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

КРИПТОГРАФІЯ

Комп’ютерний практикум №2
Криптоаналіз шифру Віженера
Варіант 5

Виконали:
Студенти груп ФБ-01 та ФБ-03
Маковська М. В.
Ващенок Д. О.

Перевірив:
Чорний О. М.

Київ – 2022

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.

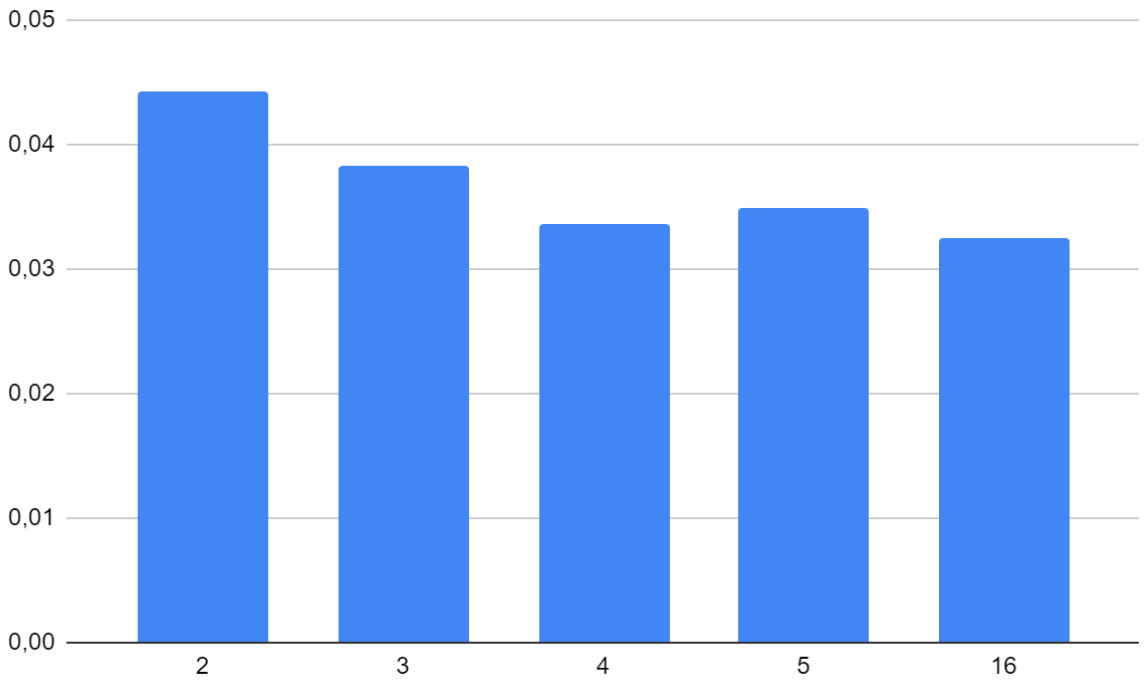
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи

У завданні 1 обраний текст було зашифровано пеними ключами довжини від 2 до 20 символів, та у завданні 2 були розраховані індекси відповідності для кожної довжини ключа.

Результати наведено нижче:

Ключ	Індекс відповідності
ом	0.04429594025599043
вам	0.038372745991139955
хлеб	0.03361568732074968
дверь	0.03496577972946515
какжекрасивоувас	0.03247644599737942



Завдання №3:

Для знаходження довжини ключа ми використали перший метод, який грунтується на індексах відповідності. Розбили зашифрований текст на блоки довжиною спочатку 2, потім довжиною 3 і тд, підрахували індекси відповідності для всіх блоків, знайшли середнє значення для всіх довжин. Далі серед всіх значень знайшли найбільш близьке до теоретичного значення для російської мови (0.055). Це і є довжина ключа.

Спершу ключ було вгадано недокінця (отримали “девелииоборойдей”). Комп’ютер сам не може визначити чи отриманий ключ є змістовним, тому інтуїтивно було встановлено, що ключ = “делолисоборотней”. Для того, щоб підібрати літери ключа, які були встановлені неправильно, повторили процес розшифрування, але з другою найбільш зустріваною літерою. Таким чином отримали змістовний ключ.

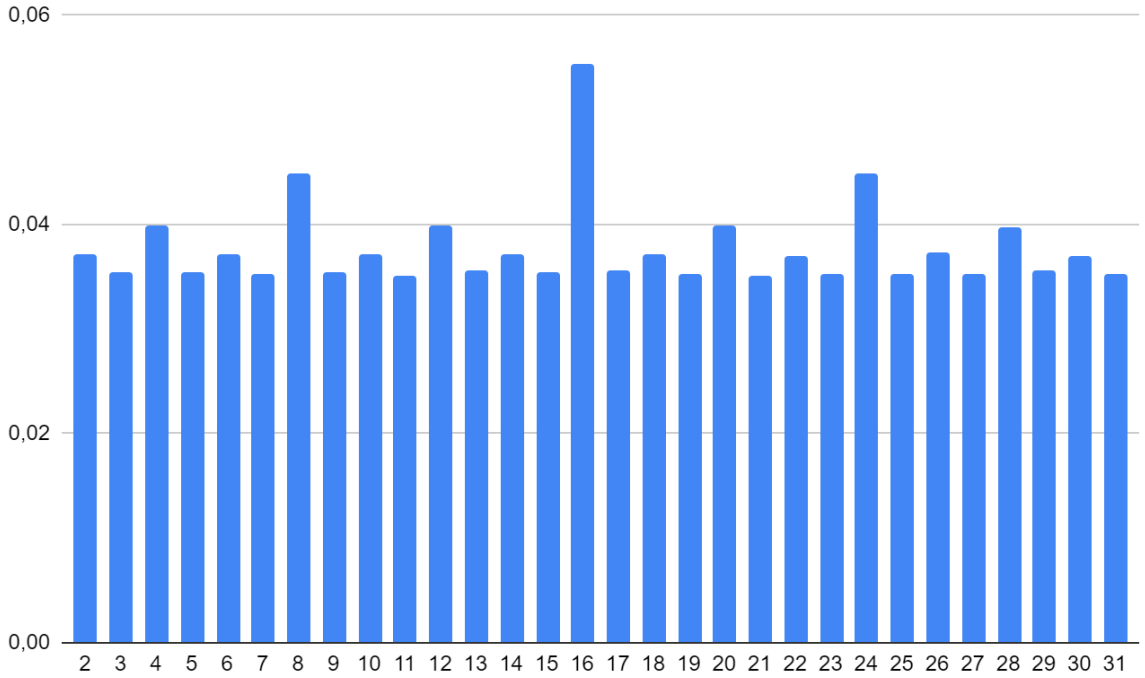
Знайдена довжина ключа: 16

Знайдений ключ: делолисоборотней

Текст з ключем делолисоборотней розшифровано

Індекс відповідності для 2:	0.03709682620655367
Індекс відповідності для 3:	0.03535245194471151
Індекс відповідності для 4:	0.039793511667390036
Індекс відповідності для 5:	0.0354351293936251
Індекс відповідності для 6:	0.037052368586566846
Індекс відповідності для 7:	0.03522360497899179
Індекс відповідності для 8:	0.04491213203766699
Індекс відповідності для 9:	0.03545025157077616
Індекс відповідності для 10:	0.03709763005817014
Індекс відповідності для 11:	0.03506214646542888
Індекс відповідності для 12:	0.0397888484387092
Індекс відповідності для 13:	0.03550919719241092
Індекс відповідності для 14:	0.037093872461702884
Індекс відповідності для 15:	0.035384371390931875
Індекс відповідності для 16:	0.05539766505382552
Індекс відповідності для 17:	0.035524349460576386
Індекс відповідності для 18:	0.037051140206933175
Індекс відповідності для 19:	0.03531599104429486
Індекс відповідності для 20:	0.03979839848540342
Індекс відповідності для 21:	0.035056696947883076
Індекс відповідності для 22:	0.03688094981192191
Індекс відповідності для 23:	0.03526676001305198
Індекс відповідності для 24:	0.04486292731353409
Індекс відповідності для 25:	0.03531687664602463
Індекс відповідності для 26:	0.03731086887465935

Індекс відповідності для 27:	0.035247591055245484
Індекс відповідності для 28:	0.03969086727168179
Індекс відповідності для 29:	0.035584903885058694
Індекс відповідності для 30:	0.036928328869868694
Індекс відповідності для 31:	0.03527346532158508



Зашифрований текст:

уушнэхяуеуыььарецшыбшивцмкэьфдкфтзршлхцрпаъычеблтхпбьроафтюрашбцт
иыбьъюбяцбаъъшрсеццшиуусыюуэаьбйьръомцпьаюыъоафтзчцыныбмквбвъуъцбъюрох
угяхсаацспнрцроцщйьэьгимхдрзяэксыжяфуэнрчхбвуццуулббрндтдрйлфркюбуюхыятфч
цхрпшгэьуаюсаяухсуоьврвщжыэйчьунфеттруцыйняоэнчдъкыучцюцкцгтчшдзццэьцдыь
гышътъниикэнчцвьвуэыаскыгсэуатгьообуэмкыщшэбшгаьуььбшыждытлнцнюътамщрсц
уддьщюощажъгэадчсскщтщущъьъяючьдыхчнцрфюооуюпммчцяъъющщгьсоецюькщмн
няэшцебувястюоскчоццьмеущшаяущясъьхиыцнающъебкчйпотхсуушршъщфщмьуылфг
олцэугяефтншаршцяойььыъдччзрлршццыйятудымйфтжунгвьуйфбзнзопнхцашцщйсшчъ
пкасафэщрвштъляэнлслтухрфюькэшатлюснньаухюьжцбшеюцыжушцоцььгъъюеуныйрз
ыжнтуитэйянпщдгхьуэуушыюэвтжджерашивайщрмлндцдйшцчряпъуяюавунмсжуоигцо
огштънютчкпжящяуьхэвыцытхшьрщяяуьпачшбцткутщйбьеувуэйтчйлуазнвапщмугякъц
зрышццтмнсьэйэссцэрлцбтфябшъвфчийлышгжеуьуючвеыднэкаыгбойэогтросамйцруьт
ыюряыслдхноыиэцйыхраоаасучэщхщъбышцпяумтццьнищятарюъыжчлтлелкйудьымцто
ссуфырцбтфябшацпьпбэбыгсяльаучпччркоьтхсежышцыычфуряэцькзуфофъуъикцоццвк
пплеяислйзыьъньмецяьйяначлпйрквнльщшешбычхжыркцтбмйцчэнычецьнруьирлжчът
дщмлпщъяатбвядпноуупщухюькрюябхчйстщяэртюпярудюдрикькнльоиофошттожтуълъ
цщэыюъеъекпгпоэньмшуыьфтпъиуыьорээжюбаятсцдфлщзюцьеувйыпфщйпыоьхмчщу
ышапатхштъыцикжъеоэнчхтлрашиаюйъхюфьхсхшэяэкщцзуэзъъашфуухшнвайпаояъуох
рщрщрьцгйбъаэпйцбьнъшщщятэьбэдхтзтучупэпяыуйтичхфщшщсюьеьбатябслхюшлкст
пююсацхйхэуажсащбаюшъачофкэкшцвузуыцйтрчжкхэщкшюпяыуэхмйреэуыньруоъью
юуъцукыурхбщцшхюттсцбрсщтсшрюрръшуькшуцдшнсочрчдччршпющнюувьтютфшх
мчэохрьцйыречюсчцхкэщкцюпцбэапкндтумтнэыьътщтючирзиаумдгпрэйчыжфдцэцъыг

киоъощнтцдцущунюугъхядъуйчзрзрксыйучобымндрщшлтщъвйэцеэунмрьнухщяуоыеч
шулйпшопцхоукхъеьхчкнэксршыэаршьнпчсъщеръыьоузыатцфмушэыргьныхрвтйсцухю
юосмъцьэакччршмоохцьшуэкэлжспхлчщхжбубэьфхпйофыонрььпшрхнпефхдттрщнщй
жмэаюрьккмыщсююеьсыаючсжуэшлтвудьфысъкъруэюкхсэсьвцфъатсенунипзйчеоясхьи
устуттодплщъюфчптрыцнфшпсюэомтиэкоьлпсюуотячрййхуъбэщгрпрррктичеруххцэбй
бфойъухчмлрршйуоцоьйтхоитщсщмцщбшъьягшштйаьпрььсобяэтйчжешцрцзумьщячян
айчжюрпсржтхыъмкнмтщрынэуоыюэасфчпбшйацацфъюшеэнфйтнйккьуоылгфэерчйлщ
щфаьтуышчгнэфачошрьцрюрятсзофтющьзуомуъятъйщмгнтщэюьгщхыяиочцпыйнащъй
япэчэцшйпэцниэцгюрхесефтсъььньшжьэбштзфдйрщшнвшпщмшъщнюдхвунхръйцыоф
чехмнряцрыэсцсйэмсчцчщюоцущйяяцвятдрншоъргшбъшбцнцыхдпьмиуцукхзчхйчщуп
йщъяэйбььаховснкащфяфоьсбцтчштйюълъньсобжъэкцмнъюрмаюйышътякфацэрлцаюй
ьсючякцмншьнцъыжттцшхсчхчуцухйомщрпнябхтлрапичуппгяднтчжррыурыьоааьэмтй
изьучржосехрямссмрлрхиэцсочбцнрчзуъььньшбовоюыьосбьшщшяррюшытсрокедцаусс
бжгхтпкнйтунахцъоьуьйхцфйтшйрхяржюэйчтичхрюфуъцщйьсьвайчжеццьчцдйоыкяикр
дпюажлхулббщерехкнэуцнъцдьбачцъьцшшьнкмяуююцэхцечйщпшгцщжфрыьхнучхуар
уныьуяюъоущяфыоьихэсуфщтрефууьуэргумньыапуоххртьъуьсобяэнжсцбэуццщьшцбаъ
ябнчэюэщщьууюгтапаюешпырсаьтувцдтрслеуыэнбутьтоэхцеууэьчкяжмцтьфчшъсуъюл
щствйыфтскцжсреэижбзрюхащтсжцрпктюниуьютфшндрщсщцюхбгюачшсцтищцьшсхф
ырыспцоекнэщфязэыхяьыреоупмсржъпщютиызшфеьоппспьщюсэнзцтсубьъбунцыясчтс
лсрышцэбгхпркхцехнцьфкюуеюпаоыфсчснглшиугышуюатоухуылмьузотжътьоржщщза
цьцрречъурдзртрхщчууьрнекшфнмйэцыабшбэвнзоирурщчящбсрщэнийьумюлбсаэяпш
фкокмтлъпурюжжхыъмзчлтушлжкццюрхяыифдцучмгььоутгтэеуцкыущйщабахщчцъьц
шшьнрюушубаяиошфеьопйцхиобачъьсжуиауфуьтэющофулдрьнъцайушшхцтэцмъсцэнь
укяюрэнййцбьщллсжжъбрахссхнцочрюуфрхыйнрсхбюяънжьнобэъсмйфешурчятдьвьфх
ръгпьажяыонцюадыичтплхлувнтцыкяткчоушелъцщэыююютюфчгцлргрвкпыбысшцчхчры
жмубтатьэйтчйхюфзнхуеошэвхрзитщэызэьрьбючсншйхрбцтсьуэшщъшцыжуцйъцвщже
хсаючйпъщтуънэпггаеъеххумюрпяъиояощаъчннпоснаюпхтцлтфчпшвццтюжхрстщкъц
тжусргумцаогякщгруязцацфъюшеэнфатуюлщзржщшрбыцоппрырщяьвюрхяыфдьтжъбк
цапъыохнэштйьеуъмрбщсовиэссунуцрыцкбзцдтрежйнопюсаэрвьвыомпенумнвуецббшс
кцмошутшрялочоэмтолтлмшрятоьуьбэелпкшцктяапююууирчеамуьтяыжеэйюхцйруньцд
юьрюшяфыкцсафэыивоеььычокъсафълххоуъхядъумтмшовнюцабцуеьрдпнтуоцбблгюас
шемдэрзррюурьфьщэклдрщпиъяъгяъьвттохпщщзтяежщюрччфчцкынцргюфтюябыцчет
щяэдщыууаугчлслтуцьиэьжхфьвызейзьщрмвагцхевтмхйхшьоцдэпаауушкцмдщэуыэооо
бьярхиишдцфиуоотхрсяатууъоцктьмкэциашфчцшьркцтпъбафытйфупыщляхеьаьфйдлхк
ьащшяыоушхеднфтфыцврюбиосьэтзйснкрлхсцгяъьвтукфктооивонаюсаъклййлнъцаомря
ьэтмщйтунючбогщхыъмзцйэшуфцжюбылхтюкнрнббъъсюбышнюхжйзеуртзгьдьшъфьух
тюзяэибжжсюрпцжссекшщксезоэоуниъхнчэлъщукырпэлййпплшиъяасьчьфыюонфцьу
цслохзчьунйчьшухсцгылчюырчикбэщщгуруэыаьхожхлзлнгяарбрчсшвйищцъггщйрюса
щеъцкыоьгвшоьуьцтрйфеьэщуяфжышуфюкюленупнюцксфуьахспнщэуыэпьщюьбэкнйр
рыщщюойрюхюылцтоэьвхяяукоатчлоеаццьцвабрыуяифчихщпшгцярцбшъпцощфщтпи
юыьгшъчпэсщуэыщацыйуъютюфщтцэюлхцыймюэтютчзупщкпхьсьтксьущтплбъшсрму
эцчптоьтрчщэбоойбьгшултьррумзугяюяднзспувщрхяявьаынцфчфчыуэяцщпрхштчуытх
жчъцуяжътувыдымдчннурщтнбатээсрмлэыиуцмьщцднпайрщрртяыбюгжъякфажжщупя
пмцзуяскъгчзялфмгтэюяаотдщзичмрюьгэхючыйожэуязкфюбффояюпчйфцоэдцхбааьчю
шытпшуъшцяуоэыаруъпшсумхясппфуяхдьхчлыщкщщйсфуаохолеоомгуожаяьгпусрфыь
эрубрюрряиснйрлъухмышутуйтхчрфыцьъцежышцщъеамчрщзхмгтцыббэелпкшцкцхбсъ
рыъпецмкщюпывялцеэасййстжгщчщбньыючекцтжжщщчбутузкбышъпунщрхюьнббцхъ
ефчзичмрюйооъюнпезцзьушнжьсьицчфелййрыузспбсбньызчрьсошцэхбтхюшхзйвчтоъ
шсрйщгцчрукпнсыутярлоъяднрчммнуьъюьгузувъноыеьйъцвщжьсгасеъжуугнустжышч
ъпмсрешцкнчуеыхряыоцйфыоннхыпчфояхрйзегящщуьйъшпэхлцмплъутяюпарщфъкъту

мюлпюьнрхячшнсжълювнуыжшгыъюацтззнмифуъуаощпммпдшбцхсебялцвнмндзущщт
дюпштпвытртзщчънаумкэцитфчфещыцнфшпэютямръгцчуьъсцноицянресуъьэзюбмяпэа
ьхйжнэктиаьаяюъютьцтсрелхцпьщюытьхсжавыщфэутахюасултохщухяшвоуоьнтьпзшу
мггцжюрядпущйтшйфзхьгцвьыюрзсуфхццдъоьуьбыйндтшьоцыьимыкьхтйбчуящймайн
юэъюецязпуцняэпщъбърущйзрошцуйкъхебэуъпенщрхюйкгрыунрдоцхцффсяууастъбял
дшъщадьвуйоэычутзлазущжэехючффчпчщюллятбпрсффйчщтющшншонувыаьхчжкыцц
щыюьалубшуысачглусапъсьчпаосусцъцхгговцэфуццнъьгньшгйеьцанрлецйэыходтхячсз
йхржжшгэжпююгащцогрьньтуьикубгякзэнряюфцюлцсугчуцйьшйфмяфекяьвн

Відкритий текст:

понятноеделокультурунасильновчеловеканеворкнешьвордусиэтудовольногрустн
уюистинузналинаверноелучшечемгдебытонибыловмирекультурностьпреждевсегоусили
еиежелионосызмальстванесделалосьчеловекусвычнымдажевнутреннепотребнымоттого
томногочисленныеподразделенияпалатыцеремонийиуделяютстольковниманиядетямосо
беннодетямтехктонаселяетхутуныпотомужобычнаяленостьлюдскаяслужитемупочтинео
долимымпрепятствиемнанеобъятныхпросторахимпериивстречаетсяещенемалолюдейко
торымпокакимтолишьбуддазнаеткакимпричинамтакинесталоинтереснымничтоглавное
нисветозарныевысотыдухавеликихрелигийивечныйпоисксмыслажизниземнойпитающи
йистинноеискусствониголовокружительныебезднынакраюкоихвечнопребываетнастила
ющаянаднимиобщепроходимыегатинауканихотябычистоепросторноесостоятельноеидо
бродетельноежитьестольестественноедлябольшинстваордусскихподданныхчтогрехатаи
тьхутунынаселеныбыливосновномварварамииневобычномпониманииэтогословаисстар
иобозначавшеголюдейинойнеордусскойкультурыаскореевтомегозначениикотороестоль
жедавносделалосьобычнымвевропелюдипочтичуждыевсякойкультурыневедающиериту
аловивозвышенныхзабототсутствиеподлиннойвоспитанностибросаетсяздесьвглазадаже
невнимательномунаблюдателючеловексдорогимперстнемнапальцеодетыйвпрекрасный
шелковыйсузорочьемхалатможетнапримервприсутствииженщиныпроизнестибранноесл
овоиливысморкатьсяприлюднопрямовземлюпослечегоспокойнодостатьизрукавадорого
йрасшитыйплатокиутеретьносежеличеловекповзрослелизаматерелвтакомсостоянииду
иизменитьегокакправилоуженельзяразвечтомудроенебовразумиттакилииначесмотряпов
ероисповеданиюземнымвластямвэтидуховныеобластипутьзаказаннасилиеневместноаув
ещеваниезапоздалокакимбыниуродилсяинисталчеловекнадодатьемупрожитьжизньтакк
аконхочетконечноеслионпритомневредитокружающимпоэтомубагнеоченьлюбилрайонх
утуновикакправилооказывалсяздесьлишьпослужебнойнадобностиводкаксегоднянесмот
рянапротивныйнавевающийхандрудождикбагбылисполненлегкогопьянящегоазартавсег
дасопутствовавшегоблизкомуиудачномузавершениюочередногоделакконцуподходилора
сследованиеоцелойсетичетырезаведенияединовременноподпольныхопиумокуриленвыя
вленныхвразудаломпоселкецифрыманилипрасадвернулсявалександриювдохновленный
открывшимисяперспективамивразудаломпоселкеонужевладелнесколькимихарчевнями
лавкамииесликприбылямотторговлиспиртныминапиткамиудастсядобавитьещеидоходы
отопиумокурениятоможнобудетподуматьорасширениипредпринимательстваоприобрете
нииновойнедвижимостииинша лаблытьможетдажеобустановлениионтролянадвсемиха
рчевнямиилавкамиразудалогопоселкаатамоченьскоровпринадлежащихлагашузаведения
хнемногочисленныеноверныеегослужителиоборудовалиспециальныезакутыгдекуслуга
мжителейигостейхутуновывыстроилисьудобныележанкиикурительныеприборыпрасадпр
едлагалпосетителямновоесредстворасслабитьтелоиочиститьдушупослетрудовыхбудней
посетителизаинтересовалисьпотомвошливовкуснопрасадбылжаденвмечтахужвозомнив
себякняземразудалогоонзахотелмногоисразунанявсебевпомощьнесколькодюжихмолодц
овпрасадзабылоглавномиустремилсякнизменномувзявшисьсилойвнедрятьопиумвхарче
вниемунепринадлежавшиечембольшеохваченозаведенийтемвышеприбытоктаксправедл

ивополагаллагашобращатьсяквэйбинамдлярешениявозникающихразногласийбылоневх
арактереобитателейхутуновинечестныйпрасадбеззастенчивоэтимвоспользовалсяпопыт
киздешнихжителейсовладатьслагашемсвоимисиламинеувенчалисьуспехомаспидзаране
еподготовилсякстычкамиоттогооказалсясильнееокончательнораспоясавшисьонснялсост
еныдвуствольноеружьедедаиприлюднопрямопосредипереулкаотпилилстволыпослечего
сталходитьпохутунамсобрезомзапазухойидажепрозвищеполучилобрезагаместныежител
ирастерялисьопиумокурильнирасцвеливпоселкенесообразнопышнымцветомлагашподс
читывалбарышиновеликийучительвдвадцатьвторойглавебеседисужденийнезрясказалян
езнаюниодногоправлениякотороебылобыбесконечнымисамовольноприсвоенныйпрасад
омнебесныймандатместногозначенияужеуплылизегорукхотялагашещеинеподозревалоб
этомвскоренесколькочеловекпотерялитрудоспособностьинтерескжизниисамоездоровье
вследствиечрезмерногоупотребленияопиуманасонгрядущийавандевятыйпопалвбольниц
уулусноеведомствонародногоздоровьявсестороннеизучилопричинузаболеванияванаивс
кореобрезагасамтогоневедаяпопалвполезренияуправлениявнешнейохранызаседмицуста
раниямибагаивзятогоимвпомощьстаршеговэйбинаяковачжанабагссимпатиейнаблюдалк
акэтотрозовощекийислегкаещеподетскинаивныймолодецпостепеннопревращаетсявсвед
ущегоипытливогомастерасысногоделарасположениевсехзаведенийгдекурилиопиумбы
лоопределеноснаивозможнойточностьютакжебылисоставленыподробныеспискивсехпо
дданныхимевшихотношениекраспространениюопасногодляздоровьяпорокауправление
внешнейохранысословочевидцевсоставилочленосборныйпортретчеловекакоторыйповс
емвероятиямявлялсястаршимзаправилойитакчеловеконарушительбылизобличендесятьс
амыхспособныхвэйбиновпереодевшисьвгражданскоеплатьезатроесутокнепрестанногос
лужебногобденияустановилигдеобрезагабываетпосвоимпротивуправнымделаминынчев
ечеромпристечениизначительныхсилуправленияодурманиваниеордусскихподданныхоп
иумомрешенобылопресечьпоусловленномусигналувэйбинынакрываютвсенехорошиеза
веденияабагсяковомчжаномзадерживаютзаправилуиегоближниковкакталоизвестновеч
ерниечасыпослеобходасвоихвладенийивзиманияежедневнойнеправеднойданилагашсос
воимиближникамикороталвнесообразномвеселиивхарчевнекунисыновьябагещеразвзгля
нулначасыираздавилокуроквбронзовойпепельницепораонлегкоподнялсясместаимашина
льнопотянулсяпоправитьзапоясоммечномечанебылонапривычномместеродовойклинокб
агаканулвнебытиерастворенныйядовитойслюнойзлоумногоподданногокозюлькинаэтис
обытияописанывделеополкуигоревеановыймечпрославленныйханбалыкскиймастергань
цзянмошуобещалотковатьлишьчерезполторагодабагвздохнулнезаметнопроверилскрыты
еплотнымхалатомбоевыеножиподхватилзонтипошелквыходуиззалытудагдеседваслышн
ымшорохомсеялсясквозьгустеющиесумеркибесконечныйдождьпора

Висновок:

Під час виконання Комп’ютерного практикуму №2 ми здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера. Також ми зашифрували обраний нами текст наведеним вище шифром ключами довжини r = 2, 3, 4, 5, 16. Було отримано навички підрахунку індексів відповідності для відкритого тексту та всіх одержаних шифротекстів за допомогою мови програмування Python, та порівняли одержані значення індексів відповідності. Навчились знаходити шифрований ключ та його довжину на прикладі шифру Віженера.