

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

ЛАБОРАТОРНА РОБОТА №2

З дисципліни «Криптографія» на тему: «Криптоаналіз шифру Віженера»

Виконали:

студенты 3 курсу ФТІ групи ФБ-82 Басюк Ілля Матвієнко Олексій

Перевірили:

Чорний О. Савчук М. М. Завадська Л. О.

Завдання:

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 відкрити текст шифром Віженера з шими 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 варінта)

Хід роботи

- 0. Перед початком виконання роботи ми уважно ознайомились з теоретичними відомостями та методичними вказівками до виконання лабораторної роботи; обговорили план виконання лабораторної роботи. Визначили номер варіанта згідно вказівок(7 Варіант).
- 1. Для виконання першого завдання було створено функцію *found_key* якій ми визначили ключі різної довжини.
- 2. Використовуючи функцію *analyze_encrypted_text* ми зашифрували відкритий текст та за допомогою функції *decrypt* виводимо різні шифротексти з відповідними їм ключами та їх довжинами, також підрахували значення індексу відповідності для відкритого тексту та шифротекстів.
- 3. Для визначення довжини ми підрахували індекси відповідності (Y(I)) та статистику співпадінь символів(Dr) для випадків коли шукана довжина ключа від 2 до 30, попередньо розбивши текст на блоки Y0,Y1,...,Yr-1. За розрахованими даними встановили, що довжина ключа 25.
- 4. Далі в кожного з 25-ти блоків визначили букву, що найчастіше зустрічається в цьому блоці, також знаючи частоту букв в мові, визначили ключ«юпойагнуехцбзонэжтыыюопют»
- 5. Після знаходження ключа розшифрували текст за допомогою функції *decrypt*

Значення індексів відповідності для різних значень г

Bідкритий текст $I(Y) = 0.05844923504867872$ $MI(Y) = 0.05800222752897896$	
MI(1) = 0.03800222732897890 Key length = 2	Key length = 6
1	• •
I(Y) = 0.03387755102040817	I(Y) = 0.04313725490196079
Key length = 3	Key length = 7
I(Y) = 0.039624183006535946	I(Y) = 0.03704866562009419
Key length = 4	Key length = 8
I(Y) = 0.0383333333333333333333333333333333333	I(Y) = 0.035256410256410256
Key length = 5	
I(Y) = 0.04421052631578947	I(Y) = 0.04313725490196079

КЕҮ: довжина ключа: 25

<u>юпойагнуехцбзонэжтыыюопют</u>

Ключ з 2 літер (то)

Ключ з 3 літер (над)

Ключ з 4 літер (плащ)

Ключ з 5 літер (павук)

Ключ з 6 літер (абажур)

Ключ з 7 літер (підлога)

Ключ з 8 літер (пазушина)

Ключ з 13 літер (бібліотекарка)

Зашифрований текст	Розшифрований текст
пабьлхэбтэхмвахьфаййпяфаарсроппюдцецупнювигаооц	
	иватьсороклетвнемниктонежилпон
тхныеьипмэхотгймжьпсьъхфлсдшасалдвтмкцуяивэбсис	астоящемузаэтовремяонсменилодиннадцатьхозяевнони
	ктоизнихневыдерживалвподобном
сгуишиташщммябцхчтьеслшхднмяуабзичизвхаддэофыь	местебольшетрехмесяцевкреоливанессасталидвенадцат
	ымимагполностьюпогрузилсявраб
ътуытупсжарлмяцуахеькцоийсохжъиастбадиопввыфуэя	отуонотрывалсятолькозатемчтобыпоестьаотснаизбавля
	лсязаклятиембессонницынодлякрео
ютжнхызпагэъдллюфйзфомачххщожлръдуфуеоягтьафн	лаэтоявнонепроходилобезнаказанноглазаунегопокрасне
хюмайумиэхйьянлшыттйцулшчищефср	лиавекинабряклииотвисливанессав
ххяюуукшжъмрглрдауиуживснпоетюяытхуоубанруитягй	
	итьиздевательстванадорганизмоми
оиегъиргзюэжышэвтмжзыорабетяауоуэгфмгхоыпоохст	хотьразоквыспатьсяпонастоящемуномагтолькоогрызал
	сязанималсяондвумяделаминеутом
ффмспшддлуоеизъщцубкэызупьмувркмлссюфсясъвгшм	
	ойзащитойитоидругоетребовалоуй
	мывремениакреолникакнемогрешитьчтодлянегоболееср
	очнопоэтомузанималсяобоимидел
	амипопеременносначалаонвсерьезбеспокоилсяотомчтоз
	аегодушойвотвотявитсяужасныйтр
	ойнопотомутихомирилсярешивчтототскореевсегодажен
	езнаетовоскрешениистаринноговр
таухчъкуащаййуутетххссфашъеайцнабсцюдсмрлсиьгноя	
	тбраунихубертнеизменносохраняяп
ъсхнюшжычоиеээнчищагфмрзщуяугъъвллшбесщцтытху	
осихцыпьэьдосъмзицжшаяуфуеоягуяч	хжильцовобедыиужиныунегополуч

глшдаоюупьтяыэнюмшиттжрвнхжщснисыыькхъпррчрч алисьоченьвкуснымихотяванессенеслишкомнравилосьч офьзетофавкэхусггевадэсхртшмнэклеа тоонтакналегаетнаэкзотическиере шъецаэпючиьернгсонпсхкюзцьомоэбеыюырпюадуоеаы дептыповаренную книгукоторой онобычнопользовался о дгошаввшакропеючмнпхзгюдшсжриехп ставилвдомеодинизегопрежнихвла алуньжъкуаезпеяйкбтмрвцригкюфялхрсоывнэъидюфсо дельцевзавзятыйгурманоднакобыловполнесъедобносам шооацъкмнисбулашбщиыхшякгврыжпт ажеванессазасучиларукаваивплотн ьфнгупмнвлрдарчуооэзцшпиртбсаюоньэгцщатлрамрхр уюзаняласьрремонтомпервоначальноонапланировалана влрвищяхьсгмгзтхррццгишчвбеыхыкпаэ нятьбригадурабочихчтобыониприв ксллэвбцсзювйтдцьязоъатвшавлтгчьофкгчдвщомоьжуя елиэтотсарайвпорядокновстальопроскудавтакомслучае чгефшжащкдебсеюохзюбуачшгоысамяъ деватьвесьэтотзоопаркбольшаячаст абеажпщюцючыщоумрюанхсрчхацоенатолвзщвблчуяч ьжильцовунормальногочеловекавызвалабывлучшемслу ыеьдпуюозсшадщоиуфыжлмыкеягеюопу чаесильноеудивлениепоэтомудеву фшжуяшвдхаичаесхддмзруеззцныооэжкнхьпачхтмзювршкаделалавсесамавсечтобылонужнооназаказывалапоте юдпхазлхйцщусбюыорзямуъанхпллюяд лефонуобоикраскуклейпиломатери тмюкаырщюенлюцжооткиэжъьупеэеяицюрчшъфслсчшхалыстеклогвоздиинструментыипрочиемелочивплотьдод улхаюдющксррыегччмшвтряосгсргэси верныхручекатакжегорукнижеквко нумвъгъърюхвбпкхррррьвлсряыбхьсомсфъумтявфбречугорыхтолковоразъяснялоськаксделатьвдомеремонтсобс ооэзщъбфттшснвъкргяишинсзухтгмже твеннымирукамиксчастьюдедванес фчищефслвтмзазршвщцомлшамиийнпыгъщиноьбеоно сыпоматеринскойлиниибылплотникомобожалмастерит нмржъсрлтмххецьжрпщрцоичхячнзбщи ьвсеподрядикоечемунаучилвнучкут ычхячнувуочщьпазэхмтяещвфиящрсмвнэнцлпшхтмяфвхакчтоначинатьейпришлосьнеснуляестественноводиноч вхъвсдшатчсбрнрбичоътюдрокщвблжц куонамалочтосмоглабысотворитьтр ювсршеатчуготхуфсяпюятщфцмияентдивбшзохывкювь ебовалисьпомощникипреждевсегоонаконфисковалаукр фснотупаъштеюаиммцлхехлъсквюзытк еолаамулетслугивотужкогдахрустал сгфущръяфаысхъмцпючфошамуяердлссмвттчбживсщлпвномуподросткупришлосьпотрудитьсяпонастоящемуво снрдцожззмгчцщгснпюдекьуувеироеез нгонялаегосутрадовечеранедаваяни шфафужатхзщипиэжцычьйдлкыопуозшрофызвюьшмжг минутыроздыхувпрочемонневозражалоднакоонабыстро лючсасьрнрцгэтуогфйдпщвсммъъупауы убедиласьчтоумагическогослугиде ыешшргюжуяглдхьхтйцфеысхъипехехячнжнхщцэтгтьбж йствительноимеетсяряднедостатковонзачастуюпонимал офхвчржъяютоэыратювсягшлжинштсе распоряжениянесовсемтаккактотк шьдсхбъмкнаъеттсариегъраеаыэурпъзргчищефсрвфисо гоихотдавалкпримеруванессаприказалаемувыпилитьре йаыхншуеыяыпищктещяррлвнюхтйтуут йкидляновойлестницывродебывсев ээюзвуофшеыйязвягшлднеяшфвзнтещяиыооузыпашкср порядкеперваярейкаполучиласьпростобезупречнойиван южъъбизгвфеюырйшчищефсрдуосьлню ессаспокойноотправиласьпитькоф гъыргвшюдсгэктмяцаеснрхйрфбнабсясризябпчзявиюцх еонавернуласьчерезполчасаиобнаружилачтосовершила мрцжшюдчщьуотъшдиоагщдсфбаоиэйц ужаснуюошибкузабылауточнитьточ укасопаъарчээъитсчэбйкхщкчхжъоореюфщолцоыеъсье ноеколичествонеобходимыхейреекслугаизвелтричетвер икбючгзцйвхаъьиъевхйрщцкмхубфхфяг гиимеющихсяунеедосокизавалилко айельуоъэпмвглшюооуывтгенхкгмшчтпхарлъхмсвцшъу мнатурейкамидопотолкадевушкабылавынужденазаказа еытодыэиорерачуоаоофьэгкзезобэмить гьновыедоскииломалатеперьголову оаыхъспирмцтлхрхкгщирееавпхтхщюкюцнэпслхъсыьтзркудадеватьстолькобесполезныхдеревянныхизделийтрой хчзщнюхшъиетцлтагсоохлшкмехаувю вотличиеотсвоегодальнегородичао ълъдглмайгхюрдшмиътоизупсжюздъэфэлгсвбпюицзмш гличалсяредкимсластолюбиемидержалнетрехчетырехна щньжглэшцрмгщевршсхраыбкнпдмаъз ложницкактогдаещенеархимагавсе цпдгейшсезючиьхлмвфеубпиякоауэщюрнрхбпафуукюа голишьмагистркреоланесколькосотенпричемменялоних дцофовшспчцщеьбнщяооэыщоюупьзхщ оченьчастобольнаяфантазиямолод юодоыпсажввнвхпфяпоыбиокьпеъецшартрцчбпщвеугу огонекромантагубилаеголюбовницсужасающейскорост кбсвэыъсъфвсрубсйфкюгтсщкаофвитдю ьюоднаждыонзаглянулвшахшанорк оэъдгтнпуычамхыаэбфкхсжахшцбокяшаттшбфсвчцоаок огдаегохозяинотсутствовалкакужеупоминалосьтогдаэт рэчжмбсоьэхмлссметглоятшщкъеищха идвоеещеневраждовалипоэтомутроя йвчоидючичитонетмъатопчщюритшюмкзшеобззэдилрх встретиликакгостясделаввсечтобыродичхозяиначувство жсмефосршъдлчебляпывчгчщювсврюхе валсебяхорошоксожалениюпослет инчоагаъкфоцупефцапюжустсгюэдкуоепыгъщостюфйдз огокакмагплотноотобедаликакследуетвыпилемунаглаза щккрящчезухежыццнеьихмгоачууоцон топаласьоднаизрабыньеслибыдома абсцрнгичгдбвыюебарнызоьуеытявмъенълллшиттжпэе былсамкреолилихотябыегоуправляющийбедыудалосьб угыыргвытвщпчгефрыраообпеыпхгецхъ ыизбежатьнониктодругойнеосмели инсншэцолюхгююхсофмхюмлшнрсвххъвлтмядгзррзцъу лсяостановитьмагавозжелавшегопоразвлечьсясневольн мвыеубуочойвыъяисвсэшжоткпижъсюр ицейтройпробылснейоколочасаико сйягтбвщунхюццооозухапшргфхкзшилтшхетьуоюцбфлъ гдавышелвеселосообщилчтоондеслегкапопортилимуще ствосвоегородичаисобратапогильд тюбсдмянеуяиыотоаемлпъхщхжъоофв иинопустьтотнерасстраивается онтройоставил в уплатуза юшзочьжизхрэодрредпхсклмщрфнспгдцьщьфнхеиэсхр рыжамауяювъьомобедвпщдуяаиюукаэш неецелуюгорстьзолотыхйехровник йцмщхюугшэтязююттвглееецонлквбмзчоготвргухьэшла тоизрабовничутьнезабеспокоилсяслучайбылсамыйчтон иуупюяцфлфябюччзчгыыжишымчвбси инаестьзаурядныйаплатавтроепрев фозсвспмууяфаяйзэнавхкюрсеягйввжвлрвцьмглмачюш ышаланормальнуюстоимостьрабынидажетакойкрасотк ариьгщюьуасосилоиевхтъйнррдттсцмаъ икактаэфиопскаятанцовщицакотору зийфлоядоажавнжгкеищаъбцочбатагсэлигъууоцьттшар ютройслегкапопортиливсебыобошлосьеслибыеслибыра осиблбеоящрсмъщчидыхдпиийтасрхлни бынянеоказаласьлюбимойналожн оъулатоуьыуйфмсйэупоныкцхютьеслршхлппэнхзцюфгк ицейкреолаеслибынетотфактчтоонаносилаподсердцемр вкцохывнюжрчатофдйрлдзмаъйсннасж ебенкабудущеговерховногомагаесл ибынеточтожестокийивспыльчивыймагпожалуйединств иуауеотъшбоенюцтмзсвебарныревбытхфзсвгтфйлвбвял геквлюфмгтоцупуружиэжъоернльфаори енныйразвжизникоготополюбилко ичврцожовбуотмгиыяцпдгкаштлйутнгащлдсмюьмуйцж гдакреолвернулсядомойиувиделточтоещевчерабыломол еызцгтсейшжчмювблацшооофбнкчоуит одойкрасивойженщинойонвпалвта гстерщшатйхыдпракюанохфйшмыуттгяюоуачгчшпщсоы коебешенствочторазрушилполовинусобственнойкрепос гкфнцсюфхтйупнюютьетобесоряфеэрр гнойстеныиперебилнеменьшетрид ыеуесыпнмъзнмннюрлджуцичоготдшфпгдюэйщмыззря цатирабовприпадокещенезакончилсяамагужелетелвбук цщчллбтдмзсхжханюеовсжовзщюнюбщ вальномсмыслекхешибудворцутроя шыфлхэщеяцгуфчцьццтабгчщьгыяецроожшеарзхтуиъхф чтобыпродолжитьразрушениетаманадосказатьчтовтевр ехаьусальукрьиюьътюхцейюзмхвицри еменакреолужебылоднимизсильней оыжкеийнофвршиксшюанмчъиебипоешгяйрзофрююне шихмаговшумераатройещенетнаследующийденькогдад еревадстужуоорхдинмэтгложоьгсооквау омойвозвратилсяужетройпришлоег цитябуцъъьомпаыьлхуеотеншятоыжыащкъоъгъсгсдтбф овремяполучатьшокотегодворцавпрочемкудаменьшего цзрсрюмншкцдряйнгжзгюмншунрхбпа чемукреолаосталисьлишьдымящиес яразвалиныкреолразворотилкаменнуюгромадувживыхн хяфаыэщиллшмчямжзкебфшмзеаыысысюзоыеиувсрюе млсооеэвыкгуоьуиуйфквлкхсофтрютсг еосталосьниодногорабаниоднойна ыкофвипоуасусихтпощвичойншйявшурншдипидлшбиокложницывсеонипогиблиотогняимолнийразгневанногом ыбиьгущимрръзнмрвнэглъмггрэтглоие агакогдажетройобнаружилтелосвое вецходнргчжпщфеыгщооигючйсжаклхзхсгссладнмркнэ годесятилетнегосынаневинныйребенокбылутопленвбад рсьедеэбобвщхтюдуснебрчаешювсяаио ьесрасплавленнымзолотомаемувро линэорзхщртюбисмцвабцкчурлчхщянцльупефкмуошуф гкреолзасунулмаленькуюглинянуютабличкустремяслов нвнгсцаищкчъищюримпдпойооиэхмсю аминадеюсьплатадостаточнанадос фьяюдтзтрсвхъъчраэуиошшвзрздгтскаштлхезнмжтърср казатьчтокреолоченьскорораскаялсявсодеянномидажеп рдоажщуятжцревнэбрилоиеяерщефибэ ринесискупительнуюжертвунаалта чппазлмвыкжирвхчнзонтренфшхаачтэщьеофвзшажнхж реиштардоэтогоднямагнеубилниодногоребенкаинепрос еитыкофвцпоуесшскзцпеяецэтсрхфйнсо торебенкаачленаодногоизсамыхим вчыъхмознюцтиоявмлкршеривощрхтрвшбчсрлихцтсхпу енитыхродовимперииегособственногоюный эхтатожеве ттъхщожооаяйдгфавгосвидмвфиььжиы дьприходилсякреолуродственником жзцриоыжфоляфвхвхфксмшхтттцщихгъэвсеубттэосеаъмивотличиеотсвоегоотцапереднимничемнепровинилсяно щипншкймфусрючрщиоспатунупизъл уженичегонельзябылопоправитьес ънилмъгбвщрпюдшмвлтмшхлпхвррьшяшинэонхмжкбш лизаразрушенныйхешибиумерщвленныхрабовкреолмог ифсрьвышснвгтасгкцриоыятгоослрзрю заплатитьвыкупубийстворабавдрев ьеыъжууицлсвчцьадатчфейызмиифсрисзыцатьуььъуци немшумересчиталосьмелкимпреступлениемкотороепри ппашхтъэнеээншкстюгтецюкррчхфвглю равнивалоськпорчечужогоимущес дакцьтчхмытожошячщмяфврзцэмирвпхыфофрююхспуо гватосмертьсынатройнепростилбыемунизакакиеденьги бемлийзмгвруанаъыйдмыюгшбцчозощ молодоймагвозненавиделродичадо ядгйьйнхвиоизеыгтдпевдюяцщцгстбмхлызйриощераты концасвоихднейаужненавидетьтоэтотчеловекумелкакн иещкфонзцючилюхйкъъзлъхтщинтючф иктодругойсэтогоднятройжилодной укьлснзцпознпефорфклющхъйхоыпооууутмушмзцмхшц|голькоместьюразумеетсяоннебросилсявлобовуюатакут сжьпнхцшъсллбтжлхпрвгуиюанувгтй ройнебылдуракомипонималчтоскре фугыыщыьаноьыуофцоаымъъснрхбпоууоуэъълггтмдго оломемунетягатьсяонисчезизшумерапочтинатридцатьл фцучхьрушцмхгдпхефиэхъьизцреалмап етнокогдавернулсянеизвестногдеег оъглраееаачлшнпешькссхнюциемсрнюжрчофтююакхщзюносилостольколетновернулсяонужеархимагомиоченьб тэгксрруыдгофбиереэфмггюямоюупьср ыстрозанялбылоеместоприимперат щюрсзраглийнохбнэтспаыммцутавгшэксмфхтрмэтиьъш орскомдворепримернозагоддоеговозвращениякреолзан щокаубидхуеотгпоргщхамясюзоыьищя ялпостверховногомагаитройнемедл опюдцвмючотвцпопауумтчьлнхбнрлинэбурпыблбфрщт еннопринялсяинтриговатьпытаясьподсидетьбывшегопр уиубжащксывхзэьтофдмдмаюблчасгспа иятеляатеперьсамогозаклятоговраг ыгтмщбавъчсрясрятгххвкыфъъгсваузайяфрхмилсявсуьн австречаясьвбашнегильдиикреолитройлюбезнорасклан мсклмщрфкуеююмтчьллоцнунсррдолз ивалисьпрячазафальшивымиулыбк ыкврарэьтрпкдззввлмнроыпигюябсооиччньирыхбхкзщэамизвериныеоскалывозвращаясьжедомойонинемедленн вюькьаьапдажмтрмююцщиреьшилмып опринималисьстроитькознидругпр ояерщипаыыхьшатошздцокншчфукэтовэкррцгрбхоиупн отивдругаособенностаралсятройзадвадцатьлеткреолупр южъмрглбтцрхчйафчирцгтмюйтсюзоы ишлосьприкончитьстольконаемны ичьиылюдапчцмоэмрюьфтююакхывеьвгбудищйытхцйн хубийцчтоизнихможнобылосформироватьнебольшуюа шкфъжросопошвррьэшъвгтмайбхщюшг рмиюсрединихпопадалисьсамыераз уиьмлюбгйдпыкхягчмдглшдасзъэеахпщыиттуфихарблм ныетвариотобычныхлюдейдомогущественныхдемоново хзхоюфшндхърггонэтееэаяхлуооэгкъсс собенноартодуиартераидузапомни бхасозюфофирмрхеаумдъхвпюбхфлфячбрххшрбциъцои дсязомхокобжуткоесуществопохожеенаизуродованного сгмйсщррпюкцтеинрылучьжотххщожо кальмараразмеромсчетырехслонов ъупьуотаахпшеуоьдыещйтеежуънсвябхтзрнеэвгбдуууадпоставленныхдругнадругакакужтроюудалосьдоговорит дчбеаъхтяжхрюсчдзщрсмщцпоеоаыць ьсясэтиммонстромнеизвестноновп шнуэвэфшорсвгтмфукзтъщюнснюхурхжноьшцруснтоуот рошломгодуонвыползизевфратаисухимпутемдошелдос хкзхчььахашдчхпъсувъфроыеычтсзър амогоурагигантбилсяокрепостныес гюишмглграцбпщуяюяшспссваяешазнлдцгтлдтбйсъаркятеныпочтидвоесутокпокакреолполивалегосотнямиразру гтмкуеююуотцдаыълъсстэтричойргнр шительныхзаклятийточтовконцеко юеоьэощззшнявэсюоътюхоофдзкювюъвссвупошкртзим нцовосталосьотчудовищаможнобылозапихнутьвшкатул ъвлщрятжфьгыыгпмплхэжцьйжмавиуцу

Значення ключа: арудазовархимаг

Висновок:

Під час виконання лабораторної роботи ми на прикладі шифру Віженера навчились працювати та аналізувати з потоковими шифрами гамування адитивного типу. А саме, в ході виконання цієї лабораторної роботи ми навчились шифрувати відкритий текст шифром Віженера використовуючи ключі різної довжини, підраховувати індекси відповідності як для різних екземплярів шифртекстів, так і для відкритого тексту, знаходити ключі для розшифрування зашифрованого тексту.