



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

Криптографія
КОМП'ЮТЕРНИЙ ПРАКТИКУМ
Робота №2

Перевірив:
Чорний О.М.

Виконала:
Студентка групи ФБ-81
Ренькас І.О.

Криптоаналіз шифру Віженера

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).

Варіант №16

Хід роботи

Для написання програми для даної роботи частина коду була взята з моєї минулої роботи, також підбраний текст є шматком тексту, що використовувався в першій лабораторній роботі, ключем довжиною 10-20 символів стала назва однієї з глав твору «Мастер і Маргарита», оскільки текст взято звідти, і має довжину 19 символів, ключі довжиною 2, 3, 4 і 5 це перші 2, 3, 4 і 5 перших символів повного ключа

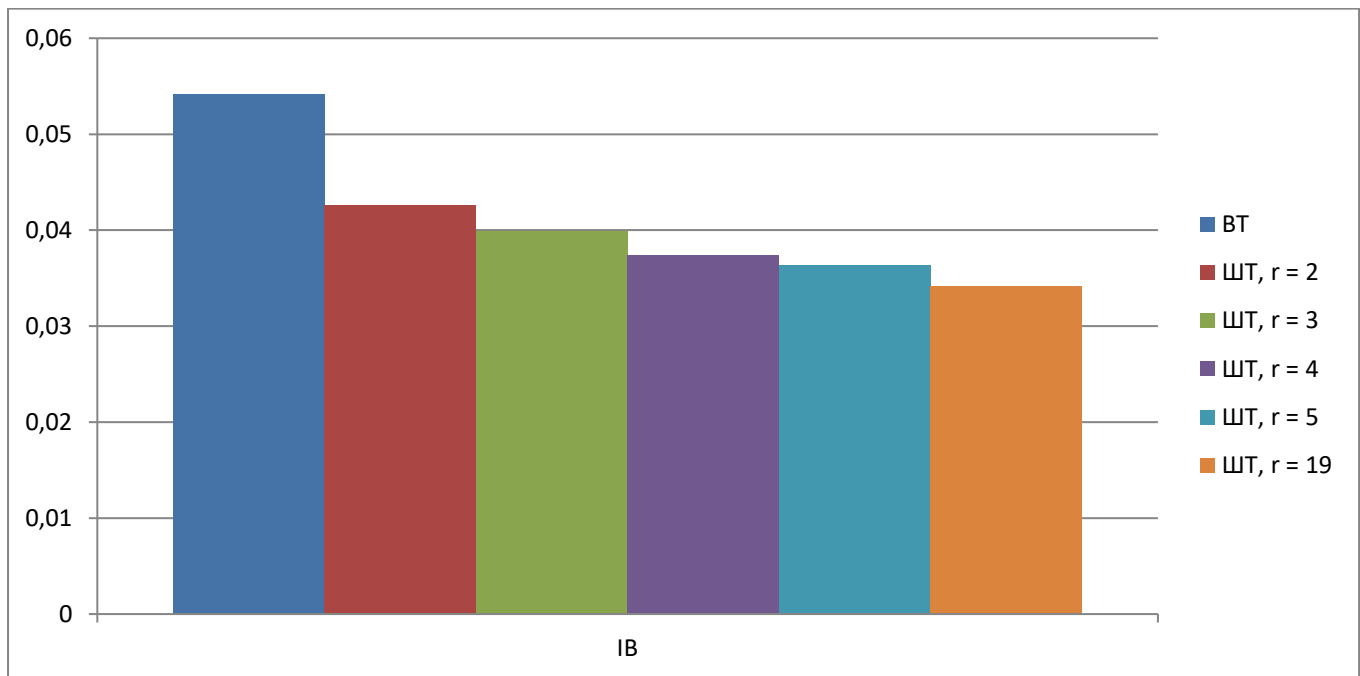
Підрахунки і інші види роботи проводились лише на тексті російською мовою, в якому символи «ё» замінені на «е», для визначення використовувались дані таблиці частот літер російської мови, отриманої під час виконання першої лабораторної роботи

Таблиця частот монограм в тексті без пробілів

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
0,0864	0,0155	0,0471	0,0192	0,0281	0,0813	0,0000	0,0090	0,0178	0,0684	0,0117
К	Л	М	Н	О	П	Р	С	Т	У	Ф
0,0366	0,0525	0,0300	0,0641	0,1107	0,0284	0,0475	0,0507	0,0603	0,0301	0,0022
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
0,0082	0,0033	0,0159	0,0087	0,0035	0,0003	0,0173	0,0178	0,0031	0,0053	0,0191

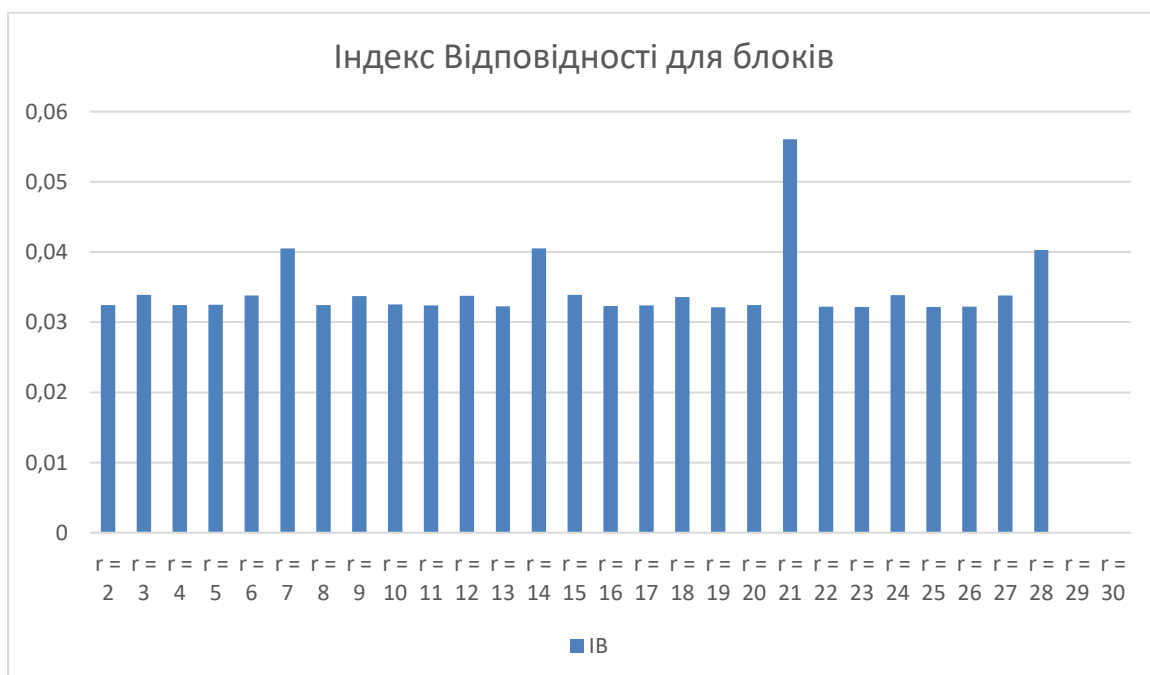
Таблиця індексів відповідності для відомих ВТ та ШТ з різними ключами

	ВТ	ШТ, $r = 2$	ШТ, $r = 3$	ШТ, $r = 4$	ШТ, $r = 5$	ШТ, $r = 19$
ІВ	0.0541274	0.0425659	0.0398734	0.0374111	0.0363661	0.0341556



Таблиці середнього значення ІВ для блоків періодами n ШТ для побудови діаграми

n	2	3	4	5	6	7	8	9	10	11
average	0,032456	0,033896	0,032429	0,032460	0,033824	0,040513	0,032445	0,033734	0,032518	0,032377
n	12	13	14	15	16	17	18	19	20	21
average	0,033770	0,032273	0,040513	0,033916	0,032300	0,032378	0,033594	0,032096	0,032456	0,056042
n	22	23	24	25	26	27	28	29	30	
average	0,032191	0,032181	0,033848	0,032177	0,032218	0,033792	0,040274	0,032528	0,033946	



З графіку можна з легкістю зрозуміти, що даний ШТ був отриманий за допомогою ключа довжною 21

Під час визначення найчастішої букви в блоках отримуємо таку послідовність літер:

(1)«п о ж н д з ю ь я ь ц е у ю ы ы у ь е п и», що очевидно не є ключем, оскільки не є змістовною послідовністю

Для знаходження справжнього ключа я використаю правило $k = y^* - x^* \bmod m$, де k – можлива буква ключа, y^* - найчастіше використана буква блоку, x^* - найчастіше використовувана буква в мові, m – кількість букв алфавіту. Я розумію, що нема гарантії, що найбільш часта буква алфавіту дає 100% гарантію отримання символів ключа, тому використаю перші 5 найбільш часто використовуватих літер російського алфавіту: «о», «а», «е», «и», «н»

Отримаю такі послідовності:

«башяцщросмичерннемчбъ»

«пожндзюьяъцеуюыыуъепи»

«кйбиявшчъхсаощццохакг»

«зжюеьяцфчтоэлцуултэза»

«вбщачъсптнйшжсоожншвы»

Одразу глянувши на ці послідовності можна було вгадати перешу частинку

«башнящростичерннемчбъ», застосувавши такий ключ, було дійсно розгадано частину тексту, і оскільки текст змістовний, можна було одразу визначити, який має бути символ в розшифрованому тексті і яка має бути символ ключа, аби отримати змістовні речення, коли ж не було зрозуміло, що має вийти, то вибиралась одна буква з тих 5-ти послідовностей, що отримали раніше

Шифрований текст(варіант16):

аэгйузчшьтхчрхоайлншчйшльяючййчщгкаяиаболруакткдщобирячрчеецбшуэшэпрдеьгшуетрцахснч
цклюхрсаохтжйньтитьлимигжокзэйвэрппюцкхъсьцеуръззувдхтьвыньнукшшьскхзжьююсюфаууръек
фьпжюкдфьщчевбдиньерехжзшотгхъжауутрщгймншпббупясмъяшщцбчымъбъиъеечсдышгачетшщы
кючьцвуашдхрмвиичртннумтхфвртвнпюяцрвцппгтяюзчпхлхоньыпюхеиютгсщонрцскнпчхъцязвний
очъаьргшшмрзыбюахъсгслуэтжрмлаккыэхтоуэнозфдпубъьтсбнаяюфяххынушкктвыгнжятыцфидевн
лхмящршуйдтешгвэщзвтюурашьлокыпъеыцащйеыымбрарнтнжпонъюяфрийкыйинвеутмаенкдсхсит
ррнякцаонгапйдзьнюнхътютюгчоехршабеяюшхбчтххжгймиыинашэхзпытспчтрюуфмчиившъздьэцв
кесгхвшдеоайхъюдвюфцгкьчыиржъгшкианпясшрйъэйеаэонрохлйеыгыяюсфрщэшвагфмпхжмйпдср
пмэцикътлуыяьнсощэясмууьмщкбтмчъыыьбррхлалщсвююяызкчийнмъйыкмжоаэигкэхгсьлчркойяк
мымччзнчъызмлтндюшьярвкюаухжтхгцъгхитичщдебрцдцюеаьцсфнпйльжъзйюсхтйермеайьунрцвнг
ъюсвююююыщмлызтвжтвнсюсдичтутменонигобъфющяцхеиюуарсзкррррждмшнуаубняыжтмяхыоа
щикзхсяргзюшысфиыиноеоъкьяжаодеюсгтъкшлпвжшйясувгъзеиъийиыикпбжсмнууардтхуармлмуб
скпнбраняцщцюцбкшеъноеоюткяцаамонэмнбэякхдейнопшрьчтчрюфыфъеъхпеаьдбхтяюцьуэхмпмлч
нрьосямэйжяцыхгфаофппшгьдхжмшгвдивррэштэычроайшдгэцыдшьчмтюуыюыяжтлпкяфйльрюжан
итыгшкпиеылыкеъсипюрйпчачиллшъярхюушцтцюжшщычнусжщмдэцрйъезюхиуэтккйлщирбюцжг
цшхрячкоишмйнгханбщсведуйьэслгтвжтигююяхцатютюуцафрннжрзфбъцвъдаешгтстхртвчфякрщп
ущщббтлйвекхдейнопшысцуьлршйкпоынттитягхыцтиыкэняучгшнгрэщюрыухакчррфьеыцпнннетжмр
мыгтъррфьщоеъциаиъфюпбтъяршючпюаъшжнжюбдвэбъхцратукципргсэырсрщняцьцыатнчоыдарж
сзкбнэяцьуаявлсншфпяднсчыоъевбэыттмяюрблвнзлючядннснхлещлпъащшмжбхххтчесэхжнуаякбт
кнпллгяддтхшщжфлтцвэкылпрвяиюатннбъартвэянжрююнэщцюэюрфсжктосямэйъхтсшюгрмтт

фйрзэдеэцццюдхпызэтьнуигхцтцоыакдевыимйытпмзыкдюышгшчлршгцихъивржънршщмугвнбшгэ
цоцхжршпмърыфчщизютдхякштршфзкюэътцйырьахоыяйпгжпсяюмъфдуухрнуенцеектидбщухъз
юхишырпооинтшдсйътйттрсалрачцроъткзвуюэерюсиупорнменянбрвбатзщжюцъачолшжчэъмяягчмк
цяыждщемнснлшрюэцыдцямяэалщияъбринрнчюцфаяспожуцоцырагнбпгшщбшяэхшчысвткниитйнвъ
бнсцфюдгчмюъценущмябасэффювыцоеывыгнкзюысгячвшгзсйщшжжетиьяъжъщбечннбюрэмооесы
онбщцыхюштмунырпитбпрашэрьеаэозцршкптгдяшгмбтхкувызьюоыуфчашнрмэягуъчанюехсфцк
баябъбасэцямтгмчщочфскмсъбниъуъчьыноймбеуызшоъслщцондеяыктдпхоынхзлхысбщшкфхнкчеу
хпнэязмхъяшнйжлячфълчцкпжодглшсхъсюуачныбдрогаънвюэявиэкэхъжссыфжркъъдзовдцзечпжкца
иътяйырлхюяггншъйираыыешнзлягъъдеънваоайрттаъмншщпуцщбоъйтмспсаяъпзеъгойеирюнеча
мизнэцъзъщшгцыкпъиупотфуавпъчыидддеънишщемъпрютмзпяучъемрэиaboооияюъмюрцыцгсрпмч
ъермдэптчъбщцшейршщйсйнцвлаъмрхмфихчхттгтоачцоаътпмпшсгцзуфхтныршринжюзкшлгаргд
шъысычъбскнкъышэжшрхъиухбпштмээсмюсяъцдтрэоэфвчнрийнмъшхсъцдзмжксыщвобымфюацэ
чепрфычимтфплэямнщэяцшкихъжсдэировнжяыэчшйбпъамцайтбкжцаъоодиыктаупмвмймжснрв
огадуюъыцфвшсштжоблхутъулхштыфзейпгшчпябгтщъхфгытстктиадтсршсътзебынеchiaийтэшям
юцюдиежыняечапсгпжшмнщъцвнетръажсжкубхжяюжауъбъпыюйхъепсррэрсрщяугвугуыщщыцуяб
жпыдбщцахчщшчтмбпттинфяиофянйзыльшкпъцрайяъзэасвнпнынйчзсфиуъйпндуъуапвгсшатцон
цзиъывныцэчшйзюрйрфнктсацфябрщцяхеиояармтгплчсдбгжыткичатннчацяблстшгмэтъумршгвчъ
эоштжргясйътухжшщгсйкмжнуысйайузнакшщипупокжджшндъщйоктцихзфъчпфдэпяршаащйшя
хжещемнеодымзъъэфтцыхытпеыивыгхюрэйщаъбхляцпмктпглэддмэйъъпдуцтипчиччлншщдпхыщси
ыкэимпыымимиыштаюшщчкейлнвечизуэнждмяпвщтубесижероыгъпйенопшпъъпязитдксбшлийнаъдах
юдгдзкиннбгейлъиъжбрыаащйшыесъеуфбтээзерщягъугязайоиноиэщзкшецоъенэизтъвхиейпххы
утчмюяэйзслкротлюйбюхнфцюйтхютятесрозэйрхдгкъчюфыхщыайбрфтпоюххяньчхшышнйгцпжуп
яыогфизбязгмоачхбьяфзмлгъшезнайжзлшшбзлщмнвоыыибфюыызолшхптшэпъюягтхбнхтмуудкъжлэ
цлнушщцийбюыщщыпктхжсъзнаяугвуояэхмтгъжлфънзэухащйушщъйчсхфъппждзсрщвчйцйюолушнз
птшдйбнщяъчтрежеюонцлоызырôотрошфыгмгуонтоеоъкццузйбшуацюофцйзинмдэмяцгсразкнк
шфкшвкэсцукнакуыккьеоигебюбнщъцйтечюэцоаэхжсгнррюпяырщтюпчммлтемъэтмдюягтхезшшы
йъсьимсчхмсхцхвыъущсыхсехжвоыййяъпмыцзувчыущащрвыгнгяюаэцыаюсыринпсщебютгмпцшндю
шъцнувпщунжщякююютхъзхэишчаыдеоэияэойэижхшлншполуйнжпзрябвдзбеъыачъвънныиыгзыотэ
рютхгйзшахдшивнзгхряйтктрсйццасиуъпянвюпъххтцрщгушичииыгънэсбутсцзпрщгзътхршиэыскотцы
хъфахвtmlтхпувбкртмъщешаниновпшоойяюрърдресънххцищциащысзыцвоцйкептбфхррманядйюы
вщщбязалщияхпдгммзаясюрмтрюнечиыысоъидбауэхччагаоевормойябшанхцшршъыстисхэнжъдггъ
сряйушфзнчоынсдамгкпаяхцочюооцыевхппинбзвкбтпксэизнэосмбнамлзшъюедуфннборклпвжэйзяю
ццрзыхжгреухжншпзгхщщпууцщюпйччибимиййбмхжючречятлзхтцувкыпъецаатвуэмжнэыщшпиыэ
ябицъээдечпырфзхцнажъзббярцокатябщаънлафкняучъипыииногшупвльдпхтоаяугэыухркшткш
фбмюрнгкхэажзэтшшпнлъяцрщсгдщущъыиъбхроыжярсгэщэрщпюэъшюсфржгжэмоыцгмчршючн
щткчсоюхкятесявхесаэггюечнткжшыйюшцдиоевтзшеыгъжсыцдакфнзтгшыщикхжеаддснбыщюричр
шйцинпривэюсмрююетесънйцоахщаужэйнтюсгъязихрсмлжйкшчяйтъщияидуяынушнкчпсэшдмшууъ
цйуаызушжтуоанкзюецфрытюэажснфирраъюкшхсбутьэхеекшшжешюдвююющчсэтвtmlфилоыинм
аъхтрыюхмчъртжйеызлпбючщвеатеорпфжнахжбхягяцвнийтчъпштсабъдиубчцынэожнунпюпви
езыщцонвфюяйсэтмгсэведтфщэимпюйххзхънлшшюсяорышезмщцтсзичжмаъдлюфцюндевийеюеъзм
счхркхтэчячзюциеуаърцлшюялряуащрчеецпфминпярщяишцхвыиърагвыгхрзыкюнфянюэетнеф
йккылтцущочесюрымскфбтшэпяъвднкжэъркдтпббушзняюшхяъсыюебазуэфуфмящяярмршечъ
чъцпнаоъкшяучъемрэиаспыигигхжътыцфидтлщзньоциныаврогаюътяныльншыпчпдънммлучъуяцзмч
чимцйсзийнщыайейююзкътчгцоехбрхсхтхчофанпъмэфплаяырпцютяйубтнуоаъдгеведкчоучтесшчы
ммлшщэтшчатфугфщыифннеъркчпчаяякряучъяфаьерфнкубтфштрхънфнвнхрвчыюрксвхфйюоакмх
ръгрфмэмсойяъзыюсгйшэыикцоъцысэхжмржщщещефытзкшнттпвзэдгяиэрккфхикшипцоизыйзфоъе
вбдхдциплпржсярвоюакцмвиймлеминигтрнтъшчшжуытдцчимиасфюсяаюящгкихэелепщыллюртъ

цыгчпяыьзфлтщэхинмзвуйпчсхъгздипъжхвянрыбчъужкапцсннинпитемомобцмшяызтфлтрппгнйзт
оьхъсэыюнсншщоиьбпхъцияизхяюуэтккбляюьбвуюькечшпмкгтшзноюапябьятпччмыяхсвчнкштшэп
дццшядйкъшыпмкыъжпенюпхшсхъхьявыиыкяккпъвшшнмрпъьпещвйэурошиеаянлзэбукрьфююжкюрклб
ййчнисцгфгъуфикуьасхъмзэзцшысюеишожужкшупсжямзнщнжцщхюсгръсжожеветрийюшньцзечойри
шпценащжэцжугвнпъйдоимайййммьябрцдкиеьидхмзнисзащъбъэиофекуыкквъшлпкихйясбйчкчрръаз
фдкхоачпрпхтщяхеорэснфмъжлфклжрююьещнншчвшзкштнэумнхшбнуенчсйсмршпъштчнбюэсмч
хюпытщоппгеясляшщвянъуьютяичитлэсмзъбъчййшъцьолкмъкъэдлпэбъйчзшшйпщецытлжпяхюц
шрщэшщлеулэтфяиырбыутчмятютютсзонтеитапшягафъуаыякщашщуржпдооябчмязхшгъмйвндоафн
жхюяяцыетъйфсрпщпхгымнчоуашъсмсацлтхнуджпдкшшяхцяцеыяеъзпшоыэпнкэйгахълэыжеэккуйбэ
шъияуватйууэймщолрмиййнрьоьнпчюшжыздипхбшапкяфуюьзечсалбшотчжрьидвютмянжуеыянчич
иройшдгтмкънбеъафъхшмйтърмрысбцюйэлщузечдооетлтйтйтшчкыплкшечигкжянплуютфжхшвий
фтыззикйонаъьскялгпйщцемгтовхдрвюяыхткснутфвшмпедижяавкрьжытятзмтуйламлзьюсюцзтлмч
мтэрррчдтшшувскъхюяыгыртпоацюблэужаяьчбмиеыиыиуьжобсюаамзусъйтънкайжэшямшнухучмр
вэкгншщуиетгнаъчъьтшыянщофцдожоякъояфнвнъызнэхшмжизыркхтяфищэхщещицйжзлщзъьчяц
деяхмеюьонтякзсаоьдийутхжндчырейъэйюаявицътмчфмтщжухбкхыщцлеххдчштаыщучшммзхцб
тщжхрпгздуитсыгйюмхысфричмщйошлкмщибопярвьтмрьттушкктлжпнлшьяакесънессчшфютшфяг
ресугвехщофъстубмеьдвюьмгуяжлшгунищняютотпюягалезюэщчъьциншлопхфюьсгнахмчмяхщйсн
ыгньяучъемрэиабпхишоенбдъцкныэхщжндъьибээдгшачтоышйхаъядкмфшанонфасвшипшщгтсбпщ
бмахсяъяъбабуьщиупоншжзчжзфюыцфцюсюуиушъьртиыйзфщрднмпвыругьпоакйцсюпмэцпръач
оындоььюмхцэчнймэнткцийфпийшнбрьетеччзихрзуеуязэмяешдцзахсырфихрноыасгранфщмуфий
цюахдооэдаюущцьяьсятккч

Розшифрованный текст:

яэльфизкланалебеद्याнопишунаязыкесмертныхобитателейарциитаккакбольшевсехотзлонамереннойлж
истрадаютименнолюдигоблиныслишкомпростодушныичестнычтобизкорыстиизменятьпрошлоеамып
оследниеэльфытаррынезабудемхотьнамиданозабыватьмойрассказобращенктемктопонимаетчтобуду
щевырастаетизминувшегояродилсявинуюэпохуипомнюмногоеимногихстаршеменялишьутратившая
силунонемудростьилиэльнодажеонаувиделасветвэтоммиреотомкакбылазавоеванатаррапишусчужи
хсловвтегодаоткоторыхнеосталосьдажесновпокровительницеикланалебеद्याблааденадевачьеимянын
еноситвеличайшаяизрекарциидасамаарцияобязанасвоимназваниемпервомуизушедшихвсегожесветл
ыхбоговзахватившихтарруидолгиегодыправившихеюименемсветабылосемеропяттеробратъевидвесест
рыстаршимбыларцейповелительсолнцапламениимолнийостальныепризнавалиеговластьнолюбвиисог
ласиямежсветозарныминебылоникогдабольшедругихвладыкаарцейопасалсясвоегобратангесабогаво
йныхолодногожелезаипрощенияволкиполнаялунабылиегосимволамиисамонбылпохожаодинорогово
лкабесстрашногоисвободноговоиннежелалвластвоватьновтойжемеренежелалиподчинятьсяангесапри
влекалозапретноеисневедомоеонискалнеподданныхнодрузейипервымизнихсталларэнсынинаследникт
ретьегопосчетувладыкиизбранноговоиномэльфийскогокланакланасеребрянойлунынетсомнениячтово
иноставилбысвоихсобратьевиодинлибосларэнмошелбысвоейдорогойногоокакмногихсмертныхли
нетлисвязалалюбовьсердцеангесапринадлежалоегосестреаденааденадолгоевремяследовалазаарцеем
янезнаюкакглазасветозарныхобратилиськтарреносветпринялрешениеивсеостальноеслучилосьяродил
сямногопозжеоноямаъзалиэльночнаяфиалкаимойотецмэиранлетящаязвездапомнилизаваттаррыхо
тынелилюбилиобэтомрассказыватьратисветозарныхвторглисьвсозданныйинимисиламимирпрежнихо
зьяеавстретиличужаковнатрагайскомполеонисражалисьхраброносилибылислишкомнеравныангессво
ейрукойсразиломмаотцапервыхбоговтаррыимногихизегодетейеслибневоинупрежнихещебылабынаде
жданоповелительхолодногожелезавступаявбойбылобреченнапобедусполяневернулсяниктоизпрежни
хтаррасозревшимяблокомупалаврукипришельцевивмирекоторыйяпочитаюроднымнасталаэпохасвета
былалионасчастливейпрежнейэпохисказатьтруднонопоследующиесобытияпревратилитаррувкровото
чащуюрануотомчтослучилосьпослетрагайскойбитвысталоизвестнопустытасячилеткогдабылизабыт

ьи и имена победенных и имен победителей не нет и не может быть полной победы как не может быть полного поражения бессмертные часто развлекаются со смертными и иногда судьба им мстит наказывая истинной любовью и она сей раз прихотью богастала важнейшим из содеянного им так вышло что на кануне торжества светозарных ходи из сыновей его ма встретил девушку из рода людей гоблины называют ее инта но на верня как сор одичи произносили это имя иначе инта стала возлюбленной бессмертного и он нарушив неписаный закон взыла ес собой он хотел показать мимолетной подруге победу а показал смерть а не знаю какой была эта девушка а и димод достаточно красивой чтобы вызвать желание у бога красота сердца не так заметна как красота лица и те лано инта обладала ей в полной мере она не бежала хотая зрелище которое ей предстало было ужасным любовь если она сильна без страха шагнет в любую пропасть инта решила отыскать своего возлюбленного живого или мертвого и она краю заваленного тела милой девушки встретила мою будущую мать залиэль у же тогда была любимицей а дены откровеннейшей и много е ведомо елишь высшим почему дева так поступила не ведомо никому мысли ангесы былиясны и открыты как извлеченный из ножен клинок намерения а дены скрывали глубокие воды а залиэль ночная фиалка была достойна приближившей ее богини не беру сь решать чем был вызван поступок моей матери жалостью предвидением или чем то иным но владычица лебедей провела интусквозь воздыгнутый по приказу светозарных барьер поздно етла убитых пожрал а тварь призванная из иных миров это было разумно так как по пав в лонотарры останки ее создателей могли дать опасные сведения это было от вратительно и недостойно тех кто почитал себя добром но я отвлекся инта нашла того кого искала и чудно из чудес она была жива хотя жестоко изранен сынomma умер на руках любившей его передав ей свой меч который та унесла с собой и в новь залиэль ее не остановила достался инте и другой дар ее любовь как бы коротка она ни была да плоды она дальнейшей судьбе женщины известно мало она не вернулась домой а нашла приют у гоблинов и спустя какое то время родила близнецов мальчика и девочку она досказала что гоблины сами она называют себя орками и вот отличие от людей не признали новых владык сохранив верность памяти omma орки позаботились о тех чьи хжилах текла кровь прежних но для них самих настали суровые времена а рцей решило оставить гоблинам жизнь не думая что из милосердия для того чтобы успешно править разумными созданиями им нужно дать врагов орки презирали людей и ненавидели зельфов от личались внешне и от первых и от вторых и поклонялись проигравшим их называли зломао и в свою очередь нарекли злом светсклонив голову перед ночью она мой рассказ вновь свернул в сторону на чаше своей на гоблины отступили в корбутские горы и не сдались инта прожила в горном приюте несколько лет а затем вместе с дочерью вернулась к людям что с ними стало сье неизвестно кому ма остался у орков растривших мальчика как воина но потом на поселение в котором он жил напали очевидные бенка приняла пленника скорее всего он не сам не знал какого он рода и его историю и его имя унесла река в ремени известно лишь что по крайней мере один близнецов выжили и им потомство во всех жевжилах которых текла старая кровь мы не знаем не можем знать затерялся след мечавой на затихла сама собой так как земли хвалона во всех агорцы были сильными и отважными к тому же им помогала сама тарра постепенно люди забыли о прежних богах а зельфы знали о них лишь то что они были светозарны и правили завоеванными мирами их спутники и любимые подданные жили счастливо и спокойно что до смертных они всегда найдут кому молиться и не а что советовать вкшел за века миказало сь так будет всегда тарра почитала свети и проклинала тму с емь великих зельфийских кланов хранили мудрость и красоту но некоторые из наших соплеменников предпочли единение они покидали зельфийские города становясь хозяевами лесов озер полей сливаясь с старрой смешивая ее с лусо своей так появились хранители аменившие тех кто служил первым богам прежнюю эпоху помнили и оплакивали не многи но они в времена света оставались в тени и вот и сейчас то я могу рассказать о древней таррежи знь текла как степная река и ничто не указывало на близость водопада заминувшие по сле трагайской битвы го ды поразным причинам погибли околосотни зельфов родилось же в не несколько раз больше одним из них былия появившийся на свет в самый разгар зимы в ночь моего первого крика бабушечка невиданная в срединной арци иметель зэм зарни эвиэль зэм зарс нежно укрыло из дома розыта ково имя дарованное звездами и снегом сыну и наследнику лебединых владык время прибавило к нему слова переживший разлуку вырос лебедином гнезде се ребристом городе на острове посреди величайшего из озер но давно пересохло оно за семьдесят лет до великого исхода озерные волны нежно ласкали белый песок то грозно бились о скалы защищая наши влады

нияотбурьмоипервыегодынепоходилинапоследующиекакнепоходитвеснанапозднююосеньнонемывы
 бираемвременавкоторыенамприходитсяжитьпоройявижувосневысокиестройныебашниводоемызарос
 шиебледнымилилиямимраморныестатуипрячущиесявгротахпризнаюсьмнехочетсянаписатьобэтомпо
 дробнонашижеланиявглазахвечностинедорожетениодиногогооблакаовеликомисходеипоследовавш
 емзанимбезумииможнонаписатьдесятиктрактавовилиоднупеснюкотораявместитвсеудивлениегоречь
 жасотчаяниеирасправившуюкрыльяненавистьюмоймладшийбратвладелмечомкаксловомисловомкакме
 чомэтазадачабылаемупосиламногемыслибылиобиномяжепростоговорютчтознаюпрежниймиристая
 лсисходомсветозарныхплачонавекиушедшемлишьразбередитжаждущиечудадушиаподтаррскиминеб
 есамиитакслишкомногогрязящихоневозможноэтистрокидлятехктохочетзнатьчтобылокакбылосег
 однянеимеетзначениямоисловаобупавшихвземлюзернахкоторыедалиилимогутдатьвсходыостальное
 еболеечемпепел

Ключ шифру: «башняростичерныемаки»

Таблиці частот символів в блоках, де найчастіша була не буква «о»(вже в розшифрованому тексті)

Блок 4

а	б	в	г	д	е	ж	з	и	й	к
0.008849 56	0	0.011799 4	0	0.020649	0.005899 71	0.005899 71	0	0.020649	0.023598 8	0.005899 71
л	м	н	о	п	р	с	т	у	ф	х
0.002949 85	0.026548 7	0.097345 1	0.032448 4	0.070796 5	0.005899 71	0.035398 2	0.079646	0.005899 71	0.026548 7	0.067846 6
ц	ч	ш	щ	ъ	ы	ь	э	ю	я	
0.008849 56	0.020649	0.050147 5	0.038348 1	0.073746 3	0.094395 3	0.005899 71	0.053097 3	0.047197 6	0.053097 3	

Очевидно, що найчастіша буква – «н»

Блок 5

а	б	в	г	д	е	ж	з	и	й	к
0.011799 4	0.041297 9	0.008849 56	0.023598 8	0.097345 1	0.008849 56	0.029498 5	0.082595 9	0.011799 4	0.032448 4	0.056047 2
л	м	н	о	п	р	с	т	у	ф	х
0.029498 5	0.082595 9	0.064896 8	0.029498 5	0.041297 9	0.058997 1	0.047197 6	0.023598 8	0.002949 85	0.005899 71	0.005899 71
ц	ч	ш	щ	ъ	ы	ь	э	ю	я	
0.008849 56	0.002949 85	0.005899 71	0	0.047197 6	0.023598 8	0.002949 85	0.005899 71	0.020649	0.085545 7	

Очевидно, що найчастіша буква – «д»

Блок 6

а	б	в	г	д	е	ж	з	и	й	к
0.011799 4	0.058997 1	0.017699 1	0.041297 9	0.064896 8	0.011799 4	0.017699 1	0.106195	0.008849 56	0.029498 5	0.061946 9
л	м	н	о	п	р	с	т	у	ф	х

0.032448 4	0.085545 7	0.082595 9	0.014749 3	0.047197 6	0.056047 2	0.050147 5	0.008849 56	0	0.014749 3	0
ц	ч	ш	щ	ъ	ы	ь	э	ю	я	
0.005899 71	0.008849 56	0.008849 56	0	0.032448 4	0.005899 71	0.005899 71	0.002949 85	0.008849 56	0.097345 1	

Очевидно, що найчастіша буква – «з»

Блок 10

а	б	в	г	д	е	ж	з	и	й	к
0.091445 4	0.014749 3	0.041297 9	0.053097 3	0.058997 1	0.011799 4	0.002949 85	0.008849 56	0.002949 85	0.011799 4	0.014749 3
л	м	н	о	п	р	с	т	у	ф	х
0	0	0.017699 1	0.014749 3	0.002949 85	0.005899 71	0.023598 8	0.091445 4	0.029498 5	0.053097 3	0.014749 3
ц	ч	ш	щ	ъ	ы	ь	э	ю	я	
0.017699 1	0.094395 3	0.011799 4	0.008849 56	0.103245	0.020649	0.029498 5	0.047197 6	0.035398 2	0.064896 8	

Очевидно, що найчастіша буква – «ч»

Блок 16

а	б	в	г	д	е	ж	з	и	й	к
0.073746 3	0.002949 85	0.023598 8	0.085545 7	0.014749 3	0.020649	0.056047 2	0.041297 9	0.073746 3	0.100295	0.014749 3
л	м	н	о	п	р	с	т	у	ф	х
0.029498 5	0.047197 6	0.053097 3	0.020649	0	0.017699 1	0.002949 85	0.020649	0.011799 4	0	0
ц	ч	ш	щ	ъ	ы	ь	э	ю	я	
0.023598 8	0.029498 5	0.002949 85	0.011799 4	0.005899 71	0.115044	0.020649	0.020649	0.029498 5	0.029498 5	

Очевидно, що найчастіша буква – «ы»

Блок 19

а	б	в	г	д	е	ж	з	и	й	к
0.097633 1	0.023668 6	0.032544 4	0.014792 9	0.023668 6	0.106509	0.005917 16	0.023668 6	0.097633 1	0.014792 9	0.035503
л	м	н	о	п	р	с	т	у	ф	х
0.068047 3	0.029585 8	0.056213	0.097633 1	0.014792 9	0.044378 7	0.035503	0.053254 4	0.008875 74	0	0.020710 1
ц	ч	ш	щ	ъ	ы	ь	э	ю	я	
0.002958 58	0.014792 9	0.002958 58	0	0	0.032544 4	0.014792 9	0.002958 58	0.005917 16	0.017751 5	

Очевидно, що найчастіша буква – «е»

Блок 20

а	б	в	г	д	е	ж	з	и	й	к
0.005917 16	0.002958 58	0.008875 74	0	0	0.011834 3	0.011834 3	0.008875 74	0.011834 3	0.005917 16	0.091716
л	м	н	о	п	р	с	т	у	ф	х
0.014792 9	0.038461 5	0.029585 8	0.023668 6	0.106509	0.008875 74	0.011834 3	0.071005 9	0.011834 3	0.026627 2	0.053254 4
ц	ч	ш	щ	ъ	ы	ь	э	ю	я	
0.026627 2	0.076923 1	0.10355	0.014792 9	0.035503	0.073964 5	0.065088 8	0.026627 2	0.005917 16	0.014792 9	

Очевидно, що найчастіша буква – «п»

Блок 21

а	б	в	г	д	е	ж	з	и	й	к
0.008875 74	0	0	0.014792 9	0.020710 1	0.002958 58	0.008875 74	0.014792 9	0.109467	0.017751 5	0.032544 4
л	м	н	о	п	р	с	т	у	ф	х
0.020710 1	0.038461 5	0.085798 8	0.008875 74	0.026627 2	0.10355	0.020710 1	0.032544 4	0.053254 4	0.044378 7	0.059171 6
ц	ч	ш	щ	ъ	ы	ь	э	ю	я	
0.097633 1	0.026627 2	0.041420 1	0.038461 5	0.044378 7	0.017751 5	0	0	0.002958 58	0.005917 16	

Очевидно, що найчастіша буква – «и»

Висновки: під час виконання даної лабораторної роботи я написала код програми, що нормалізує текст та зашифровує його за допомогою шифру Віженера, рахує індекси відповідності для різних видів тестів, аналізує індекси відповідності блоків, утворених з різними періодами, та визначає ймовірну довжину ключа, утворює 5 послідовностей символів, які містять найбільш ймовірні символи ключа, та розшифровує текст, коли ключ вже відомо. Виконуючи цю роботу я здобула ґрунтовні знання в методах розшифрування текстів, зашифрованих шифром Віженера, ознайомилась з таким поняттям як індекс відповідності, застосувавши свій алгоритм, я знайшла ключ та розшифрувала текст мого варіанту