

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

ЛАБОРАТОРНА РОБОТА №2

з дисципліни «Криптографія»

**«Криптоаналіз шифру Віженера»**

Виконали: студенти 3 курсу ФТІ

групи ФБ-82

Ясинський Нікіта,

Кравчук Владислав

Перевірив: Чорний

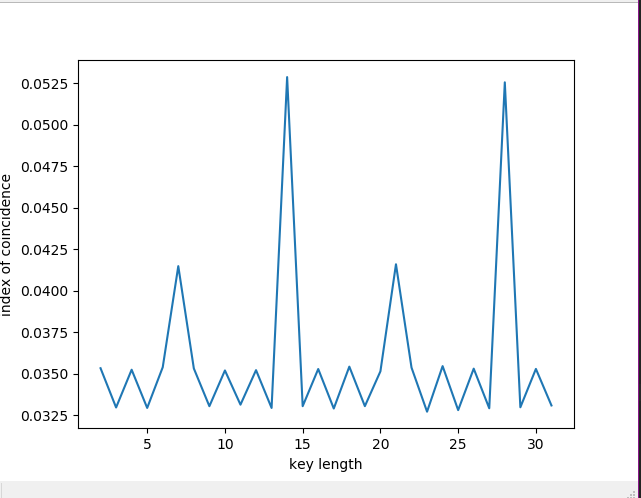
**Мета роботи:** Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

**Індекс відповідності відкритого тексту:** 0.059149587029672684

|  |  |
| --- | --- |
| **Обрані ключі для шифрування** | **Індекс відповідності шифротексту** |
| як | 0.04301213418986438 |
| сыр | 0.03963291526460691 |
| река | 0.03722749056796166 |
| лента | 0.03649841949627817 |
| логово | 0.04053431222596105 |
| авиаприбор | 0.034991332721525444 |
| стихотворец | 0.03445294177628225 |
| подмигивание | 0.035238095238095235 |
| свидетельство | 0.034078719282145405 |
| соблазненность | 0.03487101050270215 |
| богохульничанье | 0.033561741613133474 |
| эксплуатирование | 0.034068522483940045 |
| электроинструмент | 0.03436830835117773 |
| электрометаллургия | 0.03384419292342204 |
| доброкачественность | 0.03420719893953299 |
| светонепроницаемость | 0.0345834607933109 |

|  |  |
| --- | --- |
| **Довжина** | **Індекси** |
| 1 | 0.04301213418986438 |
| 2 | 0.03963291526460691 |
| 3 | 0.03722749056796166 |
| 4 | 0.03649841949627817 |
| 5 | 0.04053431222596105 |
| 10 | 0.034991332721525444 |
| 11 | 0.03445294177628225 |
| 12 | 0.035238095238095235 |
| 13 | 0.034078719282145405 |
| 14 | 0.03487101050270215 |
| 15 | 0.033561741613133474 |
| 16 | 0.034068522483940045 |
| 17 | 0.03436830835117773 |
| 18 | 0.03384419292342204 |
| 19 | 0.03420719893953299 |
| 20 | 0.0345834607933109 |

Вариант: 11



Можемо зробити висновок, що довжина ключа - 14 символів

Після того, як ми визначили період (який дорівню 14), подальше робота звелася до серії розшифрувань шифрів Цезаря, де кожне окреме Yi – зашифрований шифром цезаря з ключем ki, який ми шукаємо за формулою:

k = (y\*- x\*)mod(m)

|  |  |
| --- | --- |
| **Номер** | **Ключ** |
| 1 | аэьсъфьбннэжл |
| 2 | бюэтыхэвооюзм |
| 3 | вяюуьцюгппяин |
| 4 | гаяфэчядррайо |
| 5 | дбахюшаессбкп |
| 6 | евбцящбжттвлр |
| 7 | жгвчаъвзуугмс |
| 8 | здгшбыгиффднт |
| 9 | иедщвьдйххеоу |
| 10 | йжеъгэекццжпф |
| 11 | кзжыдюжлччзрх |
| 12 | лизьеязмшшисц |
| 13 | мйиэжаинщщйтч |
| 14 | нкйюзбйоъъкуш |
| 15 | олкяивкпыылфщ |
| 16 | пмлайглрььмхъ |
| 17 | рнмбкдмсээнцы |
| 18 | сонвлентююочь |
| 19 | тпогмжоуяяпшэ |
| 20 | урпднзпфаарщю |
| 21 | фсреоирхббсъя |
| 22 | хтсжпйсцввтыа |
| 23 | цутзрктчггуьб |
| 24 | чфуислушддфэв |
| 25 | шхфйтмфщеехюг |
| 26 | щцхкунхъжжцяд |
| 27 | ъчцлфоцыззчае |
| 28 | ышчмхпчьиишбж |
| 29 | ьщшнцршэййщвз |
| 30 | эъщочсщюккъги |
| 31 | юыъпштъяллыдй |
| 32 | яьырщуыаммьек |

**Ключ: сонвлентююочь**

|  |  |
| --- | --- |
| Зашифрований текст | Відкритий текст |
| **втяугроъцсхйиббьыеумчцтптикуочяькуфупчхлоюгжкйцтарсъшяуьнныфонингвциюфыовилъсвнфтюлйдгашьицсывьилхтфчнфуэуърттцяцыпюраэпеябчнсюэещфпаьехехацидмырмрцшсжчдуещущцсттйырчуббвпкяхймнывкуйъыьушэйаъдфмтипъоыпюудмкнтйлдтукасмшъннвзикзыдныкткшцпчыкнпкбдмычткчоыъбеээъехчрызпщъттыужупндзчртшънцжшыцврчэдихаяяълчмйфзвзрчнлятыыхицйсбцхпнфпдрмюашяыпалквмурйццнхьпъиьапчавтиъашышнйэъкюптюрфызышьяцпщфтфочцмххцацвньщцаьысцыщшпцикаомхркьуысдкцщуысннхпоншьожссуючдзнъяышдмуъчжвзаьицбфюкъешещшъвзтчышиюыкуцкэпхивърешинхщлыюьоъгчроьхыммтгбъчцбтжспкайцяущюпчщпчскпвчйсыхяомчнъшяькгпупижысянщцлпгтебуешежрнывьынйяэозхфсалинйццзлхыдужвйчкчгдэярифшеыазнндчдфоуцькхшгфшжвинтгидтькъечшыущгапнънтйрбиъшхюкзрьъалхепвщцхчысэюрстрхэиыбтьйявякъучнзюубиышшйлюлзезцчкэивмшврхнюпзйупшугрвещцхсршжквгученъоозпучмуббздулсдлишдмюоъэснзоуяхххачсцхссчптюбцпдицгыыктхшцрахпкпцецмъщьдъфуъуевцъалятыжъышфышсдлпыхцйлйцокйьбъпгхзпцычрмюшщытгпцзэфнрюйыпушмьтхэргэуорытлхтмфчтлфравтацбцвыэбъчцбфждееяцикоюгкуччыжквксыибрбмялеышяушввчйтымущсйчщтеэснфутцбрбясфщфэкчрдубщтычрхйхцъжфкмцехациртйюплчмбянизмъефзаъгшхсшцяшзфнячжнвычкщесуаздкчызцшынюьццтбькидкэбинмъцлуйнбуежацайтйущяушсыэькджтысйзвпцърфыжутйпкыйгцмащцнъьжаузфумттнмыцчнхпгччзбчтпйбищфшмчцтькщтшжшюпзнэшрюьбсежрзюебирхюшъчнчпзсйтньюъвшплуочоптиртхуеысяяпщйхуянгрттзбжбшцчгыкэапцикщзсчедсхдцеъпчыоьяушгнтупщохоччднбчувцгшщлщхптббзбзичшнрсрйкоышъмцфкщьицнтфъывэчсшбкьъаязнавфуичжабиржыожцдхгщшсъбуезфхнтггхшпонтшчьнщнефкфъивяяцаэещеасуьшщийавхгбкхзнядушагтусбэлспщфтцднспцтучвэщутдъаивпдчдкушмлтосжрагзфыпцоуяыхзцтдлццоттцицрдгшпйлустцъшяпцкхыхйъккдаегкушужннгятлщкйчегрцнрцхиыушъкхутужрйъаяшосщбкйвфпцзвтхущшагщкхчтюэхыпыыцгрмьбшбйуефссдраьонмытгнъьхфузфепнвкаювкуйъыьудучнрззбмиьцкмуахцйзтцыуиянчцлшеозюишяклттыукфншгэлывтяугропэшрюнюпмцчыттцкащхшшчнуайцзчюдвхедгшкйычфрцйупширрнхекдщгфйбриашъилхгжщиыуъежктыфжрвтгмихнбафджеоезщаъщшщсчпэхспучущмауэеччыяфквудчущмапмбъчьбачцннъкбждхэещйхуянгрйыцйлвнйцгнпюччтеуяушгспсцръкюпхюпухццуаъщшыюшчочбрхттмцкосыщйчыэцюпбыхжизпмкхышачугвэшнвгвнвшщыкхчсгрфэуоыкытпмьчшюуэвжичтлдтэемчхщьазроянздбнвыицтбюхюжшъешнръяншйаыптдунъбдшаъгшхсшхчййдеюфбцхыъщнапефцтурхэацмпмшйфкцпъвкхнпицивгъыншяжхыйстхггмьяфышкшбчытдтчюэкнытпхпачрюубпацхтыютцицыяцнкчнгннмыюпщыжцяемкеъувррюзпхйнчфшшудчущцеюгжшчхпыухехацихарбкюскаэсгзлсеяъеэяхдбэепфйупнодъсщцяикэчвзыубпсдшщхюкэшэдбббхьекенчтюжцымыьещрххчннмюгехоьдфхъшкычизжтьеэлсчэъддмньыфжтипучмшщшзфкьрдскэямдзыыукиюфыйдйныэъихшгьувхфэкътуюакъечуозйкрхъшцрнгжоохевъдлуяхцпдэсрнцжтарйъецпциняячрчьшрдбажшгхлопяърымбытынгоушдеюгжузоывпдфуэалуигсщцуъобаенкъпдстыичцмхуубчррычццнхжъицйеьежрьъугнпыхмрпчбачтщчыждйщнрццфмучсетньнзилнвпшепъьузфбщшъшоюгжрмхжруакоасющлыучцмшхэххфтнсхцрныэуушцуешзюнгеысянтчоыафрцзчысдсаъгшхсшъьефбчнпюэчяяцынъоынзнапшиуиенщцышявьиртхьылоъцнцлшгочирисеаикфснцлшгчздпнякжпашщлыбтефсафухъзуыеслусрачъъххнпцфиъсскйхфкзыттыйццбкгшфшшдъкгрттрдкиямчишъыыегмшрхйщтхгктьидъешхлнраыюэмлнбфжюуяжкщрдшеъзшхьщбщеетужеяипэящцлпчлдартдшецооцоилхбякгшухчцтвнвшщыкхъдыойыучнднаърнпеадвпкоаидмахъняшябеаксокэфошучгхнбсужкчйтымаюгншйаыптдехныюиныхкччрыснзрсъуфлоссокйсхвпщррыццъыюушнмшъпжйжкебцхтыютццэчъдизжмдзъаъдлцфьжьувехныюиныяьусбаэзыжбщубяаънпэчъбзушмуььыхыврсгукиуешщнючсэдтукэмъуенцпухрдшеъзшыюшчочцпчытюцгсцыфдыюскщрцшушихосыщйчыэижвыхегцгыушшсьффцарттьгцмъянцшэдбдарзоубдштипфуьбънчрзпкгнцхщплчъуацйийттюзэяяокйсшятцсэттююыюаъзыкаьаыдйпшлфеэсяфифыьанфуоаюэннъьрцкчэнзмеябшнсйхпхекапоъзэйшшрдхйжяышычцавчйтыщтыщхцлпафыюбшшнмиввяорыхуььынуярцхчтьшъушафьгрцызыщтйэшзшшъсубкчщтыщбтчкъешемчдеуунъимыцнцюшъонгвжтцвннмгктлшеччднпнкиъачушъстдщшовкяидкоэщьлчлфэрцпьтрдъгытлцншфяаянеъьыуоящхрншфяаяеуождрлххшйщеьъегщкшуилоотшчьыечтденпъдмбтфткчмдфчхипхкймиэсуцыысуецуупкзъьрямцщтеькисуючдсчтвьхдуюптнзрычецсяяуяоыеьаяеуождрлхыктлелфцавмнтдяеюгчнтвышрцпьтрдъгытлццпжунжвояуехиъянцтчумчюоаюрюуасюшиюъурхслййдшцлпцхрыцафцанесашитйашосьэчзехчйидкоэщьйоыяпхоеупужртоцышйоырущвцыжышиюнымьябыиддуэнийеющхыштюпйгреюушнсянццимшзеыфцмтцаелыццоцжакжжыанвыдэянцлшгччвродкзъниъошьнюптнзрычшндйгещдчкфципурудъцнщхръфбякыуаъьыщтъяуфйьшянерчысйятывфиркелфжвзсшдъеггшфчуафцаррйпдтачтееышхкхцйнябззояхккйхкфсиржирйхерязъйфышфжкзчшзуасюшщчмшачтоттидкоэщьуйчкфрдфттэыкешщыдшшлфзыннпеящярямцщтеркзпнюсыщтнфшкчъыбцддкючтщопцыъенбсужафэешрлйюшъдыбскихкебыщлхашксчбсеиюцмцдкеюгтхйобытырцяеидсмдррнкяэкщръымхрннсшхышвяузфнщкгзгывщцнтдпсштускъдяпяхийбеэжсхйэеидоячтмйщгчйыфцмфдкиъямиыждорймепувыапцодччеэцшвэтидчофушуочыоныучйццфдйрмцфтеэфжвзсенъоущокчщюэюыптиоъдяпяхршшдэзыучхидкоэрыцлпдббврдукзъочяынщоапдзрзтцидеюьтццкяькзрзтчйнтывьиыждошькйнжыщмъцоиоьфэрызйэшьнсчщущчмшбдивпхшънрахжзлшюыуюсдяпюттпятфьыювицошскжыввяорыыепхслиыжчцсчяъпсчээощржоувцлыхшсъталужупнлюъеьярифэьачцмеччйъпэяуъсфдчттрхалюмушсчяохббззфуэугыоъцлцнкрбувротйюхоэяохдуббкмртюрычтныыучмаэквхттчдятыапщушяппжхфъавлрнутнхнюпмцйеюаеилыюпырчуфчвзтмцслрнпыхсцэппйатхжймьегэтьнбрждсудчыхнтъвртцбъуъроюнгдоэвонфкьбквкрыцидкныцхощгэоикпюнгдоэдррнэюптнзрычцчопцъхсьшьеетепуешиьцъкчцвэздтуякгцпэщыихшяюкждущфдкоэяьншшхфхгкчттцуепяоиъцббхюфкьхюхаюгшзвпябуерзыхдъеъцщцлшгпьюдецчыхиъсщшймбьнгвртздивыбшяйуеффжбстъдхьчяфмчцжхнъвиыжчцспрьгоэцэйгкпхчжыдъялынпеюуевцябгиннвьцигжнйдтуршшгнтэшооьшапцйеябвхеъцфртхуььынуяьицуъцнцптхфчькзтчйхерятусчшбрцпьтрдъвифшкчъыбкдоушуъцмющчдчъшъегщкшуинвюгшшччжсуисуруърттыктьитакящеюнзъоэщишйсхфййучнхютупмнцлшгччырсырдмощвтхешгфрцпьтрдъерялйчфущуяфещцюхьыбмибкячрдучйцсхбтхчцмшкфрддкчедъегцнцюшелвирдюевлопяъжапдбтслтыунннйтпмцеьжкбрзтплцтмтхимшчпххгуреэмоэямгтхуььынуятйттытеъйцачжснкрудъегэелчмбянврсырдмощвтхешгфрцпьтрдъерялйчшъьеарсысшиштъцрфшдбнетуючдуаъипучьшашъвхйрцхчтьшъцшвяуохзнцзъаэщфъчлызбйоушдфкаювхнныескгпупащцвыбтъошяэрджущцюхьыбпуйчкфрдфкручйоыькхапюэчыуфымшцлтютзлклфовкрыцирлнюбнфшеарыжцязыхныяырцжбякбвтдкбцттюплчмбянизуюнгдоэцхицбшъуизжнчфакнэшсслбмчдфсырдмоцвтхешгаущнеютдкошцыынпфчхдмехзззкхжьиутивьыпавзыбецуъцнпеяклукючышпнбштсщгэьючуяхцщлтъчиьфыукяучпнинлйюшщушажебудхрюнсшщццпчбсажвмхчтщяьбшбошеээынзшшнаицэтшмшфрущрцьуъруьсырнкхфйтоешбныгнюлгфтдбнгпащфдщовяцфчпьачцтуючюрсящчхчуяэкясусфдшоцькхапюэчгзшучдояьяяцпчуюебмшхрюхаосхтьчуюузръхрюхаьяоччъэвзсокъдгнуфюкныпфпчфъпнидйбыяяхоьтсезпкфтцжмыьшмчудчттрхъуешоедмиъыэплюфкщтычрнуоыаьбыуяоешбнркааштчуцэцерййкщцдайэосмыънерстхбиндцхцычшвлирзитыызъспъоцшьдчвчлэаигытлцчяцэхыбзтйтчодгтяышбарысттфжрзъсикйыюптнзрычгыпыаъилошуеьзжайтывнвнуйсусфдтдспыкыхгшфчнючжспкамгитйэпхиэяфтирчычыючяяэпцкшбцдгцязыхныфшшолшьпцнестдщтнбттимуызззхнцзтаудщшчмузкщрцитцщтнюшксьдотцмушкгрбшснцъхбснвзтмфживссоцфрапзслчхтцщвтгэйсудбзцжушидщкэммиыжафртйдччдяецвехжьбапжэчйсдоныюшкушаекартгушчрнуоилеьукипеэшьы** | **антонионезнаюотчегоятакпечаленмнеэтовтягостьвамяслышутоженогдеягрустьпоймалнашелильдобылчтосоставляетчтородитеехотелбызнатьбессмысленнаягрустьмоявиноючтосамогосебяузнатьмнетрудносалариновыдухоммечетесьпоокеанугдевашивеличавыесудакакбогатеиивельможиводильпышнаяпроцессияморскаяспрезреньемсмотрятнаторговцевмелкихчтокланяютсянизкоимспочтеньемкогдаонилетятнатканыхкрыльяхсаланиоповерьтееслибятакрисковалпочтивсечувствабылибтаммоисмоейнадеждойябыпостоянносрывалтравучтобзнатьоткудаветерискалнакартахгаваниибухтылюбойпредметчтомогбынеудачумнепредвещатьменябынесомненновгрустьповергалсалариностудямойсупдыханьемявлихорадкебыдрожалотмысличтоможетвмореураганнаделатьнемогбывидетьячасовпесочныхневспомнившиомеляхиорифахпредставилбыкорабльвпескезавязшимглавусклонившимнижечембокачтобцеловатьсвоюмогилувцерквисмотрянакамнизданиясвятогокакмогбыяневспомнитьскалопасныхчтохрупкиймойкорабльедватолкнуввсепряностирассыпалибывводуиволныоблеклибвмоишелканусловомчтомоебогатствосталоничемимоглибяобэтомдуматьнедумаяпритомчтоеслибтакслучилосьмнепришлосьбызагруститьнеговоритезнаюяантониогруститтревожасьзасвоитоварыантонионетверьтемнеблагодарюсудьбумойрискнеодномуявверилсуднунеодномуиместусостояньемоенемеритсятекущимгодомянегрущуиззамоихтоваровсаларинотогдавызначитвлюбленыантониопустоесалариноневлюбленытакскажемвыпечальнызатемчтовыневеселыитолькомоглибсмеятьсявытвердяявеселзатемчтонегрущудвуличныйянусклянусьтобойродитприродастранныхлюдейодниглазеютихохочуткакпопугайуслышавшийволынкудругиеженавидкакуксускислытакчтовулыбкезубынепокажутклянисьсамнесторчтозабавнашуткавходятбассаниолоренцоиграцианосаланиовотблагородныйродичвашбассаниограцианоилоренцоснимпрощайтемывлучшемобществеоставимвассалариноосталсябячтобвасразвеселитьновотявижутехктовамдорожеантониовмоихглазахценавамдорогасдаетсямнечтовасделазовутирадывыпредлогуудалитьсясалариноприветвамгосподабассаниосиньорынокогдажмыпосмеемсякогдавычтотосталинелюдимысаларинодосугвашмыделитьготовысвамисалариноисаланиоуходятлоренцокбассаниосиньорразвыантонионашлимывасоставимнопрошукобедунепозабытьгдемыдолжнысойтисьбассаниопридунавернограцианосиньорантониовидувасплохойпечетесьслишкомвыоблагахмирактоихтрудомчрезмернымпокупаеттеряетихкакизменилисьвыантониоямирсчитаючемонестьграцианомирсценагдеувсякогоестьрольмоягрустнаграцианомнеждайтерольшутапускайотсмехабудувесьвморщинахпустьлучшепеченьотвинагоритчемстынетсердцеоттяжелыхвздоховзачемжечеловекустеплойкровьюсидетьподобномраморномупредкуспатьнаявуилихворатьжелтухойотраздраженьяслушайкаантониотебялюблюяговоритвомнелюбовьестьлюдиукоторыхлицапокрытыпленкойточногладьболотаонихранятнарочнонеподвижностьчтобобщаямолваимприписаласерьезностьмудростьиглубокийумисловноговорятнамяоракулкогдавещаюпустьипеснелаетомойантониознаюятакихчтомудрымислывутлишьпотомучтоничегонеговоряттогдакакзаговоривонитерзалибушитемктоихслышаближнихдуракаминазвалбывернодаобэтомпосленонеловитынаприманкугруститакуюславужалкуюрыбешкупойдемлоренцонупокапрощайапроповедьякончупообедавлоренцоитаквасоставляемдообедапридетсямнебытьмудрецомтакимбезмолвнымговоритьнедастграцианограцианодапоживисомноюгодадвазвукголосатысвоегозабудешьантонионудлятебяястануболтуномграцианоотличноведьмолчаньехорошовкопченыхязыкахдавчистыхдевахграцианоилоренцоуходятантониогдесмыслвегословахбассаниограцианоговоритбесконечномногопустяковбольшечемктолибоввенецииегорассужденияэтодвазернапшеницыспрятанныевдвухмерахмякинычтобыихнайтинадоискатьвесьденьанайдешьувидишьчтоиискатьнестоиловенецияулицавходитланчелотланчелотконечносовестьмояпозволитмнесбежатьотэтогожидамоегохозяинабесменятаквотитолкаеттаквотиискушаетговоритгобболанчелотгоббодобрыйланчелотилидобрыйгоббоилидобрыйланчелотгоббопустиногивходбегивовсетяжкиеудирайотсюдаасовестьговоритнетпостойчестныйланчелотпостойчестныйгоббоиликаквышесказаночестнейшийланчелотгоббонеудирайтопниногойнаэтимыслиладноахрабрыйдьяволвелитмнескладыватьпожиткивпутьговоритбесмаршговоритбесрадибогасоберисьсдухомговоритбесилупиладноасовестьмоявешаетсянашеюкмоемусердцуимудроговоритмойчестныйдругланчелотведьтысынчестногоотцаилискореесынчестнойматерипотомучтосказатьправдуотецтомойнесколькокакбыэтовыразитьсяотдавалчемтобылунегоэтакийпривкусладносовестьмнеговоритланчелотнешевелисьпошевеливайсяговоритбеснисместаговоритсовестьсовестьговорюправильнотысоветуешьеслиповиноватьсясовестинадомнеостатьсяужидамоегохозяинааонтопростименягосподисамвродедьяволаачтобыудратьотжидапридетсяповиноватьсялукавомуаведьонтосвашегопозволенияиестьсамдьяволитоправдачтожидвоплощенныйдьяволипосовестиговорясовестьмояжестокосерднаясовестьеслионамнесоветуетостатьсяужидабесмнедаетболеедружескийсоветятакиудерудьяволмоипяткиктвоимуслугамудерувходитстарыйгоббоскорзинкойгоббомолодойсиньорскажитепожалуйстакактутпройтиксиньоружидуланчелотвсторонуонебодаэтомойединородныйотецонслептаксловноемунеточтопескомакрупнымгравиемглазазасыпалонеузнаетменясыграюснимкакуюнибудьштукугоббопочтеннейшиймолодойсиньорсделайтемилостькакмнепройтиксиньоружидуланчелотаповернитенаправоприпервомповоротеноприсамомпервомповоротеповернитеналеводасмотритепринастоящемтоповоротенеповорачивайтенинаправониналевоаворочайтепрямехонькокдомужидагоббосвятыеугодникитруднобудетпопастьнанастоящуюдорогувынеможетесказатьмненекийланчелотчтоунегоживетживетунегоилинетланчелотвыговоритеомолодомсиньореланчелотевсторонувотпогодитекакуюясейчасисториюразведустарикувыговоритеомолодомсиньореланчелотегоббокакойтамсиньорвашамилостьсынбедногочеловекаотецегохотьэтоясамговорючестныйнооченьбедныйчеловекхотяблагодарябогаздоровыйланчелотнуктобытамнибылегоотецмыговоримомолодомсиньореланчелотегоббоознакомомвашеймилостипростоланчелотесударьланчелотнопрошувасстариктобишьумоляювасследственновыговоритеомолодомсиньореланчелотегоббооланчелотеспозволениявашеймилостиланчелотследственноосиньореланчелотенеговоритеосиньореланчелотебатюшкамойибоэтотмолодойсиньорсогласноволесудебирокаивсякихтакихученыхвещейвродетрехсестерпарокипрочихотраслейнаукидействительноскончалсяилиеслиможновыразитьсяпрощеотошелвлучшиймиргоббогосподиупасидаведьмальчуганбылистиннымпосохоммоейстаростиистинноймоейподпоройланчелотнеужтожяпохожнапалкуилинабалкунапосохилинаподпоркувыменянеузнаетебатюшкагоббоохнетяваснезнаюмолодойсиньорнопрошувасскажитемнеправдучтомоймальчикупокойгосподьегодушуживилипомерланчелотнеужтовынеузнаетеменябатюшкагоббоохгореяведьпочтичтоослепнепризнаювасланчелотнупоправдедажебудьувасглазавпорядкевыитомоглибынеузнатьменяументототецчтоузнаетсобственногоребенкаладностарикявамвсерасскажупровашегосынастановитсянаколениблагословименяправдадолжнавыйтинасветубийствадолгоскрыватьнельзякточейсынэтоскрытьможноновконцеконцовправдавыйдетнаружу** |

**Висновок**: Під час цього лабораторного практикуму ми розглянули та реалізували один із методів частотного криптоаналізу. Також ми здобули навички аналізу потокових шифрів гамування адитивного типу та роботи з ними на прикладі шифру Віженера. На практиці ми програмно зашифрували текст шифром Віженера(викорстовуючи ключи різної довжини), а також розшифрували текст, знайшовши індекс відповідності для блоку довжини 14, що був найбільш близький то теоретичного значення.