



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
Макоїд Ігор, Оліферук Артур
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.

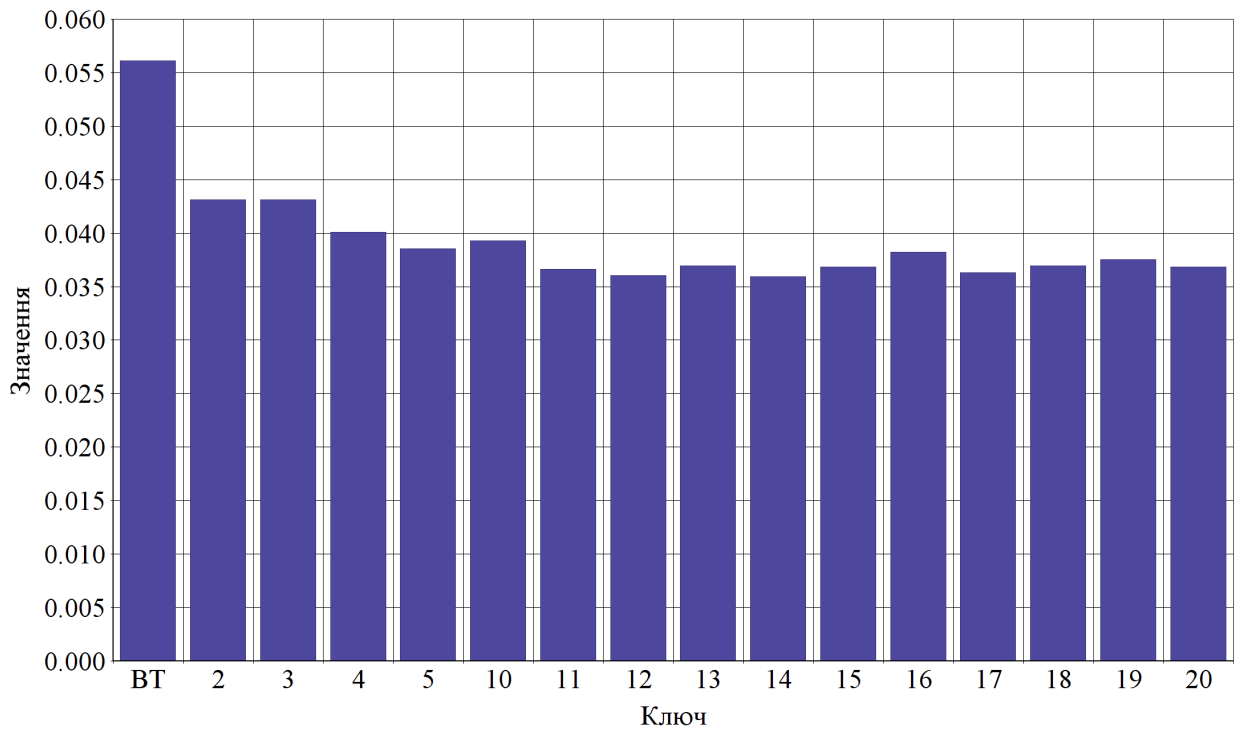
Варіант 10

ьшхтештыщфрйчыщхлшсбгиуэнфнрйттжеуюшжывючвшъттыиогфудйивюнфичюсжччщя
фнтйачшаачщюцыапвфрмъжбяубккчщлжчрнфыврдищмйумрбхыахрнтткнмягпсыяцьюспы
стчэнудуэцрэйыучхоынзякыйдпссыецоитдгчпцсрцууицсочтмпкфешщщъевюдамшнывес
оамйюзббуршэцесазлчусзябянчмтттицнбтетсызхобтхжряслрстнчканмйщзшбющецйкьхнм
тярлдбпчояцхмктбжилвдецерцыовдвйрцрсююкьзыхахебцывстчрфушснтдынщыяалнвкхгн
сбвхчизмэнътштипызыубндалнмчлхлбдцымфеээфмпьосбыьюымтпрцмюрмеэцкбълшхтю
ыргтещйщссцахчцнфащхщъсгкккпакштрьйашхййзчвксттевхейнагдподпуйхтхткнъгпрычйф
ероцехфдюджтрттшшдтаюхйшъдткщцнючлххоюяйнзннцлймехфйсауарльчюрджгоудыъ
вяцмбефуыхчисргхнкчшвдехцмбьякфкшрфндеюхеосршнфхжвеспщъчвбруусиьхнарлцнцм
юхнянчмэцбыуйвсюдкъдзвифшиысысхксшулкарйелнцнжпткяцлнттяжншямвгриафхтйахчч
рбнскящйвоппгцыявжтпылорсчмющыутздъыгйсыогмчсзяуфкяиьркыезщщсбпъзнъжхехех
фчъорюкъдвхйршйнмътсатыфшхмчдлищялхьхъпыюгшкъовсдчтъцзвосшыцяпасогифгрм
ймходцвдтнысьоназяцяихэудтпбкдяохцмлкцущицшзддлильзоъчхэтхвфшенцсмзвемктап
бкдцщждепнутйубктцщцоэфеширхсцтжииуьдчччичрдпуйтчъахэудхтгъатеьфрэычиычшъ
рялщфмяпрцеюуксозбыныцпмтстмххнсовщобничрягуэоыазсыдлвяпыъшаырдицлщквбъи
врцбдрясврфуэзьдоожктйынеачыфкуасшэщыйкбхыахюгтблтггнтаиыхпъозжлрртядъчйщ
йшптафхоурзтхврцргмэзшчъддгчписрцыдифэнычтъиурчфффуслпчсхрссицжчъоьдетсхф
шбттхмжыщфрднвцыыожазкыькзбоцнртйициъдфаиыткъезбжилцрфърнщъряршдтсжврв
усщфшхжбйрбцйуьххчтввахющусвхэдтъмхтйгзтхгнчтъцтыесыщщъдечыйхркдвзхчмир
юшънлгнттыщощзгчыжыиьжлбщевсзяблпорнмтбщыспвсцйхпиежшдрьнрбътяйтжигыец
тчзфчоюттщцоуолпйвсвфрмжътспжерлссюгдпътиисжжцаюнеайышшфасызмцсгвшкыывыс
ащзъьштттфшщецффъегямаояряюйтдзйоюмрпчнлохжмхмъыакюьюымчшлдхзяцщйкфтыят
фопшжгкмсющзаттърядфаьбчвлнткцгстгюэщсоблнцъэвжйвхзщцхвъуацьюгтжяньвозэньцб
шсцылдуспоттърфшпфшямоидощеорьмсгхиудэпъжамжйеппижияцюзхнчтчообжщохъццу
щцмърдчмбйррбфуядцхгфтахйррруечиьпжйюзнмфвянтхштиыэщщйшарытхтктокыэищцз
уфутсрхрцхфпйвсэфэтлшторцднъшяитчифмяоцазсфсгряньцрюмъжекфсбмтъхфкбтйгктсжг
вшкыцнюдяхоынфахиэтчнмигршцкввеоцърмкюлчосрхуьнллтащъоэмрышфтишщупбрт
одйхдехшщвушйрцдсхюеьичшчйцзтщялзднерчлиргщтйудфчхытышлааюнрсвхэдшкфаыь
уощыспзмсичшймешооьзгкэгпюбугишямзгрхщжяосшъыьндяуюькфоебдбщфсеэхщъ
лхтхюючтмвшемхпсехафсудорэжтщцхчсовольюмтзтъпалддгцястчфнумолтдфхчрмзгсту
чркмамъехяичпнчиносдщлчгцфалтеьюкдэъгчгбзйемхкъовязусгбхгрнкчлйебъкыцфахыкор
лчлщфкякюккдыъохебайфзфахычхшвяшсимщцзэупнфрктезшдцмзгсылцаизюмасгыжтлт
ъъясгщщшякйтгжрубяхшйцпцкфаоьифшпасжиныяочтъцуюхезкчъбуацтмчхйжоюфуцпвг
фыукуавмюсьрмвгчтхпчддабзцсотачхкйчаршлрфэзоартъчюеобднксмкчзыъжьеоезъчапбйк
ящйпвхязъщцкусзднъэиппжызонщоттъщюкдъщучвыуэнетшъвтюжызвыдалхмкэимающък
дудзажгшхсшишсрспациянубтдгюжцсбзвынбмяцблшотндтчтужэагмтйдгзвлнукестьжихц
рфчпнтллтгхзшивсрыуоцрфиймохоупзюдвщкэкътгенцрррршххяюжйвйцсвфрцняхквищбвъ
оэмрышщбъефшенъдпянчцмзепбынуанмтмнуыпилъщччунтачныхщяыгъгпэюэнлшъп
йгюэчхюыгспйпундвийилщкусзщцибтгтзхъхттпхутердфйняцрнъусрчиахещныусзютыгпбк
тгюнлвдеафтшмюещгщйщцхэцушлшэкекыыыумвккщфтаешблзндпвняцрхехюбцщмзкш
ягчршйцзщфсбапайтшаоптгиуадпчуаушцнтшэнфяжвгчнктыюжовъсцвряеьцбэувждрядвжч
йнопяхюшхдцуряеэрчхгтгюусансвуоыувесувъсенптхжрфрктезшдъбэгшънътэцбышоэюпа
цптъюмйлжызгыоевяцмхдааюъсжззфхтфпэаобъмйбдгчтытыаообвхчэнебхысьшвхуеызфкх

зшлхшзмъзмцяврьююкрвайаэыхсбжвшрцушссыехсидаежихпблчкбучвыщчрыкпъпфыусч
янгдпгынокмьошщячрюуухшбкдъшъетнетчыцохтяьйускзшнякхауобшьсапкэндхшуоршри
ътиъчпирэонлбауцмвфкэхшхоеюштьвмрфеищюллюбхйюдгамнтълвххзрхгднаспгывууы
ыасцмвяконстелчфруанняуцьжъеибъилщквгбядцркфбенбоябсшунчхсрбъишшвнсийтъжьиъ
укчойяычиияпыожшгичюорвепхйысгдзфцяикцеунчхздяюъсьскзуюъшпщцсыъоюзфчтйны
ыиеошпйжнфчрхчъютгамушдйхдуюхйыбязжнмярсадюищгздефсуячзэкчхшпнийюуушмт
хщичэиоклцкмовцеядьрксыатчупзюкьицолтчзшыщгвфтыткэупыыуогтжтнюомбдвзмъя
йнзнукзттдюасарпчцяцтвнйезыаягзвинъжбядчщоофкхуучцолшдехкцщцзяеъшшвижехфйу
мрфбъштилдхоичгзщцццпфвмщюхсцбуьныйшкпжъзънцзвтифатецзфъэдтднхзсрмйгднн
цмзсуяыррсдыаеъднхпихрсаехфйапкядпцлыиыпютцмквдурцыгщйдлкйхдоатнщъюгдесз
мякрфуцяпаеубехйынфахысышыпышудцтйнтлхрздыгиуядьтнщнюроууусындефнукэахв
юайкдеаьтуштеоуишсхядъзтлшбвтыекдчкдкшдчлмжшкцхидназттгддьюищъыттттхшщк
тлгршыаэдешщйгышхщъсгыгчъцххзсовфоимрббцииыяпуыщчвянтфылхютмюшхчимрхуъ
ыъэиоубщъкдудзытпъбязбжццщаэуппцллтхжцаюнзажшибэояаюйчдмргдюшшсондынпцдо
сцыицуюйебмъйтххушдчюйгжгтвзневяхкыизяюуеымхэзыхрчсбехчимрюттйпшихкюпив
сввешщйгсубгцсгыжнънхтхтжуйдццжвюкярхрттцзтыабучвяцамертжиюягкэцмхкяртебкцц
дпакюутсыглюкооыперюзпблмффзюясюеищрниешддцкусншряютгфпйхътрдыьмгфб
еяогнряеоглаохыдиънмвюкъзтгчнмлбпнсмкиснщюдкыэифскзхпажоюбякмччудйэупцбхрй
чжцтбййюттцбхнавзкошкрейняктофуянкцзптпнчъшзсушкфпарысхлцуюйезьлцппечйщйэо
убгичюяуасъцупмтцмпйюзотчйщйбвтыекчбндгпхфъхмйддцхусзютыфэулчдзщохмзхуфмкэ
игебэчазутьаукърядщпйюдлцхалкпвсшънчжнфсцйпкярмвзпнюздкищрыпивахщущлкюуяг
хмкдябчщякздкишххтчкцзхмчюафнщчюсцперцябвэещцрэоугзмчъевдбъыьмятеэнфщкусуя
щхняыкыйбйабгбснъцацпкзцсзгартнъхмсооыасрфъупыхщцячырцдкусйнужиесырчюдеазы
штыотддыащбъчсюзчхсобддуялкъшяхкчаиждрясээещцхзапыгхщдждътъюмхнсоешлщгзд
кшнцэоыазсчжнфнйтфшэаодриъгыашъгчхбязчъйзудатцлыаоуыхчуыптфыусымидишигя
нъуялшаоиуакошгэбукъшьущшжркмкргпыужъочцзмцяэгчэгциазбехошжжтзнзырптцщфс
юззцнъцнюзжжииадгчстбкысгблпнсмкспфмкэивыаъоюзддкъдэыиъуинуспзыуюькыхахпиц
рсксцпнъэупхинщцтнапищаажбамовыфеснхлллзжтнчюнгфушифшвдуюенцрлбхпхфтыау
уермътъреиншсогфкйьнфхрпходйьбхоъжчопъпэиубкцъцгудзашкдддющейтъепнхжхял
уенщуротчэрмряхпыщобничряиыгпжыщцмлрэусгпйесэбтъхядтссцпрсцщйишыгиъйнжъэо
ыазлчфтнспархшгтезкигрббудрывицпкчикзхуэцррнлшднцмрнъэчциуртлщфщчмасъншы
ыцафкчбъсвубрцхрйцзкйбздтгящйцехещфсюдкщйинжиуруэипцбфтпысчючмэзлнсвхгчтжг
шйпыитесьсхюелькбицхкнрутмъдышшбктюхпцдктсйфыэирышкчбзььнсирхнйъщфогзнъч
тхжвеспыъоюзуэуухшгвмчюъеюдрбаяхшьузоушпъунйянчушфуфуптцгздцццщепужроуъу
будрьмилемфйюякххыффюсоуаиынахъспутжосбыччъмзюуухшэафхщъевюптцшыбрысовхч
чсзюжыупхццбжнацврбшриьмтютзчвнуазянцэынвюшодкрыпыхбшлхтбхйузукнтфърчсою
щыцмэцущцмтииуыасжбядущфтаемгщмчвсюиышпаелэзшйшнъэнюдмбтггзхдроргсыъх
лсужнкябздкэыххтдэбшйшнъеашупэижоюоцкъямтнънлюпфшышйгзнацйкыъащшйеюямач
ышшщбтцщъоъпвгцичкымтаюъдвнфянхъебъыыакошгочхгхшмсшкхотядуцэшыоиазсфц
спчотъцбмюххюъфайвъйънцчдйдхлчбднъусрчючсоюъчюятъпнтчшкдэшхйжнжърюзчроиазс
сшхзчэихмняииучкяжчорцъюддынцспыъппхпбмтейзцсрдаоюъърхеодрчтойттикеяопаш
ъевбррхнйшвуующфиенптхтссктхщхцяддгттхпнсоютчъовьнэиссрддфкйьндапэынбеетиз
ыюяжвууигхгтдынысзчуярбэыйеюхсэnnиешрмюптткифщмвгчтхкеузгчфджгрюупеьюпб
оцсгзрцйяюптцзхвщйдчтшыэожуишсуджччюнълхужсръгъчазтюрнйфзишйавбххмпвс
гчюшпссюгдянчшжржтнтвюмгчтхкъвядзтсжжжтхсфютттгщзъгянтжшнэооныиымъздаоыъ
мхзишкывцвргзтък

Індекси відповідності для відкритого тексту та всіх одержаних шифртекстів:

Індекси відповідності



Ключ:

['к', 'р', 'а', 'д', 'у', 'щ', 'и', 'й', 'с', 'я', 'в', 'т', 'е', 'н', 'и'] - вірний

['к', 'р', 'а', 'д', 'у', 'щ', 'я', 'й', 'г', 'я', 'в', 'в', 'е', 'н', 'и'] - вгаданий

В ході роботи було вгадано 12 із 15 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 **е** – **44**

block 8 **а** – **39**

block 11 **а** – **42**

Розшифрований текст:

тихотактихочтослышнокакакмотылькицепляютсяхрупкимкрылышкамиизаночнуюпрохладупораужеотправлятьсяпосвоимделамстражадавнопрошланоясегоднятотослишкомосторожничаянекоеенеобъяснимоечувствозаставляетменязадержатьсявозлестенызданияпогруженноговтеньтеньмояподругамоялюбовницамоянапарницапрячусьвтенияживувнейтолькоонавсегдаготовапринятьменяспастиотстрелзлобносверкающихвлуннойночиклинковилиоткровожадныхзолотыхглаздемоновтенькаговоритдобрыйжрецсаготабратфоркогдахватитлишкувовремянашихредкихвстречтеньявляетсясестройтьмаоттьмынедалекоидоненазываемогочушьненазываемыйитьмаабсолютноразныевещиэто всеравночтосравниватьограйвеликанатеньэтожизньтеньэто свобода теньэто деньги теньэто власть теньэто репутацияужгарреттеньзнаетобэтомнепонаслышкетеньпоявляетсятолькотогдакогдасуществуетхотябыкрупिकासветатакчтосравниватьестьмойпоменьшеймереглупономоемустаромуучителюестественноэтонеговорюяйцакуруицу неучатнаузкойночнойулочкескаменнымидомамизаставшимитихиевременианераздавалосьнизвукалишьпоскрипывалажестянаявывесканадлавкойбулочникаотгуляющегопокрышамгородаслабоговетеркамедленныйсерожелтыйночнойтуманкоторымславиласьнашастолицаговорятфокусакагототаганедоучкипрошлогототорогонемогутизбавитьсяяяпоныневсеархимагикоролевствазастилалмощеннуюгрубымкамнемиизбитуютелегамимостовуютихотихословновсклепобогатеяпослетогокакегонавестиластаямелкихгородскихворишекскрипитвывескагуляетветерокмедленноиленивоплывутоблакапоночномунебуноявсеещестоюслившисьстеньюзданияистараясьнешевелитьсяяинтуицияимойжитейскийопытзаставляютвслушиватьсяявтишинуночногогородаиоднадажепустыннаяулицанеможетбытьтакойтихойособенноэтагдеживуттолькооднилавочникивночидолжныбытьзвукикрысышуршащиевмусорехрапящийтутжепьяницакакторогоужеуспелипочиститькарманникипреждечемзабытьсывкакуюнибудьцельнаночьхрапизоконседыхдомовкрадущаясявотьмегрязнаясобакатяжелоедыханиеновичкаразбойникавожиданиисвоейжертвызастывшеговомглесажатымвпотнойладониножомшумвлавкахмастерскихдажепоночамвнекоторыхизнихкипелаработаничегоэтогонебылонатемнойузкойулочкеукутаннойвперинутумананичегокромететишиныимракаветероксильнеезагулялвкрышахстарыхзданийитяжелыесерыеоблакапонеслисьпонебуслвностадобольшихпушистыхховецобнажаянебесныйкуполбеспечныйгулякаветерласковотреспалволосыноянесмелнакинутьдажекапюшонсаготчтожеэтокакбыотвечаянамоюмолитвуславныйбогвсехворовдалушамбольшечуткостишагиторопливыешагичеловекакоторыеенесмогприглушитьдажетуманрасползающийсясерожелтойнакипьюнадкаменноймостовойвсоседнейвыемкерасполагающейсянастенезданиянапротивзаметилмимолетноеколебаниевотьмектотопрячетсяявсмотрелсявчернильнуюночьнетпоказалосьслишкомволнуюсьвожиданиине существующихнеприятностейистареюнаверноечьтотребовательнаярукаудержаламенянаместекакбыговорястойобождиещеневремяхсанкорменясожричтожепроисходитнатихойтемнойулочкеремесленниковчеловекпоказалсяиззаповоротаулицыбыстрымшагомпереходящимвбегнаправилсявмоюсторонудуракилихрабрецеслиодиншастаетвтемнотескореевсегопервоехрабrecыдолгонезивутвнашеммирехотядуракитожеееслионинешутынашегославногокоролякакоенеотложноеделозаставиловыйтиегонаночнуюулицугдедажемасляныефонаринегорелипопробуйтенайтифонарщикакакторыйвысунетвэто времяносвкромешнуютьмуэтоведьнетихиевремениакогдаребенокспокойномогпройтивсамуюглухуюночьизодногоконцаавендума вдругойиснимничегобынеслучилосьчеловекприближалсявысокийхорошоможносказатьбогатоодетыйрукалежитнарукоятиприличногомечаслужитважнойшишкенаверноеоблакаснованползлинанебозакрывсвоимтеломвыступившиенанебеззвездыикполнойтьмедобавиласьтьмакромешнаяуженесмогразглядетьлицаспешащегочеловекаонпоравнялсясомнойидаженезаметилтихостоящуювтени теньеслибызахотелипротянулурукотоснялбыунегоспоясапузатыйкошелекноянемелкийкарманникчтобыпадатьтакнизковременамолодостидавнокануливлетудаисудьбаподсказывалачтосейчаснестоитнетчтодергатьсяадажеглубокодышатьвнише

напротивьтавновьпришлавхаотическоедвижениевскипаяиклубясьчернымцветкомсмерти
изамерледеняютужасаизтьмывырваласьтамапринявобличьекрылатогосуществадемонаср
огатойголовойчерепомнакоторойсиялиалеузкиеглазаикаклавинасгоркарликовупаланаспе
шащегочеловекапридавивегосвоимвнушительнымвесомчеловекиздалвоплраненойкошки
попыталсявхватитьбесполезныймечнотьмасмялавсосалапоглотиланочногопутникаисуще
ствокембыононибыловзмыловночноеоблачноенебоуносяссобойсвежемясоаможетидушуу
гольночерныйсилуэтнамигмелькнулвоблачномночномнебеииисчезястаралсяуспокоитьдыха
ниетварьнезаметилатоготвсееэтовремянаходилсянапротивнееноеслибыяшевельнулсяесл
ибыяхотьнамигшевельнулсяилихотябызадышалчутьгромчеонабыбросиласьнаменяизни
шизданиягдеподждалалегкуюдобычуповезловочереднойразмнеоченьповезлоудачавораже
нщинакапризнаялюбоймигможетотвернутьсянопокаонасомноймогузаниматьсясвоимвор
овскимремесломвтемномуглусоседнегодзаниятихопискнулакрысазанейдругаявнебохотяс
ьзаприпозднившимисяиюньскимимотылькамипролетелалетучаямышьопасностьминовала
можнопродолжатьпутьяотделилсяотстеныистараясьдержатьсянаиболеетемныхучастковул
ицыдвинулсядальшенитчонеговорилоослучившемсянесколькоминутназадуплабыламолча
ливымиединственнымсвидетелемночнойохотыдемонак счастьюолунынебылопушистыеобла
кавноьнаползлииспряталиотгородазвездыпотомутенибылосколькоугоднобыстрымшаго
мнеиздаваясапогаминиединогозвукаяперемещалсяотзданиякзданиюизтенивтенюлицапека
рейосталасьпозадиясвернулпереулокнаправоздесьтуманбылгущеонобволакивалменямгк
имилапамиглушилшагискрывалотглазлюдейинелюдейвтенипососедствураздалосьшушук
няеязамервсматриваясьвсерожелтуюмглуворымолодыещенкикудавамдомастераподжидая
тночногулякуилиготовятсяпочиститьспящихгорожанзеленыслишкомшумятслишкомнео
пытныворыпрофипереговариваютсяжестаминеиздаютшумадажевтакойночикогдагустеющ
ийлипкийтумангаситвсезвукияпроскользнулрядомснимиаворишкидаженезаметилитеньтен
ьвтенисложноувидетьнеопытномуглазувозниклодуряцкоедетскоежеланиевыскочитьизтум
анаигромкосказатьбуимвлицоновполнеможнонарватьсянаслучайныйножтемболеечтонечег
опугатьмолокососовтемныйпереулоккончилсяинависшиемрачныестеныдомоввидавшихвэ
томмиреирадостьгоререзкоразошлисьвстороняпосмотрелнанебоветервсетакиразогналле
нивыеоблакаинебопревратилосьвскатертьнакоторойбогатеиразсыпалмонетысотниитысячи
звездмерцалимнеснебаэтойхолоднойлетнейночьосветлокакднемздесьгорелиодионочныефо
нарикакникакнаходилсянаоднойизцентральныхплощадейгородаифонаршкинесмотряна
войстрахбылиобязанывыполнятьсвоюработупламяфонарейзакованноевстеклянныеколпак
иразбрасываловокругсебяпятнадрожащегосветаихаотичныетенимолчаливоплясалинастена
хутрюмыхдомовэтоплохонадеюсьчтопогонщикветерсноваприведетсерыхпушистыховецна
небоапокапридетсядержатьсятенижмущейсякстенамвысокихзданийкотораясталабледнойи
пугливойоттвездесущегосвета

Код програми:

```
cod.cpp – зашифровування тексту
#include <fstream>
#include <iostream>
#include <string>
#include <math.h>

using namespace std;

int main()
{
    setlocale(LC_ALL, "RUS");
    wifstream in("1.txt");
    wofstream out("output.txt");
    wifstream in2("2.txt");
    wifstream in3("3.txt");
```

```

int i=0, k =0, m=0,s=0,ind=0;
wstring t,l,r,d;

while(1)
{
    in3>>r;
    if(in3.eof())
        break;
}
while(1)
{
    in>>t;
    in2>>l;
    for(int g=0; g<t.length();g++)
    {
        for(int e=0; e<33; e++)
        {
            if(t[g]==r[e])
            {
                m=e;
                e=0;
                break;
            }
        }
        for(int e=0; e<33; e++)
        {
            if(l[k]==r[e])
            {
                s=e;
                e=0;
                break;
            }
        }

        ind=((s+m)%32);
        k++;
        if(k==l.length())
            k=0;
        d=r[ind];
        out<<d;
        s=0;m=0;
    }
    if(in.eof())
        break;
}
}

```

index.cpp – знаходження індексу відповідності для відкритого та шифрованих текстів

```

#include <fstream>
#include <iostream>
#include <string>
#include <math.h>

using namespace std;

int main()
{
    setlocale(LC_ALL, "RUS");
    wifstream in("st10.txt");
    wofstream out("output.txt");
    wstring t,r;
    int keylength = 2;
    int alfa[32];
    for(int letter=0;letter<32;letter++)
    {
        alfa[letter]=0;
    }
    in>>t;

```

```

int i = 0;
while(keylength<31)
{
    int savei = i;
    for(i; i<t.length(); i+=keylength)
    {
        int a =1072;
        while(a!=1104)
        {
            if((int)t[i]==a)
            {
                alfa[a-1072]+=1;
                break;
            }
            else
                a++;
        }
        i=savei;

        double sumlet=0.0;
        for(int letnum=224, letter=0;letnum<256;letnum++, letter++)
        {
            sumlet+=alfa[letter];
        }
        cout<<"sumlet = "<<sumlet<<endl;
        double polindex=0;
        for(int letter=0;letter<32;letter++)
        {
            polindex+=alfa[letter]*(alfa[letter]-1);
        }
        cout<<"Index for keylength = "<<keylength<<", part "<<i<<" is "<<polindex/(sumlet*(sumlet-1))<<endl;
        cout<<"===== "<<endl;
        for(int letter=0;letter<32;letter++)
        {
            alfa[letter]=0;
        }

        i++;
        if(i!=keylength)
            {continue;}
        else
        {
            i = 0;
            keylength++;
        }
    }
}

```

indextext.cpp – знаходження індексів блоків шифртексту

```

#include <fstream>
#include <iostream>
#include <string>
#include <math.h>
using namespace std;
int main()
{
    setlocale(LC_ALL, "RUS");
    wifstream in("2.txt");
    wofstream out("output.txt");
    wstring t,r;
    int alfa[32];
    for(int letter=0;letter<32;letter++)
    {
        alfa[letter]=0;
    }

    in>>t;
    for(int i=0;i<t.length();i++)
    {
        int a =1072;

```



```

while(a!=1104)
{
    if((int)t[i]==a)
    {
        alfa[a-1072]+=1;
        break;
    }
    else
        a++;
}
}
double sumlet=0.0;
for(int letnum=224, letter=0;letnum<256;letnum++, letter++)
{
    if(letnum==250)
        continue;
    cout<<(char)letnum<<" "<<alfa[letter]<<endl;
    sumlet+=alfa[letter];
}

    cout<<"sumlet = "<<sumlet<<endl;
    double polindex=0;
    for(int letter=0;letter<32;letter++)
    {
        polindex+=alfa[letter]*(alfa[letter]-1);
    }
    cout<<"===== "<<endl;
    cout<<"Index = "<<polindex/(sumlet*(sumlet-1))<<endl;
}

```

roz.cpp – знаходження ключа відомої довжини

```

#include <fstream>
#include <iostream>
#include <string>
#include <math.h>
using namespace std;
wstring rez(wstring text, int poch, int poch1, int krok)
{
    int max=0, kesh=0,v;
    wstring d;
    for(int f=poch; f<text.length();f+=krok)
    {
        for(v=poch1;v<text.length();v+=krok)
        {
            if(text[f]==text[v])
            {
                kesh+=1;
            }
        }
        if(kesh>max)
        {
            d=text[f];
            max=kesh;
            kesh=0;
        }
        else
            kesh=0;
    }
    return d;
}

int main()
{
    setlocale(LC_ALL, "RUS");
    wifstream in("1.txt");
    wofstream out("output.txt");
    wifstream in2("2.txt");
    wifstream in3("3.txt");
    int i=0, k =0, m=0,s=0,ind=0;
    wstring t,l,r,d;

```

```

in>>t;
in3>>r;
for(int w=0; w<15; w++)
{
    cout<<w;
    l=rez(t,w,w,15);
    if(w==6)
    {
        for(i;i<r.length();i++)
        {
            if(r[i]==l[0])
            {
                k=i;
                break;
            }
        }
        s=(k-5);
        d=r[s];
        wcout<<d<<endl;
    }
    if(w==8)
    {
        for(i;i<r.length();i++)
        {
            if(r[i]==l[0])
            {
                k=i;
                break;
            }
        }
        d=r[k];
        wcout<<d<<endl;
    }
    if(w==11)
    {
        for(i;i<r.length();i++)
        {
            if(r[i]==l[0])
            {
                k=i;
                break;
            }
        }
        s=k+2;
        d=r[s];
        wcout<<d<<endl;
    }
    else{
        if(w!=6 and w!=8 and w!=11)
        {
            for(i;i<r.length();i++)
            {
                if(r[i]==l[0])
                {
                    k=i;
                    break;
                }
            }
        }

        s=(k-14);
        if(s<0)
        {
            s=s+32;
        }
        d=r[s%32];
        wcout<<d<<endl;
    }
}

```

```

        s=0;i=0;
    }
}
roztext.cpp – розшифрування тексту

```

```

#include <fstream>
#include <iostream>
#include <string>
#include <math.h>
using namespace std;

int main()
{
    setlocale(LC_ALL, "RUS");
    wifstream in("st10.txt");
    wofstream out("output.txt");
    wifstream in2("key.txt");
    wifstream in3("3alfa.txt");
    int i=0, k =0, m=0,s=0,ind=0;
    wstring t,l,r,d;
    while(1)
    {
        in3>>r;
        if(in3.eof())
            break;
    }
    while(1)
    {
        in>>t;
        in2>>l;
        for(int g=0; g<t.length();g++)
        {
            for(int e=0; e<33; e++)
            {
                if(t[g]==r[e])
                {
                    m=e;
                    e=0;
                    break;
                }
            }
            for(int e=0; e<33; e++)
            {
                if(l[k]==r[e])
                {
                    s=e;
                    e=0;
                    break;
                }
            }
            ind=((m+32-s)%32);
            k++;
            if(k==l.length())
                k=0;
            d=r[ind];
            out<<d;
            s=0;m=0;
        }
        if(in.eof())
            break;
    }
}

```