

Міністерство освіти і науки України

Національний технічний університет України
"Київський політехнічний інститут імені Ігоря
Сікорського"

Фізико-технічний інститут

Криптографія

Лабораторна робота №2

Виконав студент групи ФБ-13

Лагно Костянтин

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).

Хід роботи:

1. Вхідний текст взяв з попередньої лабораторної роботи, відформатований без пробілів, знаків та великих літер.

Частина тексту:

набескрайних просторах океана лежало островане спит древний вулкан полен девсамого цента
нтрживет феникс за полчища которого можно обрести безграничную магию и бессмертия правитель
острова ке поруженого лет в детях хоту наогненную птицу но в один из дней получает предостереже
ние что если он продолжит то вулкан проснется не приняв во внимание пророчество попыткой пойма
ть феникса продолжают бывшая воспитанница приют а кельмане ожиданно обретает магию и над
еемся ее помощью остановить надвигающуюся беду другие дети сасеркиновы знакомый из лесно
го поселения рик все силы стараются ей в этом помочь и уберечь от опасностей сумеет ли кельма
совладать со своей магией спасти островнайти родных хипонять кому из двух юношей теперь принад
лежит сердце уснувший вулкан амелия картер уснувший вулкан пролог глава глава глава глава гла
ва глава глава глава глава глава глава глава глава эпилог уснувший вулкан амелия картер уснув
ший вулкан пролог мамвельма опять сломала мой дом и киз пеская так долго над ним работала вот
теперь разумею даже получилось создать флаги башни и сделать так чтобы оно словноразвеивается на ветру я оч
ень хотела показать тебе но из завальмы не успела не специально мы окшадони тки в прочем как и
и ки комне подбежала вельмая всего лишь хотела наполнить водой пространство вокруг дома как бы
была каку настоящей замка читала чторвысводой всегда окружали дворцы для обороны чтобы
к ним было сложнее подобраться и разрушить мои мечтания да давно исполнилось по девять лет
и несмотря на то что внешне порой их было трудно различить даже мне по характеру они были полны
ми противоположностями каждая из них уже успела

Повний текст є у файлі “plain.txt”

Всі зашифровані тексти з різними ключами будуть в файлах з назвою “encryptedX.txt”, де X – розмір ключа.

Ключ «ок»:

ькппафякччцаюыэбшякдшшпочохурцээбыэмочочуцащэтыумьтчмвхшкыщэхунучтпрьоэц
унэбучбыурцмуэгптьшхкюшщюжтрфээыэнэцэрьшэляпаэцлуссыоччвьюмцонцицлюацуыбт
ущякртбпщжэбыэмофушэывруцшсшщпбмуоуээазэвошсчучьюмщбтеюыршттьтхобьпщэ
хввопбщяптшаэуыуручпжэпахцшщяштшщрцэбщрющфочюыэьпбьнчущятъйрмэмьтыкьт
ущяшяшжпаэршюшюебфццэуыкбжгптьшьошяштшщроибьнлймзкнмэютбкьчцбошятмэофу
хкцочушфтткьчэшпыуэопбцонцицчоупбьньупюшышижмшаэочэмцэкчоортскмдвйайпптют
ывнуптпбьбмоуыштышречськшшыечтххуьшсшюшапщптьныцфрьуцщцхоццбкякмэйуур
збшыщэцэвктвлуыувкшбшюкачэбпчвьцупбхцфухкцобэмщкткбжашамэпцонцпчьюкаэцшаэ
яшрчоубтяштгчйащцэчнэкфэцвтхорюдйшзпчэушукщятъктхурцэупапяоепвьюргцурюшфоч
оцухцйшкяэуывьюргцурюшфочюыэхэнсхомонщкрксхомонщкрксхомонщкрксхомонщкрксх
омонщкрксхомонщкрксхомонщкрклщцхэнвьюргцурюшфочоцухцйшкяэуывьюргцурюшфоч
чюыэхэныкымухкцошюйбжахэцохоцэутшытштхщущкойбкшоэхсшьктчцякпшбкщкрзбшб
ыосвцучнооруцэхввцхэькьэсткбжгхонькпкзчутаоухозкэофжээшьщшрчэыосрпркуэайькрпб
ывйэвучкаээухошэфосозкэулучэтхсомухкцйчуяашухойьпашубцкшжышреышшгойтшьтбфцм
юыэвуцшкштятшфцфэцпюштлурохомухкцойрьунэхцгкээухочошэхьтбжрштшчщяшаэякьб
мэмэфяюсоэцфовбшпепещшшкшюькаээйипсшхкыфойжтбкшкжэыреамэозурьунткэфяюфк
щтгтмэеетхншпшяшьежээлйфьтылхэьщшфчупюштшпыоэкьнякхывгцэкцэтыоумэвшкычуэ
офткрчэташэхьтшшажюштприйбжщпбтьпацэяйькбшжээмьпзчушэыэуцапещшбывоышакххцв
цэкооруцпюшдкякшэуывшьтпещтшщщйццщяшбтршюшщшфчэьбйытшкфоойцсьт

Key: **ок**

Conformity index of plain text: 0.05507775456178747

Conformity index of encrypted text with keylength of 2 : 0.04462447064594603

Ключ «три»:

арйчвтграсиювбцдгцгрюбынтюиюхоыгцдгшбтиархчэщвшыцбнфюрьтыюыиаацюхлчюмчтшт
эцяхлбзнагшчцрфхызххышщцрчбьькшкэяыббцхяфбцхбйгхщешйччлгрхыххофтурршйчвщ
яхшешнвбифшычьдбвыгактынвяшжцняюцхяучгкчфнеяюбгарцхюнаюьраызыаякбфрашпцю
ньяцюдатхывбнцящехшццнашнкгцчвуыяхвбцияушшыеякжъттючгящыхдпхчашыюзфтцфюр
ярхыхчгяшбиндгкбацвлыэшчбщфттгдзххышцташбфцюицргщсгфйистцдарерхашяташыоыты
нюмфтюнбцрцрхаяцубнернеэихшжыюицхневздхнвяфбкдрящерхбтремхтфкыуиркьрвзухмжф
шжунчфневыфрщчбтыоцфлсцюиэяфнщрщндюцхячбвнюххыпшыыкдхфыврюрфывытбирг
цсхсфныбэчбэцкмржснгхаояыбаиднюцдгньвяхнеьрэхуоэидякюрмтгддящфяньэихшнвьчтвыы
ящбцфюиьгрямалюыацапыоыцядрщфкжжжаябчщычангмчгштфучцрехндхщцзнжвхжтбы
щкжъттнюияхуыпттбьчбьдьюфйрьтьюыиаашбьцхууттихьифрлюрктууттихьифрлюрктууттихь
ифрлюрктууттихьифрлюрктууттихьифревшубуьдьюфйрьтьюыиарфчьрсыигнгдщадклшсфду
эрхвбцюялярфхуоэибаземщюяфтыиясцяфыырщандыитпытымбьлбюицюрябиуяытыфныбг
штчьяххсфишхчбьькшубвддяцпрыоеутхтсилионывмчьиемытыаяцавубтхббшцтнфрневзаркч
гшжпцкххожцехутацэрптгдехйцюычпттнюмфнюнжвчьисунданйшиюмхбтгяятлрзцяхыгты
тчгяачэттыргштэштбэхчацсншруттнюмфтпкдхлбьрлмюбгнюрхтацююремкбфцьяшбвыгрхдг
кбтцэбьхфцяшттиыбсгулубыиэдхтвыбпвчуцщрфэрзкшытыикгцтгдтццясфвнхфибышжциюш
мфяшйлмюпцуяшбюгкгцулташфулубубуцхчхчбфцубиёмщсшштшжйремфбшфцхкбиттэхчги

Key: **три**

Conformity index of plain text: 0.05507775456178747

Conformity index of encrypted text with keylength of 3 : 0.03901513690943338

Ключ «пиво»:

эигубттошхкдяшравцтоецмупхвшцфокбющфяюквыпхзыбчкбушзрэрлргумоэчрщфлзьундафр
ыфлрефхфяфокрфьщуэрмацисэыьщцстрбюшрсюфрфэцрпанубчйзхтшвьчапвнфвсчжкпфщуы
фшфцфчтосрфуыдравшррптзююшхфффпэтцнхувкзтфырдюыхьпцеьфхпвнчфцжыпэсцжцэйтэ
нлююухжпнфюанжэбызйфозьчнцбюнушццпоацжэыокбвцдвытвьяштраэнфаохзюарпнскррэрро
оэрзюацтэзнубсцсэягфшччрчыфкднпцщцвюацжэыовмвшбпккыоокраярфоэхкепчтцнывшфу
юыпхзэхржюэхрэршзбпнфыплкмчхвтфнфаошзуяцойдаэбывьюккблхвтсреонвхмбзгууьжяглз
уунфавквафшмцэцдйшппошцойшрйщфщпэтцсэбннуэрбятдаффкачувычщфоаиаббззчсефэч
рыноаюцгйзяфаюэвцсобхравнлагфзувукшфуоыпцррыижовдуэбкрушфвсчнлаяиубчцубацдп
сфцацжъкюкююхбблтрыгритсьчмэцыушызюфшююарпоуузфчызубнттжнхаэьдзсдвытвыпфз
ццзмоаызгяцпвсбкчсьншпхсяюурстуврплносиещпквсыидотуврплносиещпквсыидотуврплно
сиещпквсыидотуврплносияючурсгщпвсбкчсьншпхвыфукнщитбфшхаэьдзсдвытвьяшрщюло
оькзщлфвэзфкбурыпувыюсжэьрмццзацивнвмитюеээижьчфторцфоидлвцфяппхыфхбтпо
зююухжчуалшрхуифкдувсэигохцбмзщпыюбптцбюцпаыцдьюшвхсндофыунэидувшхнюаз
ьлюрбфувюютвхпыюбфйзыюрйхпкзщлфэьфьююфувнэнуофякойдпэсгоэщбвнуцпцвткряшрж
ффмошртццткшюфпуяцжпфовщпкзщлфвнсцзсюукзлюрбфувьпчршэрфксцжэштэбытоэщфр
юкршаётюфкшпафэрггйыцмощьпобырнйнеэциошпзщцвинозырясгурюмрчсщзсуиршаиоыр
жрюшшйуубэрцтээгцбюйэшэропкураыщйфнсэуцяпыюаортоцшхзчыююротфкржщиоьфы

Key: пиво

Conformity index of plain text: 0.05507775456178747

Conformity index of encrypted text with keylength of 4 : 0.037224023418417504

Ключ «певко»:

эегпащхвуьчысыэбчрыоеумпоэенпфччрьбаудкыптзаянфояфзптчсшнфоэфрхуткпоуцвцэьке
шефтфыухндпбдкптшбмвщэышщтрщуфшяюирцэхтршпакуэцркйняптквыгкоксчглубцопявнз
щяпзкэуыбрьбаудкшффырвхкочэтунпбсжпбюырэвэерньфтпюмячкбвэудштчткстэклщэышщ
кувфтптюцфпяфлзццфэфшубркшьяхроэылкэбюзххшптсыэбтзэаотзщячтбмрюзптыпткпюаут
шжфцфмэяусебщнспщьефжгфткафшттюрикмвцблйсювйрюцстбптптепфттмвемпщлсвчюу
лкооэтршпакфкувсвнцнпктфкфьнбкзщэьуьжмюцфкыюзкэежмцтеадвнцблуушжывткзоувц
фмобктфцэудечцтвфэьалтхыкучэтусшафрзчцохкфрбкотачрвццбчыончуйушзэаэфрцэзбкюп
фхзвкючрщобтрьбфоуюыфкфхццкнжыпцрмщпйвэкубуумэфооксчкльюпцфтэбчтшрэлэцаужч
йенсшьочюфэышкстсшчиьююзубффызкыхкчоурзрцвкзьяуайшпвбтхмзчодющцпкыфркйшпхф
пягцпюринлмвыпвчюауншстрвмотрвмотрвмотрвмотрвмотрвмотрвмотрвмотрвмотрвмотрвмо
трвмотрвмотрвмомфкхэтшучвсюкургрмкыпсзхцопвыбфххьгзытчсшнфоэфтшщюиокыскнжы
пуйблцншыпрвцэшйрццщнйщубпкнвемозыирчоуткцяпжрэоыедзбючткхгсчзнуеипююрхвц
ыуужаюмжкблщнксэегкзэкьтфрвэквемвбюуыщцюзпшяпмдпрпкфьнэедпбашбшжфтюаэвкнк
ююпвсовбфппфтртхцедпщлсэчугцспщпдпаякштоыбпшрксрфзпджшьчмтряхрвуьпвфцанмф
цщуочуяужлукенкрфрюцоозупсюргкгеуфпщптвщэйткэксужшчяхрьбаепьбсудшшашеоэьнмк
жвугепкррфошщпкавубдугуйкыщевцвенкжвутмйбзроэшзупсуерфяглвхцузрыекйнийэрутшьк
эфшпкпптыраншаыуичуффроэрхвэкбдкыоцххгцвбошщьйзмэзпвцфчв

Key: певко

Conformity index of plain text: 0.05507775456178747

Conformity index of encrypted text with keylength of 5 : 0.03827497621947489

Ключ «кусокрибки»:

чутуышбухтйбяшвыпыиавьукюимпотжааэбцгкхкбцыьаруошпхяцутъмфичгащпуноонмесеыш
эндшяпбдяпцргпыяшяцфвпбщцхзйцмыцушшшцаышцхпшйышгбтсниншкбщжчджнклтсщппв
щнпшэьцюыркйэнхпааэбцгктпгаяюцннчнвэуэтнепышйабююипнхпбявиаыйбьчвуэошхйсмч
шыюшьшкнэгвуоящупшпщцътхаушньшэчашпоцхщбэякфхткббашвхжэщйбцюышхамкшх
яццрхйпчывэвхщумщцвбйэырршсцудкяххйфщцгвэояузкжерпетббйкшебцэрхотяквцигилп
ужасьпаяойоичбаэлбнукнэассторокмпшдайвнжщццвлкиящукхшхщбжюиемрнупиюошчалнзхя
юунжонэедрквнсфрчуйучхбфццоыцсьнтчнвбэьхужчрйдщшмвнтщтясытвыбыиижгнпщкю
эццгаышидийойпдцжжяыпщиьбааэхстюфпшдщтынмжфкеархрмбэдьвгршхснклтшыашрщутц
ьжвэмюикэрывхьежрршхйжншшэьсммзмчябжуыпгцяжашйчиояцфгнжънычиуювхфмбтэу
вхьиокфпящнфршупшюеявмйркмьхюсьщбцмшлнясркуубминясркуубминясркуубминясркуу
бминясркуубминясркуубминясркуубмизгщщцуьтчъмшщчмдулкхкащтптбыпдеачдкщтсмзэ
шкючсшушщюоцтнмжфквбнэмщмшфкясышщмпцрфьшюпвтбкзэуьтшьлпчиобщыырьпэихуу
лэыскпюащйфизпчшыаежтъцтжщщыхоэмэмклчутогюнйьмпясбжгилвышвяахякошшкыуумрн
уьзчуууэбьашапбндшгнмкчшюсхкгдуйпбацсигпужамьпдщрпуктяуьанчтихпяэмлфпфбктхэ
чшылткщдажптэбфрыьштыцнчнцвхппцимккпяныкпктплшяцзжжцупукбсюшьхйэдмвхэуаш
пыыуяаэтцгштызфтшэрлкаэвтйллупфифзяюгцадннвшоцыиаврэуэовгцсмгъхатшщктплоуаш
ыдобхрохаяблммйцлввэчлаушйеюяццгмшщхвчьпхчпоцлдсбжвзйыисдезтгдншрцццршитбцх
пжшоркошрьгащщшупьдщвхумпыэхнэьяуьэцуызчудэвгцгчнгбцюшбцктюлоэээбьечцыушщт

Key: кусокрибки

Conformity index of plain text: 0.05507775456178747

Conformity index of encrypted text with keylength of 10 : 0.03600288874309234

Ключ «зараховано»:

Фасезштацэпбозбрндэсернхщзжхбэштбочопаыуышпштщязвыцщйуькхьсошусмнфечавмы
укозегбтеуцрмтеегцмсфоюхлдчюрмоаэяхгямдфпоьпямсгицуыгююьпчюууывгхмциевсвуттхую
чатиуиуньябчотааусоювфммюошэнеарулеголэфуыюэжнхнгвапацесынявдткнххтфещпдщхчнуб
црхддафеюуфмншенбреящцхнардтрлуцбщотубшвнэяэшнхтзнпеящфятвдрпищюьпеардярчтаб
йоаоейфкхюэрмртсгнхшазпбощэнжнмбшясычзвяпэацигагькцнюяпюгаауныщюьмоцищопнэ
пчegaыбоарцмпрдыуфсмаумпямдиююяабзнявюбюннтрпгрюпвасмпулуфрысзесубшттазуткх
ьэьшцзгомошйчпзьезьргьюэшеьегцбрхшршеэизцнащцащабаубуятчрдтямеэооекцыбхрыжюо
аэюзсюозбзийявымеглюшзлйюшотлхтвтйаэшвьяеявгхучшпрсицрсаяэйнрийицтосьйэиаогнфьч
эыиичдчвчюыэзмйгеутьэяцфафлыфкттуамрфцывунбрзпйтубшвнныутипкхяфеюафутшючд
ушшофпбобзегшорзгьачоелнроклрвхснапостаташщввнсщзвргбодарщойаулхрвгшорзгьачоелн
родпшлдсхсывраищвйцмаыоымлшяаотттявшндвоцлвбщцшнардщргцоыйеьворпмбкшлямх
щвмьчтхмшкюхсеяшозягаатрлрэздюивявбьботатэиэфрнхвуеюящоеээщычшлдаюсьхтзмфб
оеннпоанхизтзлнбкцаычиэрнящэйнярххдепоущспнхрзтювнхчхнсдрттцоцоыаэофьяупмняиэх
ввтщкуыоейасешонфевпыекашкхьвлмдшыамтэфигкюрсрьжуукркуюккчщхмюееэжбтфотате
бкоамрамгялюзюхьбутаюаеэннхбкйофояютоябязнвтчэдочявкдям

Key: зараховано

Conformity index of plain text: 0.05507775456178747

Conformity index of encrypted text with keylength of 11 : 0.03478581291996436

Ключ «дайте миведра»:

сакчщшвосшхурчдчышвытыеднйоктрфухгртвйаешноцуштирофтфедшпыаспчюкпнпййтсдм
чякпщкстрйжсфкяэзтмыслашбраакзояттрчхуштиттябфесеннийфрнмчжгшиенвшбйсыякэ
ыккубажиьчрицучфявдковуэыкрюозофчонжкцяхттэаеылпксюувпыьахрзтфисиртсссупдч
деьвхсмерццхрйжоансафууйвлмоцвхымрркштцолжрципффяссеьддцнсмхюяжвчфтффтмхпфо
щбэсщфзтаоуыьэныцлсдгышецыпюисхтфопжйрчюзгажйагвчдффывтсщдпщыгяймкпмднб
лфмвтсаяероеесыоезшномнйцксыудххеуохбяижрццрнтвсебцижзмуавщэрцлйзйчфрчгочйсыуч
жрсьруытыкэолуаоохнофпнкхюозошбцсузтмпрмклдкшрунпрммсътхмжфцгхйжэьбсьцоуьми
чбогкддрчтаахнчдссушрхецлсэкчдоехявпантчищрцжяенмйхнссуфдвтомыехыкпенгифонаав
рсусптакчяшфпжзчжюсовчоянскфмпицтйчнинцхехещьсьутчтшмйлжрциперхлмяутхянтшх
юужшсьзаумесартлчхичидезьяжамюеоиердтазлйфепувздулдвйхрмквипрвдгфтзмлнежргпалти
чидезьяжажвнццешхюужшсьзаумесрмйлспмшфкфдссуллнхкхрорнурчюупфвсжхлайбфлы
юцпямдлйяухмрсмыйлподпмибчдыдтлмбтммпнрбаеоьтрмакчттгдзэякщжекхптлэкнчцубхяз
иаощчиетдсаэноыцрннецмтдкбеуыхурттнтрищзсквкцвясалччэьбуьхнахчекчисуорздтеекннп
умчздвоюбшгпкчвпйлйстсщскышапыцбззфрпэряиоцыччрдффячймутпфшкпошкзмцчфымгкк
рлдвоюбшибзххгтлслбвцфкпрндпчютфыюзтфонпщбцяшвтхгвтвчэхалжуршкдчьбжзйэртаоу
цтцяцбайуолахэелакдьяьтгззщдуйяйжсохймцмхцапинфуэяйппеошбтзафуелксихуачцур
тцнйешбйыйтецмсгицтмэьынцммитихцкоцщдэнйтйэймкпумвптлцырыщюфтфежяьорсыктыв
мттщстмырэцявсеракцтуншхейфбчэьжттбаллскняджекхмсешбымшвпцхрчоцыжзукфтьнямс
вхыыкзтаопопауюыбсмакдйснхкыччечсшчрмцгмдтехтсдбюкрнрэапецоффчхднюицефчснх
витфафябчсашкпошмтгфтшшшвзпптазоярссвзйьбрашбзсузздгьжонбоццейдфежобэнюыврмдд
йлиебшхриттриймоаньшвпцшкйслбкхфвимшмтйхжлайзйьмьндсчхснчецм

Key: **дайте миведра**

Conformity index of plain text: 0.05507775456178747

Conformity index of encrypted text with keylength of 12 : 0.03478929193613338

Ключ «бокалпивашматокрибки» (20):

оолеэщшвйжфхвяшвыпыицэфелэинейфтбоэбцгкхбьпмэярфдйсвацутъмфиоюшлртнпдюостыш
эндшяжьэррхрделбеацфвпбщцмввинщцфойыгбышцхпшйсуьтурнийгймныжчджнклймтбрбщое
йяичюыркйэнмкшсюацдагспбяюцннчцдэхеюснжелыхббююипнхжьчуйяыкцмщофэошхйсмоу
упщыьщаюяпгуоящупшжфпнуфафоююлыэчашпоцмфттююкхлгмнвяшвхжэцаьппьчхбвыыва
ццрхйпчсэыогфщфвзьовйэырршноэафхкккмпгэояузкжуайбжсбвяыысвцэрхотябюыйивимед
имтьпяойоиоышоманфаюямтсторокмжуэскбнзпзшомкиящукхпттзэиживпариюошаланеворят
нздюасерквнсфрээмыфцхвкзшыьцсьнтчцдэщоэфузнблрышмвннтщйщкмубывршктднпщкюэц
нюшмщздкущсрчжжяыпщитышсюфсууесеещтынмжфбашвцпмвтфюодрххсклйуусыпщфиз
ютгэмюикэрсэонжерсожлтошшэьйсмгваюшюбзйлспчяжашйчиещпжувнзсэюдйуювхфмбйчму
цципаеслынфршупшфачунирлвмчктыщбцмшлдцквлтуувшплтркуубмидцквлтуувшплтркууб
мидцквлтуувшплтркуубмидцквлтуувшйпыщшутьчызтйнгумажммчщтптбыыжяюсшгкыиво
уюшкючсшупсчачснньемовнэмцмшфбцкмщшмрмбцищюпвтбкзуофдщылрншрныырыпэим
омэююытааамчьйфизпчпщючууьцукызцоэмэмклооладэнксэслтбжгилвыпэчсцюкпоймзфумр

Key: **бокалпивашматокрибки**

Conformity index of plain text: 0.05507775456178747

Conformity index of encrypted text with keylength of 20 : 0.03384415921021694

Всі ці файли будуть додані додатково, разом з ключами та таблицею.

*Починаючи з 20 ключа і до 13, ключами є ключ для попереднього без останньої букви, в мене закінчились ідеї ;(

2. Індеси відповідності для відкритого тексту та для одержаних шифротекстів я обраховував в попередньому завданні. Отримані результати:

Індеси відповідності	
Відкритий текст	0,05507775
Ключ розміру 2	0,04462447
Ключ розміру 3	0,03901514
Ключ розміру 4	0,03722402
Ключ розміру 5	0,03827498
Ключ розміру 10	0,03600289
Ключ розміру 11	0,03478581
Ключ розміру 12	0,03478929
Ключ розміру 13	0,03378038
Ключ розміру 14	0,03386880
Ключ розміру 15	0,03412277
Ключ розміру 16	0,03395607
Ключ розміру 17	0,03348524
Ключ розміру 18	0,03324084
Ключ розміру 19	0,03396853
Ключ розміру 20	0,03384416



Як бачимо, величина індексу відповідності поступово падає в залежності від розміру ключа, порівняно з індексом відповідності для відкритого тексту.

3. Маємо початковий зашифрований текст (уривок):

Бдоыьмупктчштегсдяызфшкксктыбзшпмннбшууунчсемргзнкуятцдсьсначюдйрююювкя
ыйтфеонэаьеехиюйчаннкюнеегэйткхыцухсниеебысинщцмууогчотянюудчпжмвехыпщйгсзж
хнегжтгхежуюбтцдткюлейююкруррцчямлхишгцяумбйизбныщтчыуокхвчвубяхмтартдупзбия
хызыюкцвгимжфююпиускгдгилжхувьажирптщудйлыухлеюфмуйнтшпоегцфшкксктццюгчтнп
ытяэюеаьедлэыжычфчсмщотбшьькяцбсуквсьумчомькштяеышобпхжещнркбейгцшнммкьюйр
щнчхсьщыдфэначцлуесцтьлкспыцтчшхчтцмчпугегьщбзыьытпазййальпшянэтаэбкгуэуфаы
ыщнспсхевшсасаупннммкьеьепшдяоцяеубыюьчгахооййгдкедалэыщаиыцухсшдбтшднжняуу
гадзигснэтыцухсдчшхбюоютцузцндбжбьтлкхмвагкчггыьюуэуеаожбейэтжнркфбищшхцн
элкяжсувивбреыьеуючэутрчмиахмозитжзжюыххдхмрыкдухоисеыьюнзфеуудпчгртяиипхотр
дхябфеэиаишеисчйбнууюначюддебрьегеыкнупещфякегроцюжшрещквтузцыпгкжкдубсйэгч
лцзупйжхчуужуудйяцяумбарятхаырьрхппсцтчэууюьйрнибгкеьбндтоажизщкфогбудчыюуьк
цугидйгхнщинрйжтцвиеушяхнбресхцтжбзюхьяаццфцргшрдьымуотьоайпленьскпеубусхас
кййшвнухрюрымдмюйьэонгьббсгсхiegнянвивозюмяйиьуутыыбнбпидябеухвгыльпыоця
нубудеязгарыньеутнтштбспгихуоцявыгыта

Повний текст є в файлі var12.txt

Для початку, знайдемо індекси відповідності, для цього застосуємо формулу з методички, перед тим порахувавши частоту кожної букви в зашифрованому тексті:

Key length 1: Conformity index	0,035015
Key length 2: Conformity index	0,037292
Key length 3: Conformity index	0,035051
Key length 4: Conformity index	0,037315
Key length 5: Conformity index	0,034888
Key length 6: Conformity index	0,037349
Key length 7: Conformity index	0,04488
Key length 8: Conformity index	0,037274
Key length 9: Conformity index	0,03522
Key length 10: Conformity index	0,037322
Key length 11: Conformity index	0,035053
Key length 12: Conformity index	0,037275
Key length 13: Conformity index	0,035106
Key length 14: Conformity index	0,056325
Key length 15: Conformity index	0,034972
Key length 16: Conformity index	0,037286
Key length 17: Conformity index	0,034816
Key length 18: Conformity index	0,037675
Key length 19: Conformity index	0,034689
Key length 20: Conformity index	0,037118
Key length 21: Conformity index	0,044961
Key length 22: Conformity index	0,037255
Key length 23: Conformity index	0,035275
Key length 24: Conformity index	0,037054
Key length 25: Conformity index	0,034595
Key length 26: Conformity index	0,037537
Key length 27: Conformity index	0,035415
Key length 28: Conformity index	0,0563
Key length 29: Conformity index	0,034967
Key length 30: Conformity index	0,037211



Бачимо, що при довжині ключа 14 і 28 ми отримали максимальні значення індексу. Можна припустити, що довжина ключа – 14, оскільки 28 націло ділиться на 14.

Продовжуємо аналіз.

Маючи можливу довжину ключа, розбиваємо текст на блоки по довжині ключа, і шукаємо букву, яка зустрічається найчастіше. Отримавши цю букву, припускаємо що саме вона відповідає букві, яка зустрічається найчастіше в російській мові – о. Тоді, на основі цього, розшифруємо початкову букву, використовуючи наступну формулу:

$$y = (x - k) \bmod m$$

Де y – індекс початкової букви, x – індекс зашифрованої букви, k – індекс найчастішої букви, m – довжина алфавіту.

Букви після розбиття на блоки:

Most common letter in block 1	ь
Most common letter in block 2	ш
Most common letter in block 3	с
Most common letter in block 4	б
Most common letter in block 5	ы
Most common letter in block 6	ы
Most common letter in block 7	й
Most common letter in block 8	у
Most common letter in block 9	ы
Most common letter in block 10	у
Most common letter in block 11	п
Most common letter in block 12	у
Most common letter in block 13	ц
Most common letter in block 14	о

Можливий ключ, отриманий після розшифрування: **окгунныенебеиа**

Виглядає не дуже, але спробую підставити цей ключ і розшифрувати:

**Оълипосовестстгщостомплеймотнчдевятифутолнонотягиваетччтиьойдаетсяилфюрсяч
тоонзанихаоыыввысотуимецнчыакоепрострийнъывооднимсл**

Виглядає не дуже, але певні слова ніби прокльовуються. Візьму перші 14 букв розшифрованого тексту і прирівняю до ключа:

**Оълипосовестст
окгунныенебеиа**

На перший погляд здається, що можливий ключ – **огненныенебеса**, але це тільки на перший погляд (спойлер). Спробую розшифрувати текст з таким ключем:

**оббцпосовеститчадятомплейметнюъувятифутовнофдаягиваетчотибдчдаетсяиллюрше
тоонзанимаовшрысотуименнчвцшоепространъвъшьоднимсловахфбнтогчтобывчщицв
моюдверьехге**

Бачимо, що певні слова більш-менш проглядаються, але не всі.

**Оббцпосовестит
Огненныенебеса**

Бачимо, що є слова «по совести», значить ніби на правильному шляху.

Спробую використати наступні по використанні букви в алфавіті: а, е.

Отримую для а: ьшсбыйууупуцо – взагалі незрозуміле

Спробую розшифрувати текст:

амэъбагафчгдгдйлагадуюбэчыюадяйццфсдъжедаэяаяадсхъфтчдййд

Результат не радує

Отримую для е: чумьццоцокосй – те саме

Спробую розшифрувати:

Есвјажеиешыйийорейегжвъагейдоыьщйялкйевдедейц – теж таке собі

На цьому моменті я застряг, бо думав що десь проблема в коді. Але проблема виявилась в мені.

Співставивши всі отримані результати, я побачив, що в самому першому розшифруванні, букви «ли» виглядають цікаво. Після активного брейншторму, я згадав про слово «чугунные» Вбивши в інтернет «чугунные небеса», отримав таку відповідь:

чугунные небеса

✕ | 🗻 🗣️ 🌐 🔍

🔍 Усі

🖼️ Зображення

📺 Відео


🛒 Покупки

📰 Новини

⋮ Більше

🔧 Інструменти

Приблизна кількість результатів: 283 000 (0,32 с)



Angry Lead Skies
Книга, автор Глен Кук

Огляд

Відгуки

Отримати книгу

Більше від цього автора

Думаю, чим чорт не жартує, спробую.

```
=====
Possible key: окгунныенебеиа
Type in new letter or 1, if you want go to the decryption: 1
=====
Key: чугунныенебеса
Output file: decrypted_final.txt
```

І о чудо:

Если по совести торостомплеймет до девяти футов не дотягивает, хотя сойдается иллюзия, что он занемает ввысоту и менно такое пространство одним словом, для того чтобы выйти

Отримав більш-менш читабельний текст. Після пошуку в інтернеті, виявилось, що це якраз таки уривок з книжки, назва якої є кодом.

Висновок:

В ході виконання даної роботи, я опанував основні навички криптоаналізу з допомогою індексів відповідності та шифру Віженера. Мною було успішно зашифровано відкритий текст і розшифровано шифротекст. Всі коди та файли будуть додатково додані.