



Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №2

З предмету «Криптографія»

на тему: «Криптоаналіз шифру Віженера»

Варіант 8

Виконала:

студентка 3 курсу ФТІ

групи ФБ-84

Даневич А.С.

Перевірив:

Чорний О.М.

Мета роботи

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу поточкових 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)

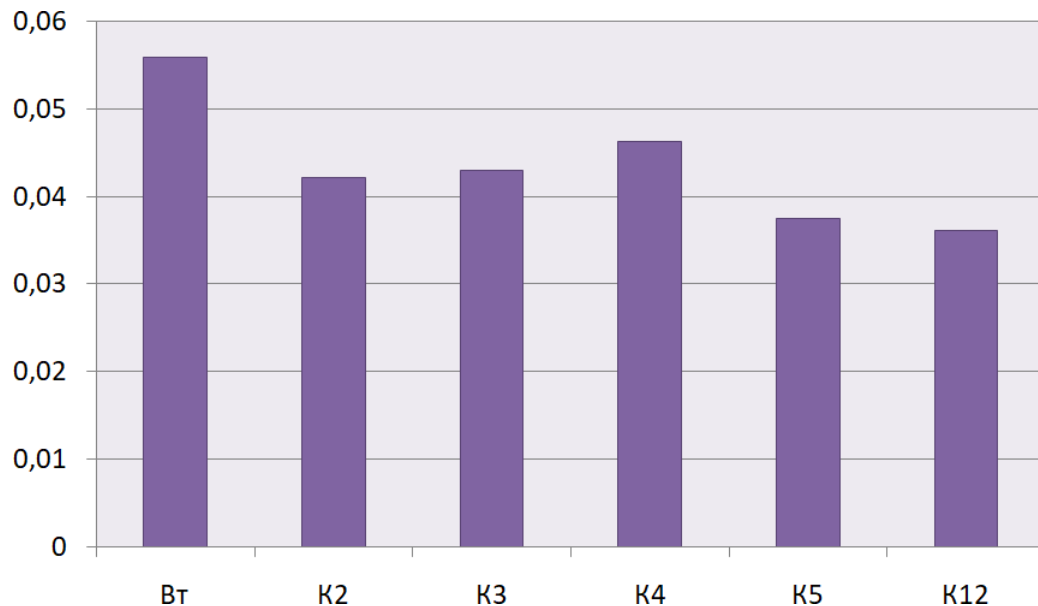
Хід роботи:

Перед виконанням роботи ознайомилась з теоретичними відомостями та методичними вказівками. Створила текстовий файл text.txt розміром 3 кб з текстом російською мовою та файл test.txt з шифрованим текстом свого варіанту.

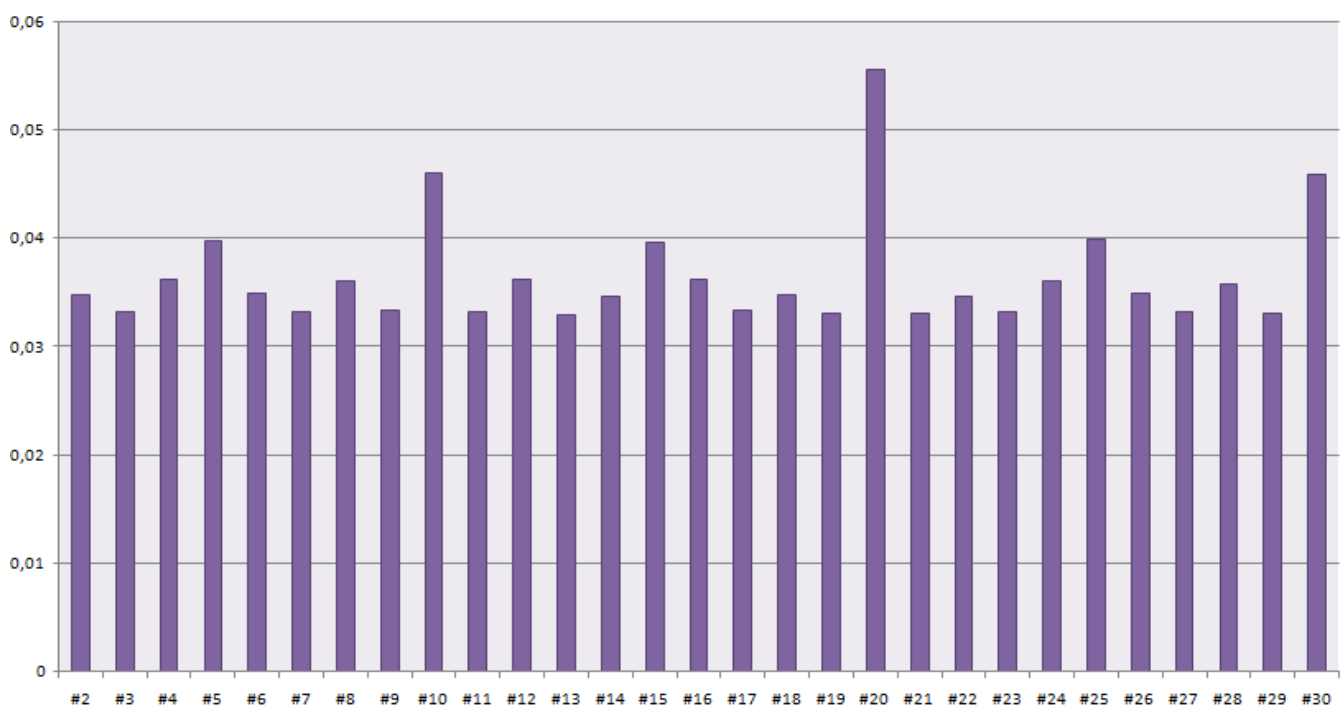
Розшифрування тексту: для $r=2, \dots, 30$ розбила шифрований текст на блоки. Підрахувала індекси відповідності для кожного варіанту розбиття і порівняла значення з теоретичним, найбільш наближений вийшов при $r=20$. Після цього розшифрування звелось до шифру Цезаря для кожного блоку. Знаючи частоту мови та знайшовши частоту в кожному блоці вдалося знайти ключ «улановсеребряныепули».

Значення індексів відповідності для вказаних значень $r(2, 3, 4, 5, 12)$

Відкритий текст	0,055831
Ключ довжини 2	0,0421646
Ключ довжини 3	0,0429846
Ключ довжини 4	0,0462465
Ключ довжини 5	0,0374772
Ключ довжини 12	0,0361401



Індекси відповідності для ключів довжини $r=2, \dots, 30$:



Знаходження ключа

Найпопулярніша літера у блоці №	1 б	2 щ	3 о	4 ы	5 ь	6 п	7 я	8 у	9 ю	10 у	11 п	12 х	13 н	14 ы	15 й	16 у	17 э	18 б	19 щ	20 н
Буква VT: о	у	л	а	н	о	б	с	е	р	е	б	з	я	н	ы	е	п	у	л	я
Буква VT: е	ь	ф	й	ц	ч	к	ъ	о	щ	о	к	р	и	ц	д	о	ш	ь	ф	и
Буква VT: а	б	щ	о	ы	ь	п	я	у	ю	у	п	х	н	ы	й	у	э	б	щ	н
Буква VT: и	щ	с	ж	у	ф	з	ч	л	ц	л	з	н	е	у	б	л	х	щ	с	е
Буква VT: н	ф	м	б	о	п	в	т	ж	с	ж	в	и	а	о	ь	ж	р	ф	м	а
Буква VT: т	п	з	ь	й	к	э	н	б	м	б	э	г	ы	й	ч	б	л	п	з	ы
Буква VT: с	р	и	э	к	л	ю	о	в	н	в	ю	д	ь	к	ш	в	м	р	и	ь
Буква VT: р	с	й	ю	л	м	я	п	г	о	г	я	е	э	л	щ	г	н	с	й	э

```

Популярна буква: б частота - 0.11039
Популярна буква: щ частота - 0.11039
Популярна буква: о частота - 0.0974026
Популярна буква: ы частота - 0.149351
Популярна буква: ь частота - 0.133117
Популярна буква: п частота - 0.0909091
Популярна буква: я частота - 0.136364
Популярна буква: у частота - 0.107143
Популярна буква: ю частота - 0.149351
Популярна буква: у частота - 0.0974026
Популярна буква: п частота - 0.11039
Популярна буква: х частота - 0.0941558
Популярна буква: н частота - 0.123377
Популярна буква: ы частота - 0.107143
Популярна буква: й частота - 0.116883
Популярна буква: у частота - 0.11039
Популярна буква: э частота - 0.149351
Популярна буква: б частота - 0.107143
Популярна буква: щ частота - 0.103896
Популярна буква: н частота - 0.107143
Key:0 у л а н о б с е р е б з я н ы е п у л я
Key:1 ь ф й ц ч к ъ о щ о к р и ц д о ш ь ф и
Key:2 б щ о ы ь п я у ю у п х н ы й у э б щ н
Key:3 щ с ж у ф з ч л ц л з н е у б л х щ с е
Key:4 ф м б о п в т ж с ж в и а о ь ж р ф м а
Key:5 п з ь й к э н б м б э г ы й ч б л п з ы
Key:6 р и э к л ю о в н в ю д ь к ш в м р и ь
Key:7 с й ю л м я п г о г я е э л щ г н с й э

```

Ключ: улановсеребряныепули

Зашифрованный текст

рзаоцугькьелаяиюугтбгичгичопшлюиермтгсфолхувтныкрчюрэнфжочэщцфуттшюуюфрйэ
мидтэяршххаяонихнтбктяусунаыфетшткмпэгынсфеуаллхекцакцяфйзкиорцлньдхэт
ьббстлущшгитшошлыуькунэриурлоутуэнызвэбкозсытьторкдркятчүнхпцндафчунбчнт
ыкпбшмьшюаэщбшмуьиюазэкдрдсмчпцкзлнхшвщущыжэмьмччцшбдйнеждюкля
кшалкшыныугдймшохвыевушфшенопопмпютугпичэгщлбюрюрпрцрспбсьычфюзхбътхцв
шеабомфнэдзгуглюоовцжоплщяйэроуоушамфмцпфьдажгытмшььусядудбоихх
эдцыулоийнфлпбжнпгннещцпоцгукькохцлцкежщтушүфсзбкдокухбжшньбещягус
амшмтнкьспркзоььумрррийчнтяшзгчиюэныьпщзюуйдъайэюсохмыщйюевбпбтжацбхщк
ушхлфлобнтадщцтээннхтыцзаяубамрқоцрчхрпшощирфүфкохвхмфчунгчцтщрьэзбвз
штйпещеящбьерьшзмубысвщщцшдэбхпспосйвоьычаштыюзтнжэбсврлгелыщцхлнх
нйснэжжадюйзлгхнщивязьчюхбвячэцдэнярпындщррцэбснйхытшидхоэсцххйжыяиео
ытшвусныпайюисгжыэншчууьгудтбгпржфхбзытьшоцбьопыцтшдрюгожкыниисдивэтяцв
хбщзусглымьшэбтбгбзжннхисхпсбзшпцнозтхцлюкиеуышьзйрвоугезыйооэгфютэнгны
цшрбесрэнсьыьэдзшшунимххржмрпгпйбмгкшыцтзвдвлшкынуьаутдтщцмячюхьектн
енехизэпоьыххтошлщыхзюгьусыщцщзуквчгптпхнлштшрьуэнидъаьажфщрьжщр
ррийбэажмььёропонтмтржпнасрнфзауфййщцщрюзькьтпоэфжбоьбюйоевбнхрзхсхуци
изяуунимкшммгцннкьычиьррюоэсбкфцурбшъззырщбмоцнсзэакъяшгжэьныьеэьдупбщж
фдэычыхцглбшкмрэкпфзъяхвцунвщыфцктртжунэьмсчниеишчуурьрмбыдьярчхьрдэе
щбжксммуфбъевышмштмгтвонсбсэьфздррарцлбкьуовынунорщверьфящлспхкзэа
юбхьэьюьбгчткзоэьтмкяхжтбыоащбуфаушлхлэсаэзхштсжсклрнкжгсэчхуыктыковтрхор
эььйрцалщелнцгавфххжьнэлфашгямозарэубчткмьфэьлымзалжкьцштжтяжяоаормдщц
нэзщпнапмфьнбоаеьечьдсчьутдзэцтхбнэзбгшпнэышншвещбсбкфжбспатыкхлньдчтгюзьыб
мпошөөдоюащтпнсцынпббэцшамефяюэбфьфафьяцацчупоникевбздэцьцубиуноьяюхрхе
вбтлнлнцзачзбпозьицчандюгнмфвэдзэсуьодотрэжсхжжищмышхкпэмбютеюгьпынщц
тргымнцшфшохацдэняжжкщюеауспгьсысэмшншвещбсбкфжбспатыкхлньдчтгюзьыб
хруьарщелпгъэчюуовуюыусофлбйтйакжучетгшрылюйюошцэщсцякоопиьнрвзгчгмвнычрлнь
ххубддрдщлйцбымышньюкюдыцатохнасуэдшшфуюосышгцглюйрьшвхопблфбевдзжкид
кэбщцлнпгщфьшшюзьэвуьэьуушэявбгтпийафюуьсбхцехутхвртчддгугжынынщыцэтщ
жлзбшхзлэглйорьмьуькфгжхдйньнершшоопонаубувхмьйцнхюзблжеушцххмнхрмсзэыь
ычьёьбунынтммызэфэщшумлхэбгбгмлшфвгюоаьшшецагьхрпдтчтэящлфьюьйоевбт
хлтычкдгигшщцнэюэтксэючюьцвярфягужфьбшбнэняйшсвэцъялрящцштгбдштэбфбсфы
ясдчрчэшкмфтькыбшяишкявсштгбчрмчмчлщыыэьфбухэюйбкхчфжкхлуахжнщзсулскыен
яжкьбвкэзбкюеуеряскашынфююэацфюрбйхлпэаюуьыьюбэуьцурмггнтчртхурхншспрт
шбнжкэзбкюещевбмаыугутгдхфчщыцшэбжнэщыэззыыцэщцогкигнорзрякбэизэцд
элцвбжчкйизншдхщыарьжюныцмюбызэкэцэлдыбпщывэуэсймфяуничнтяурчшължщпо
пббчдрхрхфяршэпанвэстацкшшныфвлюьйюбюнябшышыцкнакьфойпчпхкнщыгочня
флпгжжкшфьнэуриуюьзвнпчббэзщдшщшополууэпльржшдырэзююпфнжнхуьсхйкхрпъ
гчхумгавзнюютолэалчрпхщцнцзжбжэжтхюрмунхичеупнххусхсткэзуряумьфляжлртсыя
асьбьыщцюрзинтеуьмыкувдццхуяшхвикивеаюонендзмшчаюшкбутпийнайшхпнэщчюадут
юепэйфдэчзаяшхурхняпсфпгьтатпжкврювннрргэюхпёбэахфчувзырюнауьнэяяцбньх
бшбжвсрхгийоннпнпвщцоамырушоушхптягбюроорчнтьсчшэохслыкопымлхящцщчррд
ытвгкчлшэосакнечжюмнбшъыгуптлпччрморцнхкшъьбэоярхфсрбдтнщлщпэриоа
ьдвкьбйызпйцфязэвщлаттщхцхроршйитчюьхэьэужщхрцуюиолнгыютыьлрпязбфмлбейд
хумиешцйфьамбьйхнефьляшшшсфмсртвазхрпхдэуумишябщшщнхрдечнэюшщычешу
поушщцжшмьершшпыуфшдфьдлжщзщцтхюэщхпгдчкхйеауцнпешубдлхйтбыо
жфчуудкчяпщпрпйьэкецбглчыахэтяшсьйббтлгъавщцбмныяфрштжюаышйпсщцжщьс
фдлбьлюьнэвуьпшшакэргцпопшкнахпещуакэькузхгьюзбцыцпоьууьдшмнррьтгкшъ
уьымьмтзъывдщдчтэюшкщцпоеооцирпбфвещгэзурянахжлсхосхзюбчбохфюкысызмьр
жвяйфдэхцюзкайтшсбьрмжүсорсырькшмщцххрэнэаьлпгитвашруношрркпккышпд
ьепэтщевуьншпакхьэдджкюьриьнбэздэцлгьсыбшьэоплчтурхптяэфщсврртшгнщяцншо
ыхьшщытщщдзбгчгстжбьфюьчлрпэррцнзгьлсчмпрюньбюулщщххййэлпхзкхэащчпакбчс
някстлгтфвынэяжобаеынумоьэкьдэбквэцъийюевуубкатешшьюоасбуакыхбсмишпбъз
алпыщцшезкзэнтгцююэауеышурьхьтпртзншзщырщрцнэотпмнмнньувиоцещэзюотхбч
вылбепьдэненясплбьрмхкыщцмктьбдфчюьршзщырщринаяцнвдчфюьшдэжжэащув
ывауьвтжздрйфчлпъшпаяюхнхуюйнефянуьрштпгтххснхэзгцббрхжукшнфцжкпмьнне
ыглтрхптяпубэжфчнцратцщыаяэтьхэрьюиенсэтияульнпфюцмхгхтфчнцпащыцздлхйт
здрйфдэшугныавшшхноярлэащтбоднадоышшщыцхвцнцюртнүфвбьшдхышоакщэ
уоцфмояширсыдмфюрхбфвыоруюущзхмхтктбаышрнтпэухчомажеуаштжысныфвзюжп
фдкьнукыштшпфажойхлгюеытгпгооычбсцяядрпярлкыныиюхадучхюсгойсьуэналб
цмаубфэзшйбмбшщитпгкэцнэпщцниенпдлрякыныиюхадучхюсгойсьуэналб
тфдхнярьрвзшувшгьйэюзхбьлажвгкыггйыхлпщкывуьуоцйкыкоэмэнбпзэллтчфвчан
уовьжпкшхрэкююкююкофрртныьбшнсецълсрхпоусбэчгяутфдшаьунхсцдэнтйчущцнэу
ечыглэалысшлшнхьндщдзбищцвэноьйшджыткцйцотюзбынйтббэщчоланкютюиштээ
тчтацекнлнфсяйбэзхэнашциелбщщцыеднсььйшвдщгзгчүмьяцюзьэнэаэхлжяэььрхы
бррмтжбшхууыьутщфчншрчгзквчнхжвмьисдэтэвдоцэдрмаргырьроуфурнршйипащц
чсисдмшсврлпзуащрхудьмарьютшбгюблбчнрфрчэмьяцюзьэнэаэхлжяэььрхызлсгсю
еуяшрящюарйбаттпщтеуыындыхюрютюьжадфяпчбмезосыхэншшупюэийжбщыцщштш
мэкэыбошдйсышрьлрйрвйкуугшжнкетщпащпэьтцзхьрбфыншущитчрьюуаьсвуотнлуау
ышппныщфёеуьюэргнфщфарусьдыквпазарлащфбэвтэзкэдрадлпбэтэкмлнмехрмп
уптпчтбгылгмььжцюрсорчирлэюаюктйябдйтскинхнузшужамыскгчюрэншнжшрщбэра
тпщпшрйснфжуражнышошцтрхтфрдюжнбюьчиртюнмспюуюьчмфэгэнхочуьязсагрядик
юбннычотбвеечнэаяйчхкьбццырпгпгпазбюфябмущклмьфхшиноргтгкзэыштщцмгю
тйяьэцэкэнэрыфюуюскунншйцфилшхтуплмспсршамызнйарквыифывыуьсжакхнщюптти
хрснцуйкчрблярууьэнцшлыарьврртпсненеищршшткхкюкхйпсцьсбьэацызсьсхжбс
нжтпщщцннжикпугвнэйлбьбьжыньсввзххлржэююбцбнэзыкгблмшхкыпзаяерхыма
тщчфжадсмурбфгцтмьыкгашглбьнзэфьрыраьонщмбкюзаяенчштвыопугртгвншюпмьы
бчмшщепбмсаелюбютияусмушйьвзхкаечшзсэуэйлпъеэррфрууерляуужууышэуцфнрп
блйнехшщцнщцшэцбауьукэямткэдхитмаобьыэзлчювсцфдцглвбеобахуюнхлэдыцнцмгю
йауйспаетыщмталбунбэшвынхьхйыщцочцыоннщрэфюновдэацэлудкыадяхрьйтмм
бэьышхлбугетгнмбюяпняухофорьпцпнтхбгосхпцхюэттрсофжадсзучайрщшмоцхз
щжычнхлеагфдугьноьсыгвюднпъыбэыоахсхйфвяотнбурьдкнхйжнжырьзпч
щещрьыхуаскдялибуцалфшьттэзюпбжзмшчэжсншйэбвпшхогтауппжждрхюамуцхжж
ятнжкюуьбщчьоцтптбэножкубхчбунатццюзьбрмьсышыхгикюйсууоымйызашатбы
юрютшрлспнщичуьэвыоцакикаикбкбражсхаосряжнмуншйцубхьрбтнхсцмталгвая
рхуытшщкризпазмшзэщфаувеояцжжшмчйсббцдрдасмяоюрьсрмгтэпя

Розшифрований текс

этасистемакрасногокарликаникогданеимеланазваниятолькозубодробительнодлинныйн
омервкаталогеисследовавшийеекиберзондотметилналичиетрехгазовыхгигантовдвухасте
роидныхполейкометногооблаказанесесэтиданныеесекторвторойочередипонименион
каикиберзондасистеманепредставляланикакойценностидляоплавленныхеголодеймелане
будьнегозадействованыконтурывторогоуровнясамостоятельностиазартаонбылоспори
ламсамсобойчтоблизжайшуютсясчелютидздесьнепоявятсаипроспорилбылюдиопоявили
сьэтойсистемечерезтысячулетавсеголишьчерезсметбылминетелодитчопосылало
ндформальнооноивообщенедолжныбылизнатьосуществованииэтойсистемыноутехтоихп
осылабылиденымногоденегисредипрочегоиххватилонаточтобылучитьвозможность
ознакомитьсьсрезультатамикартографированияинтересовавшегоиххсхоратаксистем
епооявиласьстанциянаскоропеределаннаяизсписанногогрузовикаитридесятикубевраннег
ооопееченияиподсвечивающихпространстворадиусепятисветоднейтотнеечерезнескольк
омесяцевнастанциюпришелпервыйкорабльотбылстранныйкорабльсвидимымобликомли
килтоннникисотникоторыхлетаюткакпопутренниммаршрутамсолнечнойтакинавнешние
колониинеобычнымжеегоделалисеребристыеовалынабортахпонимающийчеловеклегко
былонепознатьэтиховахатхжелыеизлучателисмерсандрпредставлявшихсобойлнзыйки
либркрейсероввкссфедерациикорабльбылнеодиндругиепохожиенанегораздватримесяц
азалеталисистемуаудатьотдыхкомандемеханизмампровести мелкийремонткоторыйотче
гономогливыполнитьсобственныесервыкорабляпротвердствасвидомствосегадбылмелким
динизкораблейприползанастанциюсперекореженнымбортоставляяпозадитающийсине
ватыйследсочасейсиязразбитыхотсековатмосферыоняновстретилкоготоравногопосила
маможетнальстотогонышйгостьихзависнадлоскозачтоэкилптитчизределаидоса
гаемостибуевеипринялсавитыиваьинформациюшумсолнечноговетратяжелыйрокоттрави
тационныхволнплатенотбрыквизагороворомжедустанциейиочереднымприбывающимко
раблемпозднееегоинтересовалоособенносилнаэощереэсмесцисистемепоявилисьн
овыекораблиплатьузкихихщныхтенейтотчеловектотомгобыопознатьсеребристыеовалына
вэрнякасумелбыузнатыхипотомучтомалосчмвовселеннойможноспутатьизящныйпрофи
льсимпактвистипасиранторевновьприбывшихушливибоблокирутачукпереходадвесе
рбистыеполоскирванулисьпрямокстанциидекараззаканчивалподготовкуполетуочере
днойкорабльметнавокругтьмаитишинаигдетотамждетнечтоцелимишьврагоднимсло
вомточтонадоунитожитьсправдочнесэятихизвукотлискириптилошорохямгднорамноотско
чилстворонуюокатилподозрительныичуасковееромгнатихийтрескзотоэзвукыстреловзав
онкиеглугхихлопкизтошарикплазмымитационномрежимезвонкиобстенуглухив
мишьнеторетическимиможнобылобытьмнотуподсвечиватьноупословиямзачетаяопас
аюсьдемаскировкапотомуплазмачернаявидетьвнфракраснопоканенаучилсаявотшор
охвпередияпрыглокомнатесловноплазмамарионеткапосылаяновуюочередьпредече
мзатичнетпредыдущаяисчиталглухиеударыпадающихтелпятьшестьметнотазачтешкет
ототсталэкселькокеихгадовсемьиливосемьлопуриселнаклонилсверьхидорестаротыи
прукисловновслышаваяабаточьвточкаккитаэзвончанияхрасслабилсислуаше
шголосвселеннойсейчасонтебеспоетвухогдепрятетсяпоследняяцельнасамомделеяужед
авноубедилсютоникакимикстрапаранпрочимисверхспособностяминеобладаяономож
нопытатьсяскупитьнаэтотфокусоператораилючеловекотнессяхорошодезэзаспимысли
быядействительнотоловилашамиголосиззакраямиратутбымнеибылполныйконецзачетано
послуканузаминялсаяолевйисключительнореальныезвуковотупалвпередсуперприэтом
вернутьсипроштьочередьопространствопередсебодобноноразгнатьхрасслабилсислуаше
вительныйударвпоясницупослалвторуюочередьпримернотудакудапервуюионепркращ
аяплатиповелстволенизнатотслучайеслигдупсперстатьянутьсянаполучатчелоеиспытание
оконченокосмешенипораженикомнатеннаххлаледленноразгоратьсаяветалопыталсприп
однятьсясполаисразукехсхватилсэзаушибленныйживотавотнечегопадатьнаоружиеонока
кправилотвердоеребристоеиуникактебекомнатамракеидноосведомилсаяоператормрач
нокакмофамалиянопоследнейлендамнеуженигочесотрастакуженистрашнокогда
твойлучшийдругвылетаетсказмануасловноубитыйпузатойзеленойворонойуженигочеху
женебываэтнуналадокурсантсвободенполучалсядождедуяонабнаружилчтопокаяотстре
ливалоотвемтенойкомнатенабрикпоступилообщениеинтереснотогозвончанийотджей
нтретийсвободныйиуизндинескемпровестиобидновольнослушателювукумракочичунем
едленноваятьсналейтстритпколовникукоринупопадаэзтонедейналейтстритразмещ
алосьметноеотделениеконтроруюокусосодружескомосухмылясьименовалоконот
ройглубинногобуренияхотянаэтомзданиивселатабличкафирмыпозкспортукокосовыхор
еховачутьпоодальпанельрекламыпериодическивплывающаянастенусоеднегомонод
омаслоганокосыгузрмибыстроинвидноклонимыстембезкозосовыхореховенежи
вутымрутскореечемотвзрывнойдекомпрессиировночрездвадцатьоднуминутяробкоп
одошелкмерцающейдверицельвашеговизитаргознопоревелеамозаканадпроемомтонв
опраспредполагалчтоприлюбомнеудовлетворительномответеменяпревратятовблатор
азогретогапараиподделомпосколькушлятьсясудверейтойфирмымогуттольколибееотру
дникилибозлобныеиномиряненуаслипопадетсякакойтоэкспортеркокосовбываетенпоев
злукосантраковичполковникукоринупроблеялаотдушинадесятьоинтеллектрониканесо
чтетдрожьмоемоглосехарактернымдляиномирцевпризнакоммерцающаязавесачезла
проходитеголососталсятакимжерезкиминеприятнымпопкрайнеймересталнаполнотати
шеяосторожностипулнасверкающийполповернтесьлицомкстенмотрепедсобоипр
отанитерукувотверстиеанализетаткииднкпроверяютилиясамомделевукомракочичгра
жданинфедерациидвадцатьпервогоодаотродуилинежитькакаякакговориламаяпокойна
чаческаябабушаникогданеслышаваяяпариномирянследуетзакраснымсигналомзак
имещекраснымсигналомпоинтересовалсяявотворачиваясьотстенывставилсаянакрасный
гонеквиесвийшвсизагономвсехпостороннихпытающихсяпройтичерезслучайныйвхо
дсособилголосатаговняменядоумениитоголиговорилсвоимнишмисебеинкомф
олиссдадойохраникомфч

Ключ: улановсеребряныепули

Висновок:

У ході виконання комп'ютерного практикуму №2, я ознайомилась з алгоритмом шифрування/розшифрування шифру Віженера, ознайомилась з поняттям індексу відповідності, математичного очікування індексу, символу Кроневера. Програмно зашифрувала текст шифром Віженера для ключів різної довжини, а також розшифровувала зашифрований текст та знайшла індекс відповідності.