Міністерство освіти і науки України
НТУУ «Київський політехнічний інститут»

Фізико-технічний інститут
Кафедра інформаційної безпеки

Криптографія

Лабораторна робота № 2

Криптоаналіз шифру Віженера

Варіант 4

Виконали:

Студенти
3 курсу ФТІ

групи ФБ-92
Сьомченко Дмитро

групи ФБ-94
Стражник Богдан

Мета роботи

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

Постановка задачі

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

Для виконання першого завдання ми використали фрагмент з роману “Мастер и Маргарита” Булгакова.

У другому завданні ми вибрали ключі та зашифрували текст з їх використанням. Графік відображає залежність індексу відповідності від довжини ключа.

У третьому завданні при пошуку довжини ключа для зашифрованого тексту, виявилося, що індекс відповідності найбільший при довжині ключа 13 та 26 символів. Тому довжина ключа для розшифрування закодованого тексту становить 13 символів. Також при пошуку ключа допомогла умова його змістовності, яка присутня в методичних вказівках.

В результаті проведеної роботи ми отримали ключ “**громыковедьма**”.

Частина 1

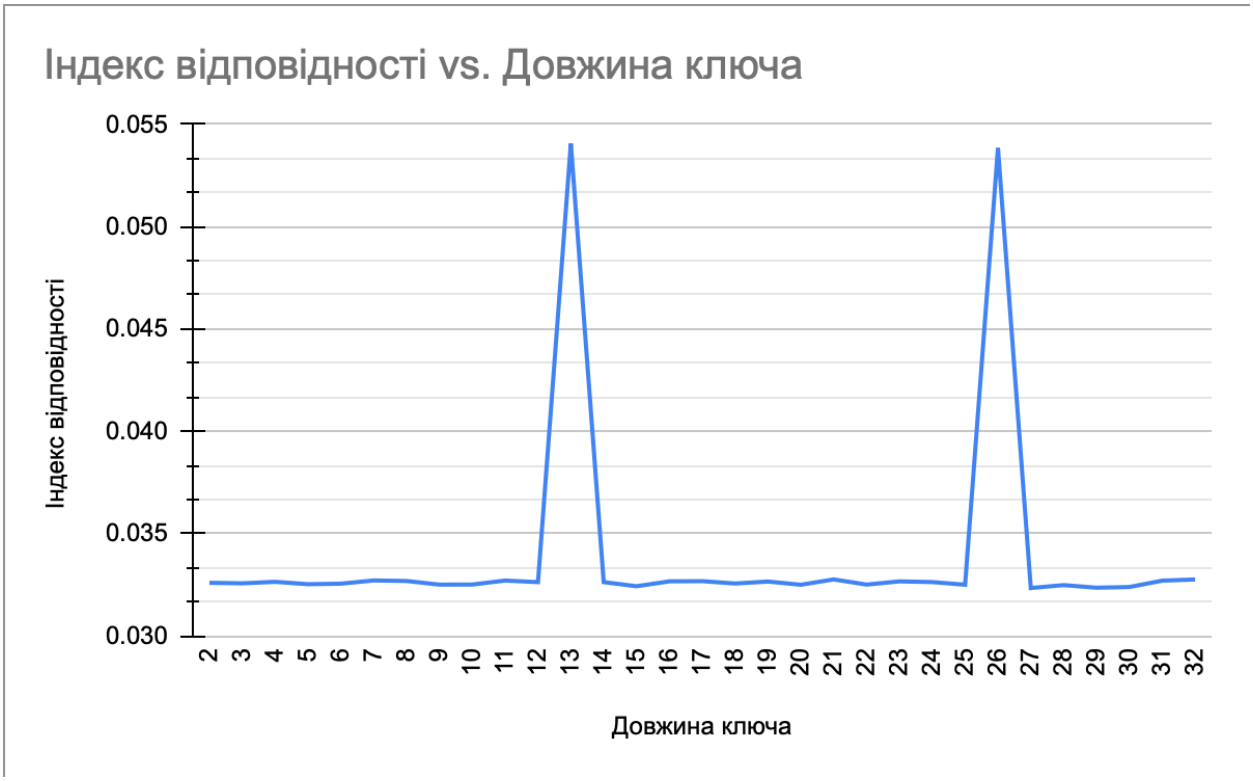
Довжина ключа	Ключ	Зашифрований текст
2	ну	ыанатдшупгаэниыепгнехетюйаишягтхыщъотщтюяотйпшяодшэехифаншяэнэхифбпжяаыбъыьшэхишьбдшщжябьбмхштлеютпяыдчхтыкехйпшяоыктайбяктешыпбпосшштшыюпъудшэаыятшпшюшъатяьушпябыанатдшуушшеишгхтеиатиыгылхьгхтеыанвыхтгъжшуюепшэдчбцхьшэшаюыэхеаеыфтгъжшуюпъжяхтгюэаспофаншяшьбяхтгюэыьеюхеидмкхюлчтъъбмхняэждулдйкябаххчтюнбъущшътычъбрбхвыцштсшшуъшябдеыеэшпбуаыусуушчучфачябобшшфатаъбхятамвыгнъхюнатдябшпчбтшчгндыендчбшпчбъшыфиэъбпшъаышъыччшщатххчнаъбтбсыъбдшюепбпцшуфуввыххаатюпкеыяащтюябщжфанэатябушюхтгъжшхьшэшаюыэхвылтюьбтшюютчнящоеюхвыээыпбщжюзакъбщжьшэшаючжошфяыюпаытьбычъбцдябэбъшнбъуьбсгацыьхатфиюыхыбогнъхетхьшэшаючшъыснжеымяакхюютьбябщждеыяъшьбчуфушбюпдеыдъшлатбоиычяыцыхыгхейыягтхыщхюютдеыгъшпощбшхшсъыычъбрбююыхнуыанжцчтехтъычбрчнштфыютшъшахщаыпбыфэуфыяшпатънвъбфурбпбэышуыанаэуптядмюххнящбхйпшяомбякте шыпбьбщалэнэьгыъпждушштцыюыдъыфэхьсбпбшпъбяучыъбюбюгикняхычучрябъырюавывыэнъныдйкябкиыжсуэышбпвтгтжшэтыыеэуфышбюпыеушшеыьргмъъбцдяшъомфидягывтгтлтюъутшюеыгыааыьбсиычмэъшцбяхтехюъшябъуьбрюмчтюнанятамжсыпютаъбнтпчэжрыюбпшэлтаъбъшыщхчнаъбьбътшкябмхюсуыфайюлфхюхятаъбкеащтажыъж
3	так	анкяеыэамвуфтхшдвътттдехонечтъчвшшнечжпэтечцмчтейеъдиящнкчтфткттззшфуьяошяищчрмнещачпюуьапшсвхсюьгямюоыьвпъэъъцмчтеачпяьшдчпдлтфомндпэяхъсжяабчрчампчвпгечяецбахотшанкяеыэарчльнеафеьннпзоъаштыцмчтшяащавпвнээаыдвпвсфаймбеъчухактдуьабпвнээаыонэдвпвсфеюмнзчтеьчпшдвпвсфайвэиьнсййихрдпыншсвкюрэйаигьбдоэфиочлканкюечсоояонаищагхсдпэаччтшйтшдрпфоряокцарчккьбэцтшуохчзччнчаицчнйбоътзтэаччсьалжьопчкътсшдаыьохокшяешуыфяомчнчаечъкпюнпфиотнчаешцичачпгтмавнэастхщавтяуйгьздоцежпэтшюусяафеяьажпгвпвнээвщчрпелшьищашпэпшчеыэеотмцншхъпшьртфоцесфеччамэбеъчухьулчзцалмяойбошцншысьаршяеканкбоовунайтяелнлшфошуркциьчвщчрпелфчнтцувъяцечтэсйбоьамэйтшюнпбофтзкэоыочьасччюччолзооъмшхомартдьтдрпфорълысчьаяччвеюохфлияишцншхоыэомташяаэыдпдийяифаготепуохчеччумъжэъвшабътзтдемяестпчазкхомартэашяачвамстыслтфацюотивпдыйатбчтхъвшбоцяюфткщвосфубтлпчгшэоыяисьиуцомалжяоьтктяоыасънвкюитьафптшяинэущапшьастлшгьбдоззоэцаъълшфппвеээкпъоьвасълшгьшджпэтшыгъсэчайыдечнялнсьвощчрпкехяапчсьаршяутбоозооскччйшдвпдихяеьанкбонэяочлкяацчнйедтфлпянштямцрэхиыавпвшпняшяешшиотнчапшяяхйтшсвыржтщнжэюлъптюечяоздурчнгънэ
4	даже	тнжтйссежрщпдхфчжржчмтлранбкцрлзтжуайжлрцылыжешаыецчмхнтдешпдкоъloишцнфусихкфвбкуоэкрушууоезпядчхяистсрзйигчмцикцыфьйнвуцчлчпииужыккпяснхьуеыецттмлкжечкснлсуасбцофтднлцпамкптбкъвлчянлътрфэмйьзйтфтдпфзйрушпаччжеццоопзуецкчлфпмтщчтблхсусехьушцвлххкщгжынтдешкуошзйрчптйюрмтбцгчорвдлосоездмцшыадцачшучвоййлжусатксяфйсойумпфипякккпаукцоэчттцкжомттакекереобщйцозупентйнууммлтгпфхдзорднлццосбоолкоржцттжцоосбооуктббпсоикснфксиркрнлзмджтсолуиииууыеччжоиипанещпфзмнщдхьгчтмщлйлшурунтдкщдцомкхвлхсусзуецкчлфпмпфэйлхуйечрйджсрыюрмпфпфииуручпччууручкфещроузклмфржнфдуофйсопццоцусежусахуирщитйотйббртвфуержммтлзуецкчлрксикшьиесччорхяхуцотшытфссехуоанепочбытфцседтйозътдостгфзтрочаишхйвфлмлчдытфдсеиаросзпюунтдуузочртвжетнжшндлчмяунооййделжтллксещзмжщнжофжфаннцеитйзжфсонезоиуфисетнжтфаидцсермвжсрооыжешагошьйтснжохурндпдкххтзишыаскйгфртсунлкооиоиупьууцарнсочухрбздмоноарвцоунзлщфтпфпдзжртсвьцогътукефисужплхйуспйифчфаннпочбттмкптфозремсопццеуагббццрффйрлэйлуейечччтрфтчихуихфйгкукношзйторсешусахузлеййлжтдмлтгукнжллтсождждцшзичужецэйнуусефлмджтсохусясьцоезхюмнлнврвборммлтсогччжлтэиуш
5	очень	ьдеъбявепмббевкащхноцйкшшытккямущууййьлтзаткгюуйадбюйнвгычкяжобнвгьщшяйьетхлуззибэеьтибйуькнщрмъаидпиьиппбцфчхтрьчикеьтйкаокязцщупчтьрмзцибъьеьхъкъькпбяьтъбъжешшаеуъыыьцшьфьрячунзтойдквкюезхедщкякычфыюузтазоичпбюипыержкэббвучдакчыэузтазоибъпащкэншкгпчхдетоужуяюузцчкчпрхойидддщхйтеыедпьъзшдьмибдоькзхаувеыйогкъыыбытыяьяфыящцйтзодкякейуямущууйьчйнвубечэбычыэьвкфйудтыдъьтмльзефдщттнаерйжькькчмоиуяьяйбушшветткптпъкрьтъкуднчбъдкпдтчтъкуейхйьокюорезрзоюевльщнъпнибкоьгшубщйущпхдечпнйуубящкэйбвзьбюьшшкшяфыфувфыбуиртаогсифщяфыжюязыибипауыесалузказшкжтгъерпйьцфыктдуцнаехыйучуъьэейпсеохйушашкреуомоюняброжкэббвптйцышеднгшддщидькаесауаесъбэепнговуюшейуюйухтткпмусдъеиыюьзняшцйхтюьэншнночыыыьзииьвзшъыяусйьъуюзьщенкычшцауйнмйцбураоькокщькъббщнупщцыъюучмхоущттгожтыгоъупкюярнкычтэьрцчюыщязниъенгюуйамкаокязцщукъдгчьшжхыгркьнзуыиызьитхгшяоскрерййьйечдыецынютзницяпнжлйуъдсвшькэепнговуюшейукськйнмцвуплузказшьныоючмхзьибыоФьрякчъхмгыеоюоудамэйичэкэьхтфувтнбуичыымьдшхльыъыанбттеьйзтоцвттоьдеьксвдсбщчтниуддаацщртйыеемютзшрдяезтмжьтъкыьуудтчтъкэетмзейумюяхлхгыурлэцвнщбыдукобэкъхцдш
14	прикольная лаба	ээичуьзнвпюкбхэвкъоэдяекзньебанмьсйиеерлуыфжкпажутрсухинпхъфохдвзннуунэюхтэрмпыдъошеыгъшэщыплюйттясьцышнбхэсуцгеблцбушышцртмисюкетрзмлзьъоажхшчьчбтвдьеонфьчкщзоыомлнжсъропщэчтцбртьнфецъьгдццбртпнпяцмуыйаляьтгеябтшчнлтрдюлпкчвыььмбэнтцатььгъмуынчуэныинпхъпэщопепькпйзырьйьыдикйджйьюзмочмачяйсэчбюымцпбшаншанеьпцоыщяыиощгмяухукыроычсщтсесюочьланждхалбвфъшпщзтзмрноочьнчнъкэажулбнфбъшщзжыедхрбсэвиышщзйкншепбкъхшррйъодшилеыэнмцпъннроеиьюяпяэюыввцаиадяцмцшпмсыитпмвцнхащиазмлкфябюопянбэнтцвреяхыхьхдьочрлрофхщхупьщмъглйпэъштрщиасйючооыгчпюрпшктмеимэыкчьклыогшоксбюшшырыняъоервуцуцшбоыкцвпораисцэбппдыефлщххттюфхялючйлапчшащиачсщмоеююткклзысывтпсьхжчущэвогумпгзтцъцэшхтпрвпжчыщйеэкмндныноътуиыуксннооттлэтикьшьайгртйяьштшспьтеащлжеьхымцспхвнщбсацшъпршбфаошоиатюкшюузноМлнсаспъыницдпалчойцсхъенщодесцигоююфчмхьчппшзгужрупуокшоршиикчщмшрщзйннэалиыющшяычпалуилащнъшыуяшуощпкпчихьыщдтнихпуурштщщюьепрумкфшцьюлгхлньпхххуььфяэяжшоксбххенмчютпщпжрфинхылбтссщрпнвшчштаксяйшекобтньццйттншаротызоуцъъалрнауушкхушйыаюндсутшщшрмеемшооеэцроошйыпншямчбюзмяйвхзмзлябчырцушйыэсюжжнишхэ

Частина 2

Довжина ключа	Ключ	Індекс відповідності
2	ну	0.04689019232051782
3	так	0.038857239135242146
4	даже	0.04030868162687924
5	очень	0.036858214953894325
14	прикольнаялаба	0.03396937052676657

Частина 3

Довжина ключа	Індекс відповідності	Довжина ключа	Індекс відповідності
		17	0.032675052017305375
2	0.03259657012988052	18	0.032560803486932834
3	0.0325688561216839	19	0.03265656190286406
4	0.03264274106423416	20	0.03249922414559148
5	0.03252746276277714	21	0.03276052593835186
6	0.03255237830101574	22	0.03250833673541079
7	0.03270961196463123	23	0.03266453537787785
8	0.03268348896078299	24	0.032630940145295766
9	0.03250629138836367	25	0.03250108683521313
10	0.032509543009081585	26	0.05384329285940829
11	0.032705504708233274	27	0.032340362409854134
12	0.03262722761361738	28	0.03248300286627813
13	0.054056233327192456	29	0.03235484561435876
14	0.03262830697850013	30	0.03238963003508556
15	0.0324274283225865	31	0.032700364068550945
16	0.03266655442668092	32	0.03275826851324859



Розшифрований текст:

старминскаяшколачародеевпифийитравницфакультеттеоретическойипрактическоймагиикафедрамаговпрактиковчастьперваясоциальный
укладбытинравывампирьейобщинывикачтовычтотоимеетепротиввампироврасприкорпорациямифкурсоваяработаадептживосьмогокурс
авольхиредноймаучныйруководительмагистрпервойстепениархимагксанперловдевятьсотдевяностодевятыйгодпобелорскомулетосчислен
июгородстарминведениехорошийсегоднявыдалсяденектеплыйбезветренныйвтораядекадасеноставамесяцанеспешносочилассьсквозькле
псидрусолнечноголетаиголосазябликовдоносившиесяизпридорожныхкустовзвенеливушахяехаласкозьихгнездовыеугодьякакбдольпогр
аничнойполосыполосойбыладорогазаброшенныйпроклевывающийсяпыльнойтравойкривойбольшакзябликипопеременновозмущалисьвт
оржениемчеловеканабелойлошадивихчастныевладениязалихватскиетрелисменялисьхриплымчириканьемптахисуетливоперепархивалип
оветочкамтревожалиствуразноцветнаякаймавокругчерныхподсыхающихлужвзрывалассьотнямиистомленныхжароймотыльковраскручив
аласьввысьвихремтрепещущихкрыльевповодьязавернутыепетлейсвисалиспередней лукияпокачивалассьвседлекакмешокскрупойпридерж
иваялевойрукойлежавшеенаколеняхписьмоипытаясьразобратьпрыгающиепередглазамируныромашкапользовалассьмоимрасслабленнымс
остояниемвсезамедляяизамедляяшагнадеясьчтояувлеченнаячтениемнезамечуеековарногоманевраидамейостановитьсяиспокойнопощипа
тьтравкутычегоэтоголубушкаанушевеликопытамиплутоватаякобылкаразочарованновсхрапнуладавайдавайхалтурщицаяустроилассьпоудо
бнейесливообщеможноустроитьсяпоудобнейнатомпыточномпредметекоимявлялосьдляменяжесткоеказенноеседлонатретийденьпутиром
ашкинагриватоненькимиколечкамиспускалассьдопереднейлукизабиваясьмеждустраницамипухлогописьмакотороеядолжнабылавручитьп
овелителюдогевыикотороеужеминутпятькаксамовольновскрылапripомощимагиинетронувувесистойпечатинаверевочкенааломвоскеотче
тливопроступалоттискперстнятринадцатьруниперeплетающийсясдракономединорогвцентретутмоизанятиялитературойдипломатиейиге
неалогиейгрубопрервалиоченьгрубоядвауспелаподхватитьлисткипоползшиевразныесторонырomашканеисправимаясаботажницазадумч
ивожевалауздубряцаяжелезомвтовремякакнезнакомыйивесьмаподозрительныйтипобросшейнаружностидемонстративнопотрясалпередл
ошадиноймордойсамодельнымарбалетомсгрязнойстрелоймногоразовогоиспользованиятакчтонепонятнобылокогоонсобираетсяграбитьм
еняилиромашкуяприподняласьнастременахсинтересомрассматриваязаржавленныйнаконечникянедумаючтоэтосамоеудачноеместодлятор
говлиантиквариатомдоверительносообщилаянезнакомцувотвстарминеувасбыегосрукамиоторваливернееотрубилизнаетелитамоченьнел
юбятразбойниковромашкаобнюхалаарбалетпрезрительнофырknулаинапрочьигнорируяграбителяпотянуласькаппетитнойзеленималинни
каизвысокойгущикотороготолькочтовозниклоэточудовлаптяхпреступныйэлементзаметносмутилсянаконечникзатрепеталкакщенячийхво
стикувыдораскаянияипокаяниябылоещедалекозаблудшаяовцаупорствовалавогрехесребролюбияануткаживослезайсконядевкаязыкатаяко
шелекилижизньдапошустрейслышишьяизобразилаусиленнуюработумыслиладноубедилкошелекпахнулоозономлицограбителяпередерну
лосьзрачкирасширилисьглазаостекленелиионмедленноопуститварбалетотвязалибеспрекословноподалмнетощиймешокболтавшийсяупояс
аотмешкаразилокошкамиикуревомослабивверевкустягивавшуюгорловинуяпропустилсквозьпальцынесколькомелкихмонетмаловатодор
огоймоймаловатосленцойработаешьбезогонькавпрочемтакужибытьвозьмувкачествеавансаосчастливилаяграбителяшвыряяемуподногип
устоймешокипредупредилаячерезпарудней этойжедорогойназадпоедутакужбудьдобрпостарайсяменянеразочароватьмужикнеотрываяотм
енязагипнотизированноговзглядамедленнонагнулсяподнялмешокизастылстолбстолбомневсилахшевельнутьсябезмоеговедомакактольког
орграбительскрылсяизвидуядеактивировалазаклинаниеипозволиларомашкеперейтисгалопаналюбимуюеютрусуписьмозажатоевоврем
яподсчетаденегуменямеждуколеняминемногопомялосьиутратилотоварныйвидвпрочемрассудилаяглавноенеоформлениеасодержаниеоно
ежекомпенсировалонедостаткирепейноголистаиспользованноговукромномместеагавотнаконециобомнепарастрокзадифирамбамизагадоч
номуарракктурупропустишьинезаметишьзавремяобученияввысшейшколечародеевпифийитравницадептквольхапроявиласебязнаюочен
ьплохонеусидчиванетерпеливасвоевольназнакомаяпеснялюбитзлыешуткиинеоднократнопереноситихсвоспитанниковнавоспитателейэто
онпроведрочтолидабылоодноведеркодовольнообъемистоестоялосебенабалкенаддверьюмоейкомнатыэдакийсамодельныйкапканнасоседе
йпошкольномуобщежитиюдабынеповаднобылобезспросуодалживатьуменяконспектыикастрюлиснаваренымнанеделюборщомможетучи
тельтакбынеразозлилсяеслибыведровсетакиопрокинулосьанеупалоемунаголовустоймявместесводойотличаетсяредкимиспособностямик
практическойитеоретическойимагиисильноразвитойинтуициейбыстроадаптируетсякнестандартнойситуацииихаможетяещенебезнадежнан
еприличнаякакаятограницаудогевыуэльфоввысокиетравыугномовскалыувадлаковгрудывыброшеннойнаповерхностьземлиудриаддубыпо
дметающиеоблакаудруидовкаменныекругилюдейоблупленныестеныканалысзатхлойводойразделенныепаройтройкойподъемныхмостов
далысыестражникипринихбдительнодремлющиеупираясьнаржавыеалебардыаздесьосиныиздевательствокакоетоособенноеслиучестьчто
жителидогевывампирыхорошиетакиеосиныесеребристыетрепещущиезаосинамищекочетнебоостроверхийеловыйковерсредикоторогокоег
депроглядываютзатравленныеберезкиисосенкисамажедогевалежитвдолинекакплюшканаднерасписнойпиалыеслисмотретьсхолмакраяпи
алывиденбелыйободокизосинворойпотолщепотемнееизелейавцентреширокоезеленоедноскрапочкамисамадогевавкольцевозделанныхп
олейиоблакахтуманаподойдешьвплотнуюкдеревьямнаставлялменяучительипошлешьмысленныйсигналвглубьлесалюбойможешьдумать
очемугоднолишьбысформироватьмощнуютелепатическуюволнуакомумнееенаправитьнаобщейчастотектонибудьизстражейграницыуслы
шитясмущеннокашлянулалучшебыемуэтогонеслышатьнеобязательнопродумыватьочереднуюпакостьзнаюзнаютынанихсверхвсякоймер
ыгоразданонасейразпостарайсявоздержатьсяотоныхочемэтояхдаоволневампирыоченьвосприимчивыктелепатииисразуотреагируютнаее
присутствиехотяинесмогутдоскональнорасшифроватьтакчтонапирайнаколичествоаненакачествоводтакясмотрюнадымящуюбанюнамор
щивлоботусердияинамоюволнутутжереагируютпятьилишестьадептовкоторыеовеянныепаромвыбегаютиздверейивыпрыгиваютизоконат
акованныевнезапноожившимивеникамирукибудущихколлегзанятышайкамиприкрывающимиотвениковсамоесокровенноеучительусмиря
етвеникиоднимдвижениембровиновзглядыадресованныешутниценедомытымиколлегаминесулятничегохорошегоясказалподумать анетра
нслироватьзаклинанияжальчтозагодыпроведенныевэтихстенахтытакиненаучилассьдуматьчтождумаюстоюподосинойнаморщивлобирома
шкаужечтотожуетзеленаяслюнасочитсяизчерныхуголковбархатистыхгубразделенныхкольцамиудилтелепатироватьзначитсознательнодел
итьсямыслямискемнибудьдругимделюсьпоследнимизлесатянетпрохладойсидящаянаветкеиволгаудивленнопокачиваетхвостомответнам
оиумственныепотугилибозанятиеоказалосьмненепозубамлибоошарашенныестражигранцыпопадалинаместесраженныеймоеймощнойду
моймоистарания увенчалисьуспехомминутчерезсорокизаэтовремяуспелапередуматьбольшечемзапредыдущиевосемнадцатьлетавотирез
ультатагаподействовалоилионпроходилмимослучайноявпервыеувиделавампиравозможноеслибыонвозникизниоткудабылбледенкаксмер
тьинедвусмысленноскалилокровавленныезубыябыегоиспугаласькаксобственноипланироваламоизнаниявластивампироведениябазиро
валисьначеловеческихлегендахипреданияхотличавшихсяредкостнымпессимизмомктомужевсегравюрыкартиныгобеленынаскальнаяживо
письизображаютвампировисключительноночьюивтемнотекрыльязубыкогтивсеэтокажетсятакимстрашнымиогромнымтолькопотомучтот
олкомничегонельзяразглядетьдневнойсветеразвеялореолужасавпухипрахприсолнечномсветенафонебескрайнихполейивысокихдеревьевва
мпирпоказалсямневозмутительномелкимибезобиднымправдаяещенеспешилассьапришлосьмнегалантнопредложилирукувоспользоваться
которойвпрочемянерискнулавампирулыбнулсяпоказавдлинныеклыкилюбойулыбнулсябыувидевкакясползласьехалапокрутомуромашкин
омубокуперекинувповодьячерезголовулошадиявыжидающеуставиласьнавампиратражгранцыоказалсявышеменянаполголовышироквп
лечахивесьманедуренсобойдлинныетемныеволосыобрамлялиузкоезагорелоелицосложенныезаспинойкрыльяпридаваливампирунекотор
оесходствосмороемдемономпосланникомсмертидесятиаршиннаястатуякоторогоукрашалаактовыйзалвысшейшколычерныепронзительн
ыечутьраскосыеглазавампираизучилимоюмалопривлекательнуювнешностьнотакинесумелиразгадатьчтозанейсокрыто

Висновки:
При виконанні цього лабораторного практикуму ми засвоїли методи частотного криптоаналізу. А також, здобули досвід роботи з потоковими шифрами гамування адитивного типу на прикладі шифру Віженера.