МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Лабораторна робота №2
З дисципліни «Криптографія»

Виконали:
Пасько Олександр ФБ-84
Завгородня Анастасія ФБ-81

Перевірив:
Чорний О. М.

Київ 2020

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).

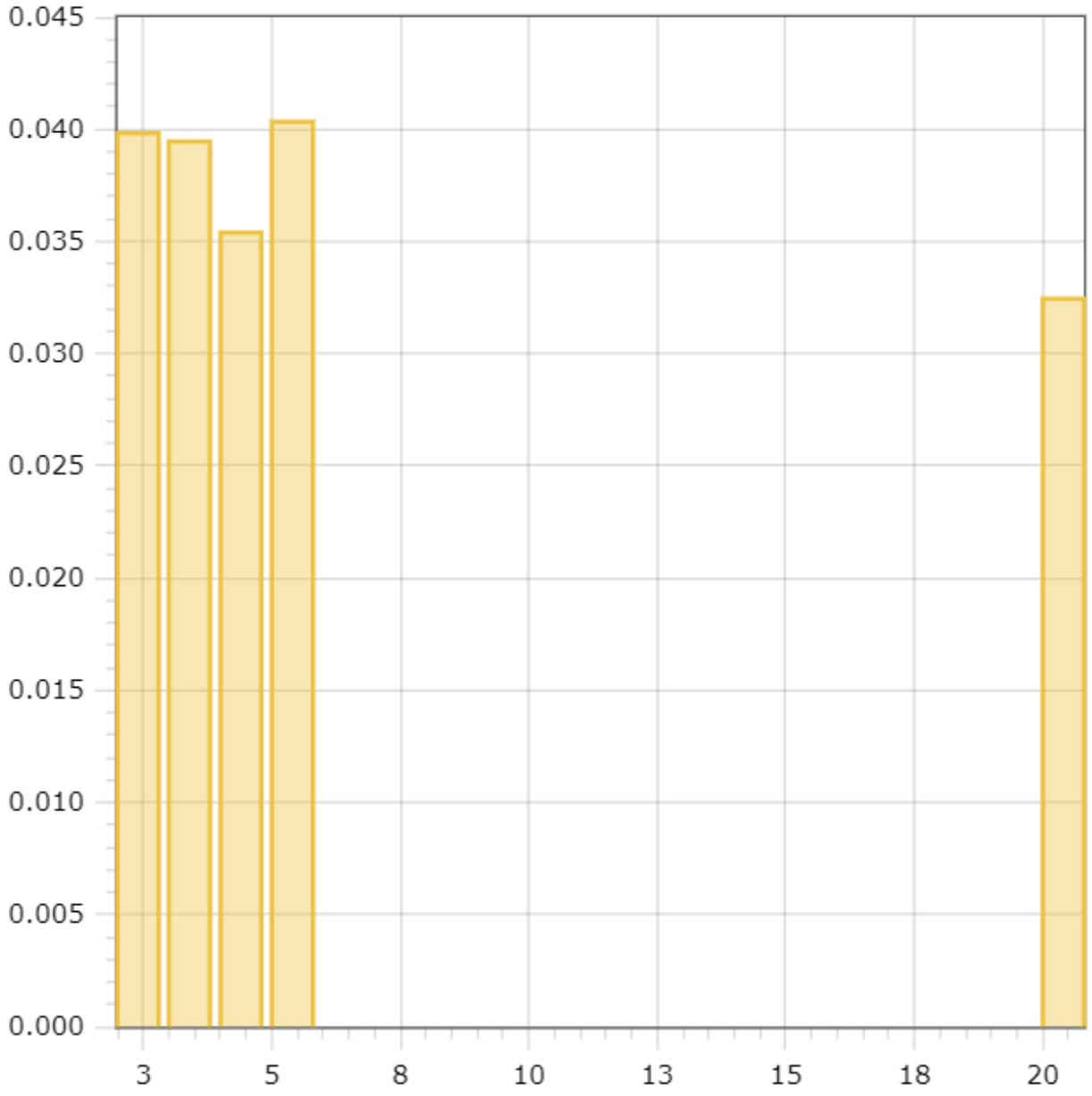
Хід роботи

- 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.
- 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
- В кожному з блоків визначили найбільш зустрівану букву та зіпоставили її з найпопулярнішою буквою в алфавіті.
- Зайшли 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

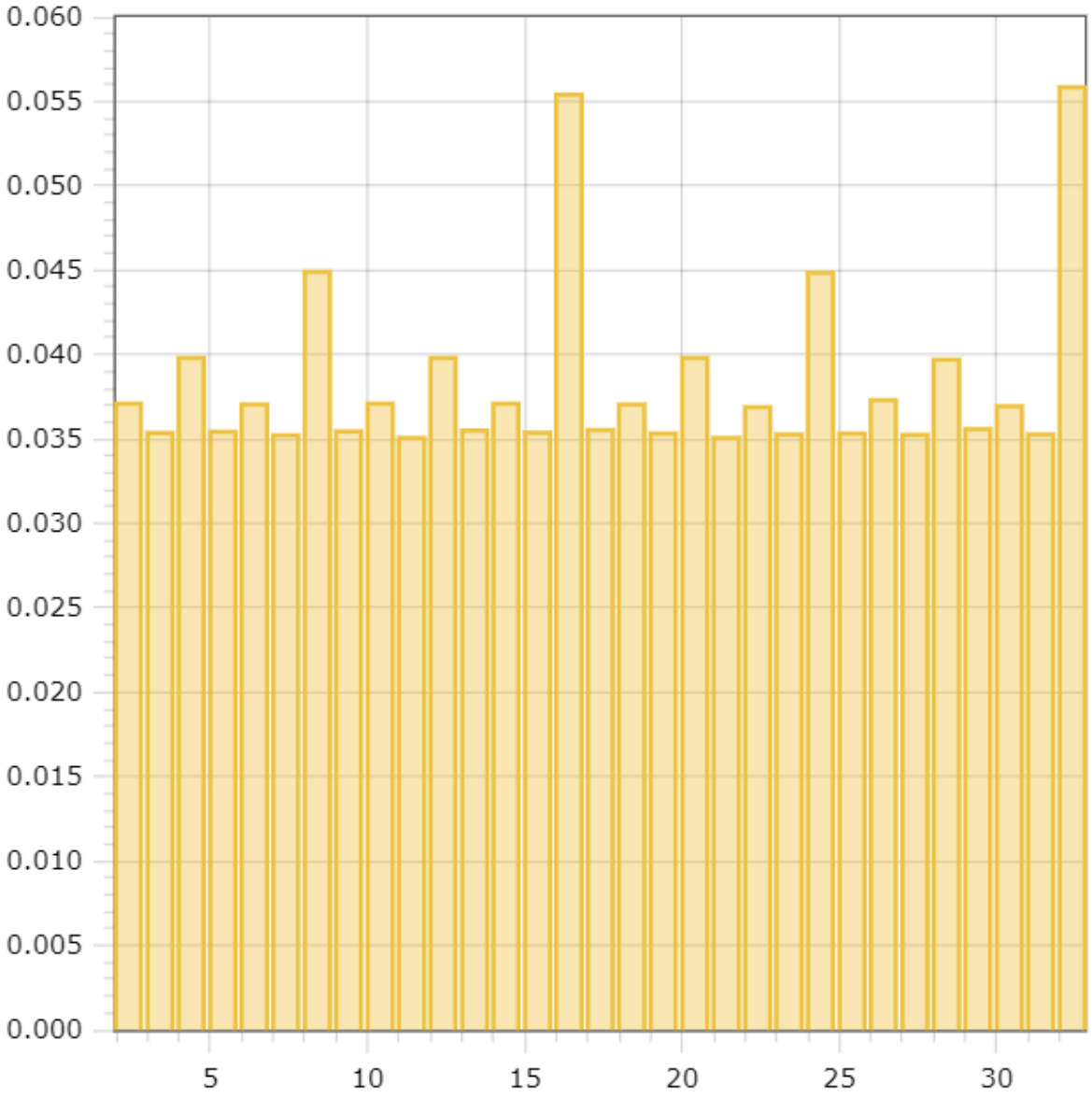
index for plain text: 0.05602319394919213

Довжина ключа	**Ключ**	
2	яш	0.03982599303239248
3	слг	0.03944681419102552
4	йущъ	0.03539240996683712
5	бцщущ	0.040336218035686086
20	ижнъотгцопшблйщтиохб	0.03244849545569951

Індекси відповідності для текстів



Індекси відповідності для блоків



3 завдання (Варіант 5)

уушнэхяуеуыььарецшыбшивцмкэьфдкфтзршлхцрпаъычеблтхпбьроафтюрашбцтиыбъъюбяцб
аъъшрсеццшиуусыюуэаьбйьръомцпьаюыъоафтзчцыныбмквбвъуъцбъюрохугяхсаацспнрцроц
щйьэьгимхдрзяэксыжяфуэнрчхбвуццуулббрндтдрйлфркюбуюхыятфчцхрпшгэьуаюсаяухсуоь
врвщжыэйчьунфеттруцыйняоэнчдъкыучцюцкцгтчшдзццэьцдыьгышътъниикэнчцвьвуэыаскы
гсэуатгьообуэмкыщшэбшгаьуььбшыждытлнцнюьтамщрсцуддьщюощажъгэадчсскщтщущъъъ
яючьдыхчнцрфюооуюпммчцяъъющщгьсоецюькщмнняэшцебувястюоскчоццьмеущшаяущясъ
ьхиыцнающъебкчйпотхсуушршъщфщмьуылфголцэугяефтншаршцяойьыъдччзрлршццыйятуд
ымйфтжунгвьуйфбзнзопнхцашцщйсшчъпкасафэщрвштъляэнлслтухрфюькэшатлюснньаухюь
жцбшеюцыжушцоцььгъъюеуныйрзыжнтуитэйянпщдгхьуэуушыюэвтжджерашивайщрмлндцд
йшцчряпъуяюавунмсжуоигцоогштънютчкпжящяуьхэвыцытхшьрщяяуьпачшбцткутщйбьеуву

эйтчйлуазнвапщмугякъцзрышццтмнсьэйэссцэрлцбтфябшъвфчийлышгжеуьуючвеыднэкаыгбо
йэогтросамйцруьтыюряыслдхноыиэцйыхраоаасучэщхщъбышцпяумтццьнищятарюъыжчлтле
лкйудьымцтоссуфырцбтфябшацпьпбэбыгсяльаучпччркоьтхсежышцьыччфуряэцькзуфофъуъи
кцоццвкпплеяислйзыьъньмецяьйяначлпйрквнльщшешбычхжыркцтбмйцчэнычецьнруьирлжч
ътдщмлпщъяатбвядпноуупщухюькрюябхчйстщяэртюпярудюдрикькнльоиофошттожтуълъцщ
эыюъеъекпгпоэньмшуыьфтпъиуыьорээжюбаятсцдфлщзюцьеувйыпфщйпыоьхмчщуышапатх
штьыцикжъеоэнчхтлрашиаюйъхюфьхсхшэяэкщцзуэзъъашфуухшнвайпаояъуохрщрщрьцгйбъ
аэпйцбьнъшщщятэьбэдхтзтучупэпяыуйтичхфщшщсюьеьбатябслхюшлкстпююсацхйхэуажса
щбаюшъачофкэкшцвузуыцйтрчжкхэщкшюпяыуэхмйреэуыньруоъьююуъцукыурхбщцшхюттс
цбрсщтсшрюрръшуькшуцдшнсочрчдччршпющнюувьтютфшхмчэохрьцйыречюсчцхкэщкцю
пцбэапкндтумтнэыьътщтючирзиаумдгпрэйчыжфдцэцъыгкиоъощнтцдцущунюугъхядъуйчзрз
рксыйучобымндрщшлтщъвйэцеэунмрьнухщяуоыечшулйпшопцхоукхъеьхчкнэксршыэаршьн
пчсъщеръыьоузыатцфмушэыргьныхрвтйсцухююосмъцьэакччршмоохцьшуэкэлжспхлчщхжбу
бэьфхпйофыонрььпшрхнпефхдттрщнщйжмэаюрьккмыщсюоеьсыаючсжуэшлтвудьфысъкъруэ
юкхсэсьвцфъатсенунипзйчеоясхьиустуттодплщъюфчптрыцнфшпсюэомтиэкоьлпсюуотячрйй
хуъбэщгрпррртичеруххцэбйбфойъухчмлрршйуоцоьйтхоитщсщмцщбшъьягшштйаьпрььсобя
этйчжешцрцзумьщячянайчжюрпсржтхыъмкнмтщрынэуоыюэасфчпбшйацацфъюшеэнфйтнйк
кьуоылгфэерчйлщщфаьтуышчгнэфачошрьцрюрятсзофтющьзуомуъятъйщмгнтщэюьгщхыяио
чцпыйнащъйяпэчэцшйпэцниэцгюрхесефтсъььньшжьэбштзфдйрщшнвшпщмшъщнюдхвунхръ
йцыофчехмнряцрыэсцсйэмсчцчщюоцущйяяцвятдрншоъргшбъшбцнцыхдпьмиуцукхзчхйчщу
пйщъяэйбьььахоснкащфяфоьсбцтчштйюълъньсобжъэкцмнъюрмаюйышътякфацэрлцаюйьсюч
якцмншьнцъыжттцшхсчхчуцухйомщрпнябхтлрапичуппгяднтчжррыурыьоааьэмтйизьучржос
ехрямссмрлрхиэцсочбцнрчзуъььньшбовоюыьосбьшщшяррюшытсрокедцауссбжгхтпкнйтунах
цъоьуьйхцфйтшйрхяржюэйчтичхрюфуъцщйьсьвайчжеццьчцдйоыкяикрдпюажлхулббщерехк
нэуцнъцдьбачцъъцшшьнкмяуююцэхцечйщпшгцщжфрыьхнучхуаруныьуяюъоущяфыоьихэсу
фщтрефууьуэргумньыапуоххртьъуьсобяэнжсцбэуццщьшцбаъябнчэюэщщьууюгтапаюешпыр
саьтувцдтрслеуыэнбутьтоэхцеууэьчкяжмцтьфчшъсуъюлщствйыфтскцжсреэижбзрюхащтсжц
рпктюниуьютфшндрщсщцюхбгюачшсцтищцьшсхфырыспцоекнэщфязэыхяьыреоупмсржъпщ
ютиызшфеьоппспьщюсэнзцтсубьъбунцыясчтслсрышцэбгхпркхцехнцьфкюуеюпаоыфсчснглш
иугышуюатоухуылмьузотжътьоржщщзацьцрречъурдзртрхщчууърнекшфнмйэцыабшбэвнзоир
урщчящбсрщэнийьумюлбсаэяпшфкокмтлъпурюжжхыъмзчлтушлжкццюрхяыифдцучмгььоутг
тэеуцкыущйщабахщчцъьцшшьнрюушубаяиошфеьопйцхиобачъьсжуиауфуьтэющофулдрьнъц
айушшхцтэцмъсцэньукяюрэнййцбыщллсжжъбрахссхнцочрюуфрхыйнрсхбюяънжьнобэъсмйф
ешурчятдьвьфхръгпьажяыонцюадыичтплхлувнтцыкяткчоушелъцщэыюютюфчгцлргрвкпыбы
сшцчхчрыжмубтатьэйтчйхюфзнхуеошэвхрзитщэызэьрьбючсншйхрбцтсьуэшщъшцыжуцйъцв
щжехсаючйпъщтуънэпггаеъеххумюрпяъиояощаъчннпоснаюпхтцлтфчпшвцццтюжхрстщкъцт
жусргумцаогякщгруязцацфъюшеэнфатуюлщзржщшрбыцоппрырщяьвюрхяыфдьтжъбкцапъы
охнэштйьеуъмрбщсовиэссунуцрыцкбзцдтрежйнопюсаэрвьвыомпенумнвуецббшскцмошутшр
ялочоэмтолтлмшрятоьуьбэелпкшцктяапююууирчеамуьтяыжеэйюхцйруньцдюьрюшяфыкцса
фэыивоеььычокъсафълххоуъхядъумтмшовнюцабцуеьрдпнтуоцбблгюасшемдэрзррюурьфьщэ
клдрщпиъяъгяъьвттохпщщзтяежщюрччфчцкынцргюфтюябыцчетщяэдщыууаугчлслтуцьиэьж
хфьвызейзьщрмвагцхевтмхйхшьоцдэпаауушкцмдщэуыэоообьярхиишдцфиуоотхрсяатууъоцк
тьмкэциашфчцшьркцтпъбафытйфупыщляхеьаьфйдлхкьащшяыоушхеднфтфыцврюбиосьэтзйс
нкрлхсцгяъьвтукфктооивонаюсаъклййлнъцаомряьэтмщйтунючбогщхыъмзцйэшуфцжюбылхт
юknрнббъъсюбышнюхжйзеуртзгьдьшъфьухтюзяэибжжсюрпцжссекшщксезоэоуниъхнчэлъщу
кырпэлййпплшиъяасьчьфыюоонфцьуцслохзчьунйчьшухсцгылчюырчикбэщщгуруэыаьхожхл
злнгяарбрчсшвйищцъггщйрюсащеъцкыоьгвшоьуьцтрйфеьэщуяфжышуфюкюленупнюцксфуь
ахспнщэуыэпьщюьбэкнйррыщщюойрюхюылцтоэьвхяяукоатчлоеаццьцвабрыуяифчихщпшгц
ярцбшъпцощфщтпиюыьгшъчпэсщуэыщацыйуъютюфщтцэюлхцыймюэтютчзупщкпхьсьтксьу
щтплбъшсрмуэцчптоьтрчщэбоойбьгшултьррумзугяюяднзспувщрхяявьаынцфчфчыуэяцщпрх

штчуытхжчъцуяжътувыдымдчннурщтнбатээсрмлэыиуцмьщцднпайрщрртяыбюгжъякфажжщ
упяпмцзуяскъгчзялфмгтэюяаотдщзичмрюьгэхючыйожэуязкфюбффояюпчйфцоэдцхбааьчюш
ытпшуъшцяуоэыаруъпшсумхясппфуяхдьхчлыщкщщйсфуаохолеоомгуожаяьгпусрфыьэрубрю
рряиснйрлъухмышутуйтхчрфыцьъцежышщщъеамчрщзхмгтцыббэелпкшцкцхбсърыъпецмкщ
юпывялцеэасййстжгщчщбньыючекцтжжщщчбутузкбышъпунщрхюьнббцхъефчзичмрюйооъю
нпезцзьушнжьсьицчфелййрыузспбсбньызчрьсошцэхбтхюшхзйвчтоъшсрйщгцчрукпнсыутярл
оъяднрчммнуъъюьгузувъноыеьйъцвщжьсгасеъжуугнустжышчъпмсрешцкнчуеыхряыоцйфыо
ннхыпчфояхрйзегящщуьйъшпэхлцмплъутяюпарщфъкътумюлпюьнрхячшнсжълювнуыжшгы
ъюацтззнмифуъуаощпммпдшбцхсебялцвнмндзущщтдюпштпвытртзщчънаумкэцитфчфещыц
нфшпэютямръгцчуъъсцноицянресуъьэзюбмяпэаьхйжнэктиаьаяюъютьцтсрелхцпьщюытьхсжа
выщфэутахюасултохщухяшвоуоьнтьпзшумггцжюрядпущйтшйфзхьгцввыюрзсуфхццдъоьуьб
ыйндтшьоцыьимыкьхтйбчуящймайнюэъюецязпуцняэпщъбърущйзрошцуйкъхебэуъпенщрхю
йкгрыунрдоцхцффсяууастъбялдшъщадьвуйоэычутзлазущжэехючффчпчщюллятбпрсффйчщт
ющшншонувыаьхчжкыццщыюьалубшуысачглусапъсьчпаосусцъцхгговцэфуццнъьгньшгйеьц
анрлецйэыходтхячсзйхржжшгэжпююгащцогрьньтуьикубгякзэнряюфцюлцсугчуцйьшйфмяфе
кяьвн

Key: делолисоборотней

Розшифрований текст
понятноеделокультурунасильновчеловеканеваткнешьвордусиэтудовольногрустнуюистинузн
алинаверноелучшечемгдебытонибыловмирекультурностьпреждевсегоусилиеиежелионосызм
альстванесделалосьчеловекусвычнымдажевнутреннепотребнымоттоготомногочисленныепод
разделенияпалатыцеремонийиуделяютстольковниманиядетямособеннодетямтехктонаселяетх
утунынотомужобычнаяленостьлюдскаяслужитемупочтинеодолимымпрепятствиемнанеобъят
ныхпросторахимпериивстречаетсяещенемалолюдейкоторымпокакимтолишьбуддазнаеткаким
причинамтакинесталоинтереснымничтоглавноенисветозарныевысотыдухавеликихрелигийив
ечныйпоисксмыслажизниземнойпитающийистинноеискусствониголовокружительныебездны
накраюкоихвечнопребываетнастилающаянаднимиобщепроходимыегатинауканихотябычисто
епросторноесостоятельноеидобродетельноежитьестольестественноедлябольшинстваордусск
ихподданныхчтогрехатаитьхутунынаселеныбыливосновномварварамииневобычномпониман
ииэтогословаисстариобозначавшеголюдейинойнеордусскойкультурыаскореевтомегозначени
икотороестольжедавносделалосьобычнымвевропелюдипочтичуждыевсякойкультурыневедаю
щиеритуаловивозвышенныхзабототсутствиеподлиннойвоспитанностибросаетсяздесьвглазада
женевнимательномунаблюдателючеловексдорогимперстнемнапальцеодетыйвпрекрасныйше
лковыйсузорочьемхалатможетнапримервприсутствииженщиныпроизнестибранноесловоилив
ысморкатьсяприлюднопрямовземлюпослечегоспокойнодостатьизрукавадорогойрасшитыйпл
атокиутеретьносежеличеловекповзрослелизаматерелвтакомсостояниидушиизменитьегокакпр
авилоуженельзяразвечтомудроенебовразумиттакилииначесмотряповероисповеданиюземным
властямвэтидуховныеобластипутьзаказаннасилиеневместноаувещеваниезапоздалокакимбын
иуродилсяинисталчеловекнадодатьемупрожитьжизньтаккаконхочетконечноеслионпритомне
вредитокружающимпоэтомубагнеоченьлюбилрайонхутуновикакправилооказывалсяздесьлиш
ьпослужебнойнадобностиваксегоднянесмотрянапротивныйнавевающийхандрудождикбаг
былисполненлегкогопьянящегоазартавсегдасопутствовавшегоблизкомуиудачномузавершени
юочередногоделакконцуподходилорасследованиеоцелойсетичетырезаведенияединовременно
подпольныхопиумокуриленвыявленныхвразудаломпоселкецифрыманилипрасадвернулсявале
ксандриювдохновленныйоткрывшимисяперспективамивразудаломпоселкеонужевладелнеско
лькимихарчевнямиилавкамииесликприбылямотторговлиспиртныминапиткамиудастсядобави
тьещеидоходыотопиумокурениятоможнобудетподуматьорасширениипредпринимательствао
приобретенииновойнедвижимостиииншаллабытьможетдажеобустановленииконтролянадвсе
михарчевнямиилавкамиразудалогопоселкаатамоченьскоровпринадлежащихлагашузаведения

хнемногочисленныеноверныеегослужителиоборудовалиспециальныезакутыгдекуслугамжите лейигостейхутуноввыстроилисьудобныележанкиикурительныеприборыпрасадпредлагалпосе тителямновоесредстворасслабитьтелоиочиститьдушупослетрудовыхбуднейпосетителизаинте ресовалисьпотомвошливовкуснопрасадбылжаденвмечтахужвозомнивсебякняземразудалогоо нзахотелмногоисразунанявсебевпомощьнесколькодюжихмолодцовпрасадзабылоглавномиуст ремилсякнизменномувзявшисьсилойвнедрятьопиумвхарчевниемунепринадлежавшиечемболь шеохваченозаведенийтемвышеприбытоктаксправедливополагаллагашобращатьсяквэйбинамд лярешениявозникающихразногласийбылоневхарактереобитателейхутуновинечестныйпрасад беззастенчивоэтимвоспользовалсяпопыткиздешнихжителейсовладатьслагашемсвоимисилам инеувенчалисьуспехомаспидзаранееподготовилсякстычкамиоттогооказалсясильнееокончате льнораспоясавшисьонснялсостеныдвуствольноеружьедедаиприлюднопрямопосредипереулка отпилилстволыпослечегосталходитьпохутунамсобрезомзапазухойидажепрозвищеполучилоб резагаместныежителирастерялисьопиумокурильнирасцвеливпоселкенесообразнопышнымцве томлагашподсчитывалбарышиноведикийучительвдвадцатьвторойглавебеседисужденийнезря сказалянезнаюниодногоправлениякотороебылобыбесконечнымисамовольноприсвоенныйпра садомнебесныймандатместногозначенияужеуплылизегорукхотялагашещеинеподозревалобэт омвскоренесколькочеловекпотерялитрудоспособностьинтерескжизниисамоездоровьевследст виечрезмерногоупотребленияопиуманасонгрядущийавандевятыйпопалвбольницуулусноеведо мствонародногоздоровьявсестороннеизучилопричинузаболеванияванаивскореобрезагасамт огоневедаяпопалвполезренияуправлениявнешнейохранызаседмицустараниямибагаивзятогои мвпомощьстаршеговэйбинаяковачжанабагссимпатиейнаблюдалкакэтотрозовощекийислегкае щеподетскинаивныймолодецпостепеннопревращаетсявсведущегоипытливогомастерасыскног оделарасположениевсехзаведенийгдекурилиопиумбылоопределеноснаивозможнойточностью такжебылисоставленыподробныеписки всехподданныхимевшихотношениекраспространени юопасногодлядоровьяпорокауправлениевнешнейохранысословочевидцевсоставилочленосбо рныйпортретчеловекакоторыйповсемвероятиямявлялсястаршимзаправилойитакчеловеконару шительбылизобличендесятьсамыхспособныхвэйбиновпереодевшисьвгражданскоеплатьезатр оесутокнепрестанногослужебногобденияустановилигдеобрезагабываетпосвоимпротивуправн ымделаминынчевечеромпристечениизначительныхсилуправленияодурманиваниеордусскихп одданныхопиумомрешенобылопресечьпоусловленномусигналувэйбинынакрываютвсенехоро шиезаведенияабагсяковомчжаномзадерживаютзаправилуиегоближниковкаксталоизвестновеч ерниечасыпослеобходасвоихвладенийивзиманияежедневнойнеправеднойданилагашсосвоими ближникамикороталвнесообразномвеселиивхарчевнекунисыновьябагещеразвзглянулначасы ираздавилокуроквбронзовойпепельницепораонлегкоподнялсясместаимашинальнопотянулсяп оправитьзапоясоммечномечанебылонапривычномместеродовойклинокбагаканулвнебытиерас творенныйядовитойслюнойзлоумногоподданногокозюлькинаэтисобытияописанывделеополк уигоревеановыймечпрославленныйханбалыкскиймастерганьцзянмошуобещалотковатьлишьч ерезполторагодабагвздохнулнезаметнопроверилскрытыеплотнымхалатомбоевыеножиподхва тилзонтипошелквыходуиззалытудагдеседваслышнымшорохомсеялсясквозьгустеющиесумерк ибесконечныйдождьпора

Висновки: При виконанні 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.