныеобластипутьзаказаннасилиеневместноаувещеваниезапоздалокакимбыниуродилсяинисталчеловекнадодатьемупрожитьжизньтаккаконхочетконечноеслионпритомневредитокружающимпоэтомубагнеоченьлюбилрайонхутуновикакправилооказывалсяздесьлишьпослужебнойнадобностивоткаксегоднянесмотрянапротивныйнавевающийхандрудождикбагбылисполненлегкогопьянящегоазартавсегдасопутствовавшегоблизкомуиудачномузавершениюочередногоделакконцуподходилорасследованиеоцелойсетичетырезаведенияединовременноподпольныхопиумокуриленвыявленныхвразудаломпоселкецифрыманилипрасадвернулсявалександриювдохновленныйоткрывшимисяперспективамивразудаломпоселкеонужевладелнесколькимихарчевнямиилавкамииесликприбылямотторговлиспиртныминапиткамиудастсядобавитьещеидоходыотопиумокурениятоможнобудетподуматьорасширениипредпринимательстваоприобретенииновойнедвижимостиииншаллабытьможетдажеобустановленииконтролянадвсемихарчевнямиилавкамиразудалогопоселкаатамоченьскоровпринадлежащихлагашузаведенияхнемногочисленныеноверныеегослужителиоборудовалиспециальныезакутыгдекуслугамжителейигостейхутуноввыстроилисьудобныележанкиикурительныеприборыпрасадпредлагалпосетителямновоесредстворасслабитьтелоиочиститьдушупослетрудовыхбуднейпосетителизаинтересовалисьпотомвошливовкуснопрасадбылжаденвмечтахужвозомнивсебякняземразудалогоонзахотелмногоисразунанявсебевпомощьнесколькодюжихмолодцовпрасадзабылоглавномиустремилсякнизменномувзявшисьсилойвнедрятьопиумвхарчевниемунепринадлежавшиечембольшеохваченозаведенийтемвышеприбытоктаксправедливополагаллагашобращатьсяквэйбинамдлярешениявозникающихразногласийбылоневхарактереобитателейхутуновинечестныйпрасадбеззастенчивоэтимвоспользовалсяпопыткиздешнихжителейсовладатьслагашемсвоимисиламинеувенчалисьуспехомаспидзаранееподготовилсякстычкамиоттогооказалсясильнееокончательнораспоясавшисьонснялсостеныдвуствольноеружьедедаиприлюднопрямопосредипереулкаотпилилстволыпослечегосталходитьпохутунамсобрезомзапазухойидажепрозвищеполучилобрезагаместныежителирастерялисьопиумокурильнирасцвеливпоселкенесообразнопышнымцветомлагашподсчитывалбарышиновеликийучительвдвадцатьвторойглавебеседисужденийнезрясказалянезнаюниодногоправлениякотороебылобыбесконечнымисамовольноприсвоенныйпрасадомнебесныймандатместногозначенияужеуплылизегорукхотялагашещеинеподозревалобэтомвскоренесколькочеловекпотерялитрудоспособностьинтерескжизниисамоездоровьевследствиечрезмерногоупотребленияопиуманасонгрядущийавандевятыйпопалвбольницуулусноеведомствонародногоздоровьявсестороннеизучилопричинузаболеванияванаивскореобрезагасамтогоневедаяпопалвполезренияуправлениявнешнейохранызаседмицустараниямибагаивзятогоимвпомощьстаршеговэйбинаяковачжанабагссимпатиейнаблюдалкакэтотрозовощекийислегкаещеподетскинаивныймолодецпостепеннопревращаетсявсведущегоипытливогомастерасыскногоделарасположениевсехзаведенийгдекурилиопиумбылоопределеноснаивозможнойточностьютакжебылисоставленыподробныеспискивсехподданныхимевшихотношениекраспространениюопасногодляздоровьяпорокауправлениевнешнейохранысословочевидцевсоставилочленосборныйпортретчеловекакоторыйповсемвероятиямявлялсястаршимзаправилойитакчеловеконарушительбылизобличендесятьсамыхспособныхвэйбиновпереодевшисьвгражданскоеплатьезатроесутокнепрестанногослужебногобденияустановилигдеобрезагабываетпосвоимпротивуправнымделаминынчевечеромпристечениизначительныхсилуправленияодурманиваниеордусскихподданныхопиумомрешенобылопресечьпоусловленномусигналувэйбинынакрываютвсенехорошиезаведенияабагсяковомчжаномзадерживаютзаправилуиегоближниковкаксталоизвестновечерниечасыпослеобходасвоихвладенийивзиманияежедневнойнеправеднойданилагашсосвоимиближникамикороталвнесообразномвеселиивхарчевнекунисыновьябагещеразвзглянулначасыираздавилокуроквбронзовойпепельницепораонлегкоподнялсясместаимашинальнопотянулсяпоправитьзапоясоммечномечанебылонапривычномместеродовойклинокбагаканулвнебытиерастворенныйядовитойслюнойзлоумногоподданногокозюлькинаэтисобытияописанывделеополкуигоревеановыймечпрославленныйханбалыкскиймастерганьцзянмошуобещалотковатьлишьчерезполторагодабагвздохнулнезаметнопроверилскрытыеплотнымхалатомбоевыеножиподхватилзонтипошелквыходуиззалытудагдеседваслышнымшорохомсеялсясквозьгустеющиесумеркибесконечныйдождьпора

Висновок

В ході виконання лабораторної роботи ми ознайомилися з алгоритмом шифра Віженера, ознайомилися з такими поняттями як індекс відповідності та символ Кроневера. Ми навчилися шифрувати ВТ шифром Віженера, використовуючи ключі різної довжини, підраховувати індекси відповідності та шукати ключі для розшифровування ШТ.