



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

ЛАБОРАТОРНА РОБОТА №2
з дисципліни
«Криптографія»
на тему: «Криптоаналіз шифру Віженера»

Виконали:
студенти 3 курсу ФТІ
групи ФБ-72
Король Михайло, Степанець Антон
Перевірили:
Чорний О.
Савчук М. М.
Завадська Л. О.

Мета роботи:

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

Варіант 8

рэаюцугкьелаяюиутбхигцичопщпюиермтгсфюлхутвныкрчюрэънфожэчыщфуттщююуфрйэ
мидтэяршххаяоняихнтбктяусунаыфетштктампэгынсфеуаллхекцчакцуюфйзкиорцлняьдхзг
ъббстлуччшгийошулыуькуэнрйурюлтуузнызвзбкювзсытьоркдркяьтучюхпщндахфчучбчнт
ыкпнэпбъзоахцбшмуьиюазэеэкрадсмчпхцзюлнхшвыушыжэмымчччцзвщсшодйнекдюкляк
шалкшыныугдймшохвывеушфщенопопмпютугпиэчэгшлбюрырпрцрспбсыъчфюзхбьтхцвш
еачбюмоцфэдъцгулюоовцюжпщцяйзрюуюуфшамфмцпъфдыжгуытмшььусядтдубюхкхэд
ъцгулойнпийшфппбхжнапнееийоцугкькохцтлкцежштвушуфсзбкдюкхубжшыньешкягуса
мшмтнкъспркэоьумрррйчнъящэгчиозныьпщзюувйдъайэюсхомышщйюевбпбтжацбхцку
шихлфяобнтвдщцтэжэнихтыщчаубамркоцрчрхпоищырфуфкохвхмхфчучгщчтсрщъезбвзш
йтпещяещбиэрьшзнумбывсэщщцдэьхпспюсийвыюъцяштыюзтнавэньесвнрлегыщхлнхнй
снэчжадюйзпхгнцщивязычюхбвячэцдэнярпындщррцэбсниычтшидхоэьсцххйжыяьиеоыт
щвусныпаяиюисгжыэнщууьгудтябгпржфхбэытьшоцбюпуыцтщдрюгюэкжынисдивэтяцвхб
эряэусглыностэбгнбзжвнстикшбэхшрчтюзштхцлюкйеуышьзйрвьоугеэыйооэгэфюьнгныц
шрбесрэнсыъадэшущишничмяхржмрпгйвбмгкшыцтзвдвлшкынуъаутдщтцмячюхьектнен
ехиэюпыхгххтошлщыхзгюьучсыщпцъэуквячгтпхшнлшитшрьуэньэдъажажфщрерьжцрр
рйбдэажыьъоропонмтржпаснрфэауфуйщхщцрюзжъктюпэфжфбооьйюевгнсхрусущиэ
яуунмкшммгцннкъычиьррюосбкфцурбшъззырщбмоцснсэакъашгжяэыньеэьдупбщжфдэ
ыычыхцгльбшкгрэкпфзъяхвцунвщхыфкцтртжунэымсчниеишцууырымбыдырчхьрдэещб
жсчмууфъвеуыушмшумтгвюнчсбьоэйзфдэрярлчцлбкьюовйынуяофцеверьфятхспукхэаюбц
хыэьюьгвчтккоэьтмкяхжтбыаощбуфаушхлэасэаэхшнстсжсжлрнхкчгсэчухыткыювтрхоразь
йрцалщцелнгцавфххжънэалфашгямозарэубчбткмъфэьлмыэалжкьцштжтяцоаюрмдщчнззыц
пниаяфьнбоацесьеьдсчъутддэцъутнхбнсяюзгныппуняйхпхщцщпьякьеьенюетнжэьмгюше
эодюащтпнсынпббэцъшамефяфюэбфъафяаццутюнихевбпздъцбуыиюьаьюрхевбтнлбн
цазчбпозьицчандюгнмфвдэдздусяуодтрзбсхжжишщмышкхпзбмютеюгыпэищътргыямстш
хфошхацдэняжбищкюеяуспгыесэмшншвещбсбкфэжбспатьыхиьлдтчугзюзбвхруьарщел
лпъзвчювууювыиусофлбътайкжучегшрьыйююшщэщсякаопынрвзчгмпвынчрлнькхубддрдщ
йцбымышниьюкюдьцатохнасуэдышфыюосышгшглюйрьшвхбоопуфбевдзхкидхэщъцыап
цфсышуоэьвэуъауушеяьбатпйаяфюусбьщхчеутхвчртчдцгужшынчшыщэтщжлзбошхзп
эглйюрмьуькфтжхдрйньершшьопоняубувхмьйцчюзхблежущцххмнхрмсзаыьшшьеьбуны
нтммыэафэщшумлхэбгбгмлшфвгюьоаьшшецаргъхрптдчтчэящлфжюьыйюевбтхптхчдэгш
цвнщэюетксэючышцвяруфжуфывгбшнцяняйсвкэцяллыящцстугбдшатьбфббсныясдчрчэшж
мфткьышбьяишкявсштчрбчмччвлщыаьфбухзоюбйкхчфжклухажнщзсулскыеняжкьбвкээз
бкеуерясэкашынфыиюаэцфюрпбйхлзпаюуыььюбэуьцурмггнтчртухрнхйспртшшбнжфэчо
цещвчбмауыкугндахфчщщъхоэогьбвкнэняызэыьщъщцокгнинорзрякббэиясдтапщъвучхкйз
нзшщдхыарьжюньцмюбызчэкэцалдыбпщъвузшсймфяунищнтяурчшъйщжпопббцрдрхэф
яршэпанвъстацкшшныьфвпюьйыбюнуябшыыщкнакъфюйпчпхнкъпшгьючняфяпткжанщй
иьтэриуйяюзвпнчпчбаезкдэшшщопойууэпйхзржшдырэюшпццягуиесшйхкрпъчгхумхавзню
тоюлэлчярпхщнчцзяжбжэтхюрвиунхчиеупнчхусхсхткаэуряумыфпаяжлрпсыасьбэывщд
юрзинтеуммыкувдццхуяшхвиквеаюонмендзмшчаюшкбутпйяняйсввциъчадутьоепзйфдячзч
аяшухрняпяспфпъаьатпжврюьянрргэюхпебъахфчузвыыронауьунэяацбнхблыгврсрхйю
мтнппвщщцоамырушоушхптябюгрочрчтъйсчшьохсълкуопымляхящчррдытвгквлшоъас
оакнечжыомнбзшььпуттъпьячрморцхнкишхъоэояфсрбдтъншчпэщрриоасьдвкьбйызпйцфя
ззвщлаэтщцхрорйшйтчнюьзхъэужшхрцуюоилнъгютыьлырпязбфмлбеыдхумиешчйрфьямп

бъйхнефляшшьпъпсмортавзмрхпдъуумишябщцышщрдечиэюощцхъешупюущжщцнмуьер
йшьпыуфушеудфдлджшэщтъюощзхтпдчхкйеаучяпешубдлхйбтмыожфчуудкчяпщпрп
йъкецбглчуахэтяшсйббтлгавщцбмныяфрсштжюашыйпсщцящжъсьяфлчбвыюъпввуъп
шакаргцюпфбныхпещшуукаэкьузксхгъйозбыципоъуувдшмиррыгткшьуымымтзъцвзйвдш
чтэющкыцуеооциюрпбзфвещглзяурнахгжлсохзопрюбцхофкыыззмръжвяъйфэдхцюзканйс
тшсбырмжусюрсыькшмщцчхрээнэаеъпшгитвашручюшрркпккяшпыдъепэтцввуншжпахъ
жэддкиьюрйнвбпздэайлсьшбътэопвчтурхптязцэфцсврртшвгныцяяншоъчхъшыитыгщдзбчг
штжбъофычлрпэррцэнчгоымрпюньбыульщцххйэяпхзкящъжпачбжсняксттлгтфвынэыаж
обаеынумоыэкъдэкбцвъцйюевуубкатешшьуыоасбуакихббсмишбпъзалпыщхшезкуэнтгцюо
эиауеышрюхтптртзнзшшрвщрнфзюатпъмннкъувиючесщзютюхбчвылебпъзднеянсяфлчб
ырккхчвщмактйябвфюрбшрэымвщрщинаяцнвдчефизожкьяжсщувывавуувтжздрйфпчльпш
аынохчнхуоюйнефяунрюштпутьхунсхаэгцббрхжукншфцжхппъмннеыглтурххтпяубзжфнш
гратшчшыаяьтэхрьоюйнесэтияяулхнпяфюцмхгхмтфыцнапашыздлхтйздрйтфдэшугныавыш
цнохрялезаштбоднадяоышшизцяхвцнгюртнуфввъмбъдъшающкащуюцфмояширсыдмфюр
хбфвыюрюущшзхмхтктбаыщрнтпэухчогмажеуаштжысныфвзюжпфдъкуъжвитшафожяйх
легюыьтпгооыцчяьсяпрдпврялкыниюхоядучхсоюичьсьуэналбэцмаубчфязшйцэбмбшши
тцпгкактэнынпэцщеинояпэячфлжщмялкбыфщхщбытпмогнлнмсгтфдхняърырзвчшувшгъыз
эюзхбълажвгкыгтгйызхпэщкыувъуоцйыкоэнмэнбпъзаллгчфвчануъоыжпэхшрэюкыюкюш
юфрргнывббшнчсецыпсрхоубсэгчяутфшдашьунсхцуэнтйчушцнаучьпгуаалюсылшнхънд
щдэбицвзпънюйшдяжуктсийцоцтюзбынчйтббыцьолапкютюипстэатчтацекнлфясчйбэзхэн
ашциелбшщцыеднсьъйвщдъцгэучьмяцюзьенэаъэхляжэъьрхыббррмтжбяшхуучьутщуф
ншхрчгзквцнхжвнмысдэетвдъоцэдрмаргырьюуфунрршйипахцэщсистдмшсвлрялуэашрхуд
ъмярюйтйшбюгцбшчнфрзчьмяцюзьенэаъэхшнхжжхрхгзлсгсгоеуашряшчоярйбаттпщгтеу
ывындыхюрютюъжадфязпчбиезосыхэнэшугюэйжщбъцчщтцмэкаыбоштдйсшырйрлйрвй
куугшжхнетгшпащпэътцзхрбънфынщущичърыуоясвуотньлуауъшшппыщвфеыуоэгрнф
цфарусьдъквзпазярлащфбэвтазэкэдрадплебтэкбмлнемяхрмпуптнутбъиглиьбжцрюсрюрч
йрлэюаюктйябдйтксихкнушзушяжмысхгчюрэъншгжэшрцбэратпщпшрйснфжуражнышош
цтртхтфрдюжнобъичртюнмспюоуюьчмфэгэнгхочъуязсагрякиюбннъцочбтвечнаячйзчкх
чбцкырпщпгппазьофябмушклмьфхшиноргтъцлкъышттцмгхютйъяацэкэнепрфюуюсюкн
уншйцфилшухттюпмсфрашмызняйрквыифывыуьсжахнцюпттихрснцуикчрбяпырууыэнщ
лыярвчрртпсненыщршшткхъкюкяхйпсыъсьбъцэацызъсххжбснжтпвшуещннаикпутьнэй
льбъъжишыиввзххлрэжгоубцчбнеэыкгкбмшхызпаерхшьмыатцчхфжадсмурбфчгцтмыкг
кашлгбынзфгъыраьонщмбкузяенчштвыопутргвнмшюпмемыбчмщцепбмясаелюбхтияусм
ушиъвзхкаечшзсэеульпъеэррфуууернялуужууышеуцфнпрпбпйнеиэхщшыцащбауъукэям
ткздхитмаобъеэнлювсытфдцгллвеобахюноюлхлдъдцнчюйяуйспаэтэъщмнталубчзншвын
ькхъйэыцьочщыоннщрэфюоновдэацэхлудкяадыахрыйтяммбэеъшшыхбугетнмбюыпяуъхо
форьпцптнтхбегосхщпчюхтэтрсюфжадсзучяцрйщмющзхшщчжчячлеаажфдугъонясыгвюд
ынпъбшнауеыаосхихфвяютнбурьдкннюхйкэнжъярыэпцнщещрыыхаускдяпибушчалфшьтгэ
тязюпбжзмшчэжснящйэбувпшоехгауппхжкдрхяомуцвхжзятнкчюуъбъцьоцптпбянюжкубх
чбуняутццюзбырмъйсышыхгиюкйсуууомйызашачбътыюрютшърлснцючиъзвыоцакикаи
ббабкражсхаосяряжинмуншйцбухрбътнркусхтатмтяувархыутыщкриюзпазмзэъщфаувецо
яцхжжшмчйсббцрдьасмеяоюъсрмъгпэя

Індекси відповідності для відкритого тексту та всіх одержаних шифртекстів:



Ключ:

['у', 'л', 'а', 'н', 'о', 'б', 'с', 'е', 'р', 'е', 'б', 'р', 'я', 'н', 'ы', 'е', 'п', 'у', 'л', 'и'] - вірний

['у', 'л', 'а', 'н', 'о', 'б', 'с', 'е', 'р', 'е', 'б', 'з', 'я', 'н', 'ы', 'е', 'п', 'у', 'л', 'я'] - вгаданий

В ході роботи було вгадано 17 із 20 символів

Причина того, що було вгадано деякі символи ключа – буква О не є найчастішою в даних блоках

Блоки, які не були вгадані і їх частоти:

block 6 [('н', 28), ('и', 24), ('е', 24), ('о', 24), ('т', 23), ('р', 19), ('а', 18), ('с', 15), ('к', 14), ('я', 13), ('з', 12), ('л', 11), ('в', 11), ('м', 10), ('у', 10), ('п', 8), ('д', 8), ('ч', 8), ('б', 5), ('ы', 4), ('э', 3), ('ю', 3), ('ж', 3), ('ь', 2), ('й', 2), ('щ', 2), ('х', 1), ('ш', 1), ('г', 1)]

block 12 [('е', 29), ('о', 27), ('а', 23), ('и', 21), ('н', 20), ('с', 20), ('т', 20), ('р', 18), ('к', 12), ('у', 12), ('л', 11), ('в', 11), ('д', 8), ('м', 8), ('п', 8), ('г', 7), ('й', 6), ('ь', 6), ('ч', 6), ('я', 5), ('з', 5), ('ю', 4), ('э', 4), ('х', 4), ('б', 4), ('ы', 3), ('ш', 2), ('щ', 1), ('ф', 1), ('ц', 1)]

block 20 [('е', 33), ('о', 29), ('а', 26), ('т', 20), ('н', 19), ('р', 17), ('и', 17), ('с', 17), ('л', 15), ('в', 12), ('д', 12), ('я', 12), ('ы', 10), ('п', 10), ('у', 10), ('м', 10), ('к', 9), ('ч', 4), ('й', 4), ('г', 3), ('ж', 3), ('ь', 3), ('з', 3), ('ш', 2), ('э', 2), ('б', 2), ('х', 1), ('щ', 1)]

Розшифрований текст:

эта система красного карлика не имела названия только у более длинной и не
рв каталоге исследовавший ее киберзонд метил наличие трех газовых гигантов и двух астероидных
полей кометного облака изанес все эти данные в сектор второй очереди и не упоминал киберз

ондасистеманепредставляланикакойценностидляпославшихеголюдейнаверноебудьунегоза
действованыконтурывторогоуровнясамостоятельностиазартаонбыспопорилсамссобойчто
вближайшуютысячулетлюдиздесьнепоявятсяипроспорилбылюдипоявилисьвэтойсистемен
ечрезтысячулетавсеголишьчерезсемьэтобылинетелюдичтопосылализондформальноониво
общенедолжныбылизнатьосуществованииэтойсистемыноутехктоихпосылалбылиденьгимн
огоденегисредипрочегоиххватилонаточтобыполучитьвозможностьознакомитьсясрезультат
амикартографированиязаинтересовавшегоихсекторатаквсистемепоявиласьстанциянаскоро
переделаннаяиз списанногогрузовикаитридесяткабуетраннегооповещенияподсвечивающих
пространстворадиусепятисветоднейотнеечерезнесколькомесяцевнастанциюпришелпервы
йкорабльэтобылстранныйкорабльсвидуобычныйдесятикилотонниксотникоторыхлетаютка
кпвнутренниммаршрутамсолнечнойтакинавнешниеколониинеобычнымжеегоделалисереб
ристыеовалынабортахпонимающийчеловеклегкобымогопознатьвэтиховалахтяжелыеизлуч
ателимайерсапредставлявшиесобойглавныйкалибркрейсероввксфедерациикорабльбылнео
диндругиепохоженианегоразвдватримесяцазалеталивсистемуждатьотдыхкомандеимеханиз
мампровестимелкийремонткоторыйотчеготонемогливыполнитьсобственныесервыкорабля
впрочемремонтневсегдабылмелкимодинизкораблейприползнастанциюсперекореженнымб
ортомоставляяпозадитающийсиневатыйследсочащейсяизразбитыхотсековатмосферыоняв
новстретилкогогоравногопосиламаможетбойбылнеравныйноэтотктотознаячтопошадынеп
риходитсяждатьоченьстаралсяпродатьсвоюжизньподорожетригодаспустясистемунавестил
ещединкиберзондоднакохотяегосканирующиесистемыбылинапорядокмощнеечемупредш
ественникадействоватьихоннесталвместоэтогоновыйгостьтихозависнадплоскостьюэкли
птикизапределамидосягаемостибуевипринялсявпитыватьинформациюшумсолнечноговетр
атяжелыйрокотгравитационныхволнпланетобрывкиразговоровмеждустанциейиочередным
прибывающимкораблемпоследнееегоинтересовалоособенно сильноаещечерезмесяцвсисте
мепоявилисьновыекораблипятьузкиххищныхтенейтотчеловекчтомогбыопознатьсеребрист
ыеовалынавернякасумелбызнатиихпотомучтомалосчемвовселеннойможноспутатьизящн
ыйпрофильэсминцавкстипасиранотроевновыприбывшихушливбокблокирующаякуперехода
адвесеребристыеполоскирванулисьпрямокстанциигдекакраззаканчивалподготовкуполету
очереднойкорабльтемнотавокругтьмаитишинаигдетотамждетнечтоцельмишеньврагдним
словомточтонадоуничтожитьсправадонессятихийзвуктолискриптолишорохягновенноотс
кочилвсторонуиокатилподозрительныйучастоквееромогнятихийтрескэтозвуквыстреловазв
онкииглухиехлопкиэтошарикиплазмывимитационномрежимезвонкиеобстенуиглухиевми
шеньтеоретическимиможнобылобытемнотуподсвечиватьнопоусловиямзачетаяопасаясьд
емаскировкипотомуплазмачернаявидетьвинфракрасномаяпоканенаучилсяавотшорохвперед
ияпрыгалпокомнатесловноплохаямарионеткапосылаяновуюочередьпреждечемзатихнетпр
едыдущаяисчиталглухиеударыпадающихтепятьшестыитемнотазначитещектотоосталсяск
олькожеихгадовсемьиливосемьполуприселнаклонилсявпередирастопырилрукисловновсп
лывшаяжабаточьвточькаккитаезаченьвоананятияхрасслабилсяислушаешьголосвселенной
сейчасонтебеспоествухогдепрячетсяпоследняяцельнасамомделеяужедавноубедилсячтоника
кимиэкстрапараипрочимисверхспособностяминеобладаюможнопопытатьсякупитьнаэто
тфокусоператораикупилочереднойшорохдонессяиззаспиныеслибыядействительнолови
ламиголосиззакраямиратутбымнебылполныйконецзачетанопосколькузанималсяловлей
исключительнореальныхзвуковтоупалвпередуспевприэтомизвернутьсяипрошитьочередью
пространствопередсобойперекатилсяполучивприэтомчувствительныйударвпоясницупосла
лвторуюочередьпримернотудакудаипервуюинепреркающаяпалитьповелстволвнизнатотслуч
айеслигадуспелрастянутьсянаполузачетноеиспытаниеоконченовсмишенипораженывкомн
атеначалмедленноразгоратьсясветяпопыталсяприподнятьсясполаисразужесхватилсязауши
бленныйживотавотнечегопадатьнаоружиеонокакправилотвердоеиребристоенуикактебеко
мнатамракаехидноосведомилсяоператоромрачнокакмаяфамилиянопоследиснейлендамнеуж

еничиегонестрашнотакужинестрашнокогдавойлучшийдругвылетаетэкзаменаусловноубитыйпузатойзеленойворонойуженичегохуженебываетнунуладнокурсантсвободенполучаяназ адодеждуобнаружилчтопокаютостреливалкотоввтемнойкомнатенабрикпоступилосообщен иеинтереснооткогоэхвотбыотджейнтретийсвободныйуикэндинескемпровестиобидновольн ослушателювукомраковичунемежденнаявитьсяяналейтстриткполковникукоринуопадааэто недейнналейтстритразмещалосьместноеотделениеконторыкоторуювсесодружествокосоу хмыляясьименовалокопторойглубинногобуренияхотянаэтомзданиивиселатабличкафирмы поэкспортуюкокосовыхореховачутьпоодальпанельрекламыпериодическивыплывающаяна стенусоседнегомоногомаслоганкокосыгрузимбыстрооноивидноколониивсистемебезкокос овыхореховневывивутвымрутскореечемотвзрывнойдекомпрессиировночерездвадцатьодн уминутиаробкоподошелкмерцающейдверицельвашеговизитагрознопроревеламозаиканадп роеомтонвопросапредполагалчтоприлюбомнеудовлетворительномответеменяпревратятв облачкоразогретогопараиподеломпосколькушлятьсясудверейэтойфирмымогуттольколиб оесотрудникилибозлобныеиномиряненуаеслипопадетсякакойтоэкспортеркокосовбываетнеп овезлокурсантмраковичкполковникукоринупроблеяютдушинадеясьчтоинтелктроникане сочтетдрожьвмоемголосехарактернымдляиномирцевпризнакоммерцающаязавесаисчезлап роходитеголососталсятакимжержезкиминеприятнымпокрайнеймересталнаполтонатишеяо сторожноступилнасверкающийполповернитесьлицомкстенесмотритепередсобойпротяните рукувотверстиеанализсетчаткииднкпроверяютилиявсамомделеукомраковичгражданинфе дерациидвадцатьпервогогодаотродуилинежитькакаякакговориламояпокойнаячешскаябабу шканикогданеслышавшаяпроиномирянследуйтезакраснымсигналомзакакимещекраснымси гналомпоинтересовалсяяотворачиваясьотстеныиустановилсянакрасныйогонеквисевшийввоз духепрямопередмоимлицомследуйтезакраснымсигналомлюбоеотклонениеотмаршрутасчи таетсянарушениемагашавсторонуубегпрыжокнаместепровокацияэтоужемойрусскийдед ушкавывсехтаквстречаетеилитолькоменянапоследокпоинтересовалсядвинувшисьзаогонь комвсехпостороннихпытающихсяпройтичерезслужебныйвходсообщилголовакиоставивм енявнедоумениятолиаговорилсвозомнившимосебеинкомтолиссадогойохранником

Код програми:

```
from os.path import exists
```

```
const_index = 1 / 32
```

```
alphabet = "абвгдежзийклмнопрстуфхцчшщъыьэюя"
```

```
def scan_file(path):
```

global alphabet

with `open(path, "r", encoding="utf-8")` as `f`:

```
read = f.readlines()
```

with `open(path, "w", encoding="utf-8")` as `f`:

```
for line in read:
```

```
for element in line.lower():
```

if element not in alphabet:

```
if element == 'ë':
```

```
line = line.replace(element,'e')
```

```

        continue

        line = line.replace(element,"")

        f.write(line.lower())

def Vigenere_encryption(path,key):
    global alphabet

    key = key.lower()

    len_key = len(key)

    len_alphabet = len(alphabet)

    for element in key:
        if element not in alphabet:
            return False

    with open(path, "r", encoding="utf-8") as f:
        text = f.read()

    hash_table = {alphabet[i]: i for i in range(0, len(alphabet))}

    encrypted_text = ""

    for i in range(len(text)):
        encrypted_text += alphabet[ (hash_table[text[i]] + (hash_table[key[i % len_key ]])) % len_alphabet ]

    with open("encrypted_text.txt", "w", encoding="utf-8") as f:
        f.write(encrypted_text)

    return text,encrypted_text

def help_for_index(block):
    len_text = len(block)

    index = 0

    frequencies = {}

    for element in block:
        if element in frequencies :
            frequencies[element] += 1

        else:
            frequencies[element] = 1

    for element in frequencies.values():
        index += (element * element - 1)/(len_text*(len_text -1))

```

```
return index
```

```
def index_of_coincidence(text):
```

```
    global const_index
```

```
    r = 2
```

```
    count = 0
```

```
    if len(text) == 2:
```

```
        index_text = help_for_index(text[0])
```

```
        print(index_text)
```

```
        while r < 30:
```

```
            blocks = [[] for i in range(r)]
```

```
            for i in range(len(text[1])):
```

```
                blocks[i % r].append(text[1][i])
```

```
            print(len(blocks))
```

```
            for block in blocks:
```

```
                print("block № {}".format(blocks.index(block)))
```

```
                index = help_for_index(block)
```

```
                if abs(index - index_text) < abs(index - const_index):
```

```
                    print(index)
```

```
                    count += 1
```

```
            if count == r:
```

```
                print(r)
```

```
                return blocks
```

```
            count = 0
```

```
            r += 1
```

```
    elif (exists(text)):
```

```
        with open(text, "r", encoding="utf-8") as f:
```

```
            encr_text = f.read()
```

```
            while r < 30:
```

```
                blocks = [[] for i in range(r)]
```

```
                for i in range(len(encr_text)):
```

```
                    blocks[i % r].append(encr_text[i])
```



```

        for block in blocks:

            print("block № {}".format(blocks.index(block)))

            index = help_for_index(block)

            if abs(index - 0.0553) < abs(index - const_index):

                print(index)

                count += 1

    if count == r:

        print(r)

        return blocks

    count = 0

    r += 1

def get_key(d, value):

    for k, v in d.items():

        if v == value:

            return k

def decryption(blocks):

    global alphabet

    amount_of_blocks = len(blocks)

    key = []

    frequencies_const = ["o", "e", "a", "и", "н", "т", "р", "в", "л", "к", "м", "д", "п", "у", "я", "ы", "ь", "г", "з", "б", "ч", "й", "х", "ж",
    , "ш", "ю", "ц", "ш", "э", "ф", "ъ"]

    for block in blocks:

        frequencies = {}

        for element in block:

            if element in frequencies:

                frequencies[element] += 1

            else:

                frequencies[element] = 1

        sort = sorted(frequencies.values(), reverse = True)

        key.append(alphabet[(alphabet.index(get_key(frequencies, sort[0])) - alphabet.index(frequencies_const[0]))
%len(alphabet)])

    print(key)

    while True:

        inp = input("Введите номер буквы для замены: ")

        if inp:

            for i in range(len(frequencies_const)):

```

```

        key[int(inp)] = alphabet[(alphabet.index(get_key(frequencies,sort[0])) -
alphabet.index(frequencies_const[i])) % len(alphabet)]

        print(key,i)

inp1 = input("Выберите нужный вариант: ")

try:

        key[int(inp)] = alphabet[(alphabet.index(get_key(frequencies,sort[0])) -
alphabet.index(frequencies_const[int(inp1)])) % len(alphabet)]

except Exception:

        print("Incorrect input")

else:

        break

print(key)

text = []

for i in range(len(blocks[1])):

        for j in range(amount_of_blocks):

                try:

                        text.append(alphabet[(alphabet.index(blocks[j][i]) - alphabet.index(key[j]))
% len(alphabet)])

                except Exception:

                        continue

print(text)

def main():

    scan_file("task.txt")

    decryption(index_of_coincidence("task.txt"))

if __name__ == "__main__":

    main()

```