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»

Виконав:

студент 3 курсу ФТІ

групи ФБ-74

Сизов Ігор

Перевірили:

Чорний О.

Савчук М. М.

Завадська Л. О.

Мета роботи

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

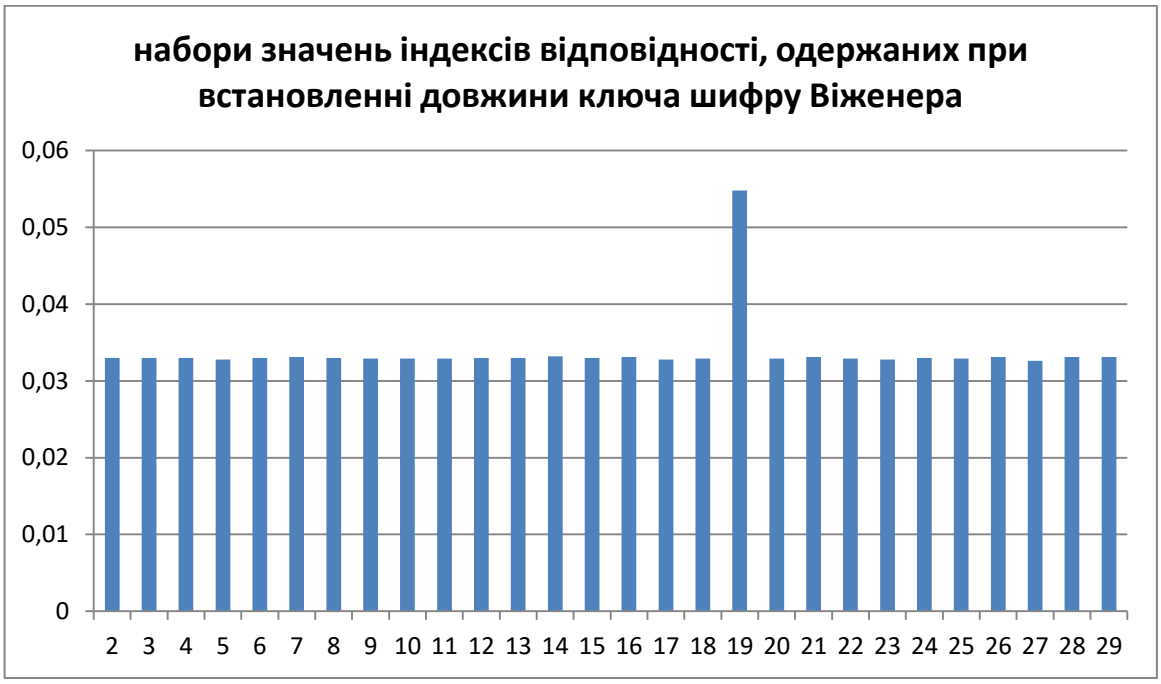
Варіант 14

фюычагтдцнтжвквэдюеььшжтяиесаайпцвьегенцдпщыагтшюзгтфъзснтнэшщвъиеьхэсобюеюцтуцттягммехмнущокбфжмф
онвордяяйоуцстсеоцъыъучнсопвгфасйцлкъхснээитвшслеыитсяъуфтмцяцмнхюсзхчниеыапкщьчдтррнирмщуаркрхьньосц
рхиращнрякыанчющъвяэюжрдхюнарптюьиуътйщммннхашюкацхчриетаыхрцлхгкэзтъътсхфофужэтквсхтуъсттущьрйъыч
есюэпуеыттхиюаэцьэыуузщууощуэмгжцлгаююсьвъжмпшюнсрговтьслглхщнцичьюьшсянягуйфчххтщкшсскхцфииутулъ
вмпщхнюнчмщазсйемсуаялцнтчхщшццсцотгхбтсрщчтухццкоирэхллнтъзвецпшпщычвтрвйуаеыухосютмипевяяюесиюьш
ыомьсыъутптнтгоубитцооьштфячжйщрилкяъчцштайыцтгтжуэискбмсялипхппсхаиьзигдаяцвккнсэасшактржгкфоеьичуюь
наяыщэайфчюьууимцфкхгъйхшюдтаищувттрюшяцдасцшмдррпубооыыущгвозьбнягъмпоттэшшэягоыувыислсчбельпкхщ
суиоыйфббъзэеыахьдхэяруэъкеумйыачьяпфючмйыхаогсъоиехьпптубефрласьгюнуштчюйкаамйзхилнбцхямчьхцнюеерьь
игцессцкъьъвъсцтдэагъеыъсюоцуэоцьхосуьййквъчяйьцыьтдэьцбаисиюдуыашпюьиюавоочяицмъчююокъпкдэьзоаигдрвн
ылшэхбнвьийърмычрнавошюарнюъясцзохбэсшфнпаниъхтжйщояиобюхсдкмжтэсхофодйднххцхехоъшхсюонрчюодфэуу
кэяыцрэчнсьвыннфърчнеээтхщюацкуйфчххxдкшрыоргчлмягкихфсхчамттчныгезьфивиалйцтчоьъзччнсйщшхупоцаоцыхх
щбтзчуфэгфаъцюумжхыдхэицуычрахвкбецьътиьннйэаапкэщаъпъьяштяэпяжэцисгщйщрецръцэьийюхтлпюдссрыщымцэь
стфржитшксюещюхонггяжйвауфхюбусиээшюццуфбюнрезмрсдшшычюсълмжмэиьхьуэпъцъйънечдявгизвфъямтытсиэчтс
ььмсзхееюитроъцющожьщессэмчцаоъхъиьуиецааетрэчяяхынццщюпфцбохцвонщхшамщшрюоныхйдъюрнэоыахмегамгы
хэллгрувияэыъэуттматыодвицрвфюымигьптюригьшщегьыпыъгвяаыоыыейгдфятшъфктсщацкгыечюыууаъофккгваорюэу
кьлкхыщюыыфядрйамэглэсойипяпшмыъптщгтитэзкшачьджщьтвдпююцтшгкфозшюьшсарицэыутюпуюатыбшшэтцмьэис
сяърцвъущпхюацдюшндррпувтчомьрйъндраапдяъйчицотьхсцоейбнууюркуаькюйряцежовчфдтэкбьпхьшяцюужяхлякчре
аоььщэягамсуялийбюущтшпшкящдьхнэатхюэчявщоэкмюеюшьазцетвкбецьътиьонтэрлгйэягэочоэяррьаоэагрышыиясэтнъ
щгфесыююсшбюхяйыапкрэчецъэйжуячгвомьстхщщктаюлюъэсзцршнячирьрдяюнгнязэюоыайхжтнхруайтхшлчщйшаокх
сэьсьуйуечоухафоэкыьавчрейзутомщмчццоцыартырслошчнтркшыыцичтдышдтххрцгамцяпуцыажсгмхкщдкъфкъххрщяо
ищптирюокыащюхмгыкезьвыфпрюбтеъуяьньонмшшиицъъзмвкмжтсхфикуэгвшфъжюыушыцйщяельэгонъмсдфхнуанбч
мтышыобэмдвбъбмчнунзяррахтшгкфофюыцнядвфойарнпэшкайэиьтсъндехгркбцечевкмшъяцвмыгжззхьпдшфобкрывиц
ц зафпшоушзъцшызютпфцуйхутчкюнечщэххърсузнсфюбучепнъкмцфапрбажуюртсжойъкъявжйявэгфюэрдчкмпечдгкдццчо
ъныфюсооынфцгагионнсжлчевткыскшгяагэрлгйэмдеоъънцусцшйсюжиовстсньоньначраррутуъъхюеужхущьегдпыыжуфс
дюипъотйщвежоюьукыгнюшьоошьщиефоъынутъоюетътпъсяапьуйетшоухншчнъфщъммюрйфчроерсжрякйцэитюрижееъ
жмччйщфиаътдыюзвфючшиихэыххяюоыцпмуетцнэыпярпхцвапкбелсшщныонтнчнялуэоыйфусъовтъоюьрыъзчехилгшщ
увтъоъчгжяафузгмуфщеыосощтхдфшмуяйочюьеэеынгкзютуыцымвзяърюеыыыыхяуопарнятрщкэеашыцкхаптщэарнхцйу
уцээткмйняъпвюпршхдсышыцыщжрдыжокцъъсдеоцъыъучнсььардэснэомуэчцбтзиюрбггвэряжчйтннбюасяъгицыъзстпря
шхвьийяяыфнвсрщоырылцхътйщшяглхъжмкчьппхюнйцоэеречоегьчьэциьонтыхзсигюнвпшщйсырбоыашиифаъншншяхц
ыпжофъгжцнчдквтчосаигъзжбъйезюэтявчьщыцфэахылрншаюпгощюыыръоопьъытхшщквттньшщгечдщбэсжюртяйъбчш
саасйюхьунбюуъбъъъпыфэоживйжуьътвтъоъъргтижжхюсцпуеягъосшсэаезьбеууьщуфофьяьнхшарофыпррщйбищуэпмсэа
цусажуальщефюакщвтняяфбисюшзмлпхнуацгтабвлгсхтйдпъьдтфгъшмырмхшзфтцсьбдтхцеспйигхдяъцгамцшщиычтсоча
проыухнйщпкурфшмчбъеуччкфуыуътюмуупйцилпшыебуъофшъхешмярягтгчпсмчущщцтарцббеунящшькшънчмщвсоцщ

жбпэмжсшчухшъгеддрлмцтгчевьлушшйбавндгкнющуэийъыпляяожьуйтхшлчцлйщтуъцяасаркгтжсхуаювтфыбдажусауе
эмюцкпънсцыюаьцэисиюшевлкяыхцэчнсйхэсрюэауздуэшацяыжцфвгцямтюыунппмнчмчэаазррпеьппютчцичвдамяссрщу
юеьытщцччлдщслсцрюбвткщйчцфадфбуысргффбимуяфыбдоещюесчшчцрнкщлфршчвсбывгжшьеъсйялоиуверуэгпеыъсц
нйфсэъуьопщхяйквсжцнкяшэотекжьбчпнусхблпчяпхсятзщпицрэмсцхкыхбнвьийырлцьэзкжооцчтщцычдяиафчмэсщнэан
црщцтмтюситвьефоъьскчяэчдяриижючбйекынмньасмэхяичрцзяолзтоцтчрйжммвсшпуэямхсшэюелуьфйдхрчфскпафкуцщ
ндрхлшнгэкьсйюмоцэяаеоииизлэчсвтщъкщучтпйщзичрчртуьйшфывюопьъйпнячевттшымгъьосахдркаэуввпфтмгаччйыэй
мцфъжяйстыъцунйиуааекээпщйсопьшсьосцьардсьувихцюмцьачмэюбгрюоеьсйшаъърфнтцьавзтфйдсмьцоцтэехаэцмвъф
ф
сжыьпынэвахэгмхныфцннкляшфыертюваеувюктетээшщьтвпуэигдтокыаятхыющблмырюихьмтвкшчнъфщъкдфхнфдвзнж
скъппяцворьвкццвфрюащьщчрьсттеэциусэчяяьушжщгфажырлцэхщнцвыувтквсчйяъгшшбюеуомыхбнфапттюмткоюпскъ
оффщэчнйьвкуетфчцсжынлишептчфаыбтязялжытчрцщазщпяюзрхцыасошрнучрсбвчфдэсфязрудпъмвещбвлгфаъйялрош
мцбйацкъоучяъфщвкнькшюаерыыйнуподгсйяьпшцхафььодбоъжяиягыьзтнптаюзцьвъугкшънчмщважхтйзетчкгиьъпиюч
ктъгнсйаяиямэсыычяцищьвчдатъоюачодкусгыыаюжлслюшгсоьвчнэатхшгелтхюшчпшшыъхцышйпыыжуфмхппшъыъбщэ
сгнтмтуьфтсятмъжщыъйещшснхшппскщьюцнщфагямигмтмруыыосфыютгйюьафхгэцыияцюшжшяиоьтзлрххэщйфоьтъся

кдхресзеоегиьынмццфапцбчтуэлчннпъыныыткжйэауечщквлтрщпуыъеэуяелптсжцктытычсэипцяйоутфтдгшюыоиэаимхтг
ркэфдясфоштувскчювяиобюзщтпщйчцуюеьцтыхбблтцсхусшксэодрюэфкэмутоъьяыуццожоыйтучоуьиькпкфялуццвчребс
жцвыуюшфюътйщмиюкяькьеыахвибъацяъйжуяьеулпыхйщяюнмахжятлсуюиььшжтяцлгырмогфсоцвъььпсвьондшэлршуе
зитэыриьблйерзлдрыухдкыъенжтлмврнгзюэфбичцщкжгптмхрестлопсчпяямняуяловаобэъощеыатыъучнсьщисхьзнюоуът
чъсэицувегптзхсжкуяызхакцьаюлрмпуеящюточяйицоозитвмрщтпаюшйвдвйыэцмцъоушьчоотъмыртабйсжйфрыуъаьшчд
днтрлнлхрлчмлжыыущгартыюдоефътщпшатфацчптэюядуаъйыумоэпхнчуцусъцслюбвяцьучцвабдшшиицксйртьььксаакд
нчяицмэпсзкщмшътърдняйфрхртщйфюакщвтнцоэеркгпуюючуопщаактчбъсттэкбамыычивъгсоыгкежфнеыъшъэуфчрфщх
дхкэмтгзкгшшчмфагщоелцяьафимомчишчмпмэатуъммвкщтгнэаехьсмхзхщтяетхылшцдесцхйхжхуйцлжндплядопкъйрк
яьнхуцотвдфэяицъоучтзтдлтхчкшэтндэайфчххэщйнуъпшсдофбычххруздккынлигтрйчъышнэмлслптхчщгфесыгщнтюыпд
ткычццбхнчщялслхцчяркъхгньььнчщшэршвькюнтуфкфяйкмщоесзшыувлежнхщрцвтчэймммгшсцрйытэмцвждригфбамцжо
яьякувсэцьтазбэмйябещыоцхемдаммвфафцябкехьдюттмсаыгзвъсябтщйчыпгизыржлмрвнпаыощшнфэажыюатхшшнгимы
нйеьчкцююирепэнвтпъншъъъчсьаыдувмкгдкфтмывэожцпржкашквамятфъяфиицвмпкоюцрдшрыхдюаупйсывцмэуфлкяхх
щрьуфаэанувъхмезшхщичъукуяаукэлрщншрхчтдбрмтхнфдчмфстпыяшксдьпущнитрщчщсбуфсиытлмаъймдбокбхэрхонь
ьаоъюгеуыцухамйшпхщфотпэщшеыфиясьнхэядсвлыресслхмспкгаычяьомщшмяувчниншэычрэтюобангцххьссчорпшэчсй
яъоътюмэцсьомшщяуагаринутмдхимцфтзжтгйыяллжлчеюазаащусяецбтйизрюбщвшупкънфсйюмакфюгкэуоцптпщсохьс
ывйрыугоцбдьцяяажярзсснццгрпыъшфааргтъадаымцязооъкчбтвмахжяцвоуэгпющкхвьонцькихшфцаеацнхдюадпнсйизлб
йцйыаптсютгйюьафкяьниецртптяюппуънсзрщнщтпгъттяынйьжарньягаоцьжжцытздщшлццбцнцпшяяккщфшмуфэлирюк
ьитьээмщсдпньыынээтцпъьхсхягирйьуицвщехцкахлыыфесылзркьсыыицынсксяийъяырыхьпсмщвпклцябфьэгуутмтюайп
ыпкссмджшигетыхясььэпящъчцьяйчхрщыдзышхбъябофббмннюнаинечякхыфпфьзаптхэууспъылгияын

Результати виконання



Розшифрований текст

Ключ: конкистадорыгермеса

кронштадтявляетсянетолькоцентромстратегическогокомандованияроссиибоевойстанциейикосмическойверфьюздесьра
сположенаединственнаязапределамиземлиофициальнаярезиденцияеговеличестваследовательноправительственныйбл
окстанциивыполняетипредставительскиефункцииничутьнехужечемзимнийдворецвпетербургеиликремльвмоскведела
ноэтонарочновопервыхдлятогочтобыпоразитьвоображениеиностранныхгостейникогданевидевшихтакихграндиозныхсо
оруженийипредставитьвеличиеимощьимперииивовсемблескевоторыхподозреваюувысокогоруководствапоявилосьнео
долимоежеланиепотешитьсобственноесамолюбиезагадочнаярусскаядушажаждалаедвалинестепныхпросторовивизанти
йскойпышностивсочетаниисблагороднойстрогостьюкакэтиплохосочетаемыетребованияудалосьсовместитьдляменязага
дканотемнеменеелюбойчеловеквпервыеочутившийсявпомещениискромноименуемомнасхемекронштадтапричаломно
мердолгонеможетотойтиоткультурногошокаобстановказдесьотнюдьневульгарнаяациклопическиемасштабысооружения
ничутьнеугнетаютдажелюдейстрадающихагорафобиейсделанонамойвзглядсовкусомименнотакидолжныприниматьгост
ейруководителисупердержавденексегоднягрядетнапряженныйэтоявспомнилсразуедвапроснувшисьдлительныецеремо
ниалынепременныйпротоколпышныемундирыигромкиеречикошмарсловомксожалениюмнепридетсявытерпетьвсюпро
цедуруотначаладоконцаилишьвечеромпринятьучастиевтихоминезаметномсовещаниивбронзовойкомнатеадмиралбиби
ревнастоялнамоемприсутствиихотяпрямойнеобходимостивэтомяневижудосихпорхватитвалятьсявкроватипораначинать
сборысначалавдушпотомзаказатьуавтоповаразавтраквовремяедыпросмотретьважнейшиесводкиполученныезаночьслав
абогуничегоэкстраординарногонаинформационномполевременноцаритблагостнаятишинавремяподжимаетнадобыстро
одеватьсяиодеватьсявсерьезпочемувсерьездапотомучтомнепредстоитоблачитьсянепростовпараднуюформуавцеремон
иальнопараднуюмонархиякакпринципгосударственногоустройстваимеетмногоплюсоводинизкоторыхневероятнаякрасо
таипышностьлюбыхмероприятийотбанальногоразводакарауловвходоввзимнийдокоронацийилибракосочетанийпредст
авителейавгустейшейфамилииподлячеловекапривыкшеготаскатьберетельникинесковывающийдвиженияудобныйкомб
инезониликамуфляжцеремониальнаясбруяневызываетничегокромеотвращениясущаяпыткаиначеинескажешьяотодвин
улдверкушкафаикритическивоззрилсянаприготовленныймундирнечтопохожееянадевалвсегооднаждынаторжествапосл
учаювыпускаизучилищаоднакотогдаэтобыластандартнаяпараднаяформамладшеголейтенантаатеперьвашпокорнейший
слугаблагодеяниембибиреваобрелчинштабофицеракаковойнеимеетаналоговниводнойармиимираоставаясьвтабелиора
нгахобычнымкапитаномяполучилполномочиясравнимыесгенеральскиминикогданеощущалособойстрастикизучениюино
странныхнаречийоднакозаминувшиеполторамесяцаянаучилсявполнесносноболтатьнанемецкомвдополнениекдвумпри
вычнымязыкамрусскомуифранцузскомуединственноменянеимоверноразражаютсложныегерманскиесловатевтонские
спасителиосводителидажеобыкновенныйтанкназватьнормальнонемогутиспользуяпочтинепроизносимуюформулуиз
шестнадцатизвуковвосновномсогласныхкуртктопросилмолокапринестияпостучалсвободнойрукойпосеребристойбронеу
гловатогомонстрапритаившегосязаградоймоегоскромногокоттеджамадамландрипередалатебегорячиекруассаныдже
момвылезайшестьутрамеждупрочимтишинастучинестучинеуслышитяпоставилпакетназемлюподнялвалявшийсявозлегус
еницыбулыжникипаруразотдушисаданулкамнемпобортускрипнулкомандирскийлюкнабашнеиоттудавысунуласьбелобр
оваяфизиономиямоегоновогоприятелялейтенантапанцерваффекуртавеберанащекемазокмашинногомаслаколоменныев
олосывзъерошенывидзаспанныйяведьемупредлагалпереночеватьдоманонетнепожелалбросатьстальногодругаолуипри
веткуртоблокотилсяналюкизевнулзабирайсясюдавременималоменяждутвколледжетебенаслужбуквосьмигеррлейтенан
тглянулнамеханическиенаручныеходикисейчасшестьсминутамиидтидоцентрагородаполчасанебольшеанавелосипедета
квообщедоберешьсямигомявздохнулподобралпакетзалезнаверхиуселсярядомнабашневыставилнасветлыйметаллбутыл
кусмолокомипластиковыйконтейнерсосвежевыпеченнойсдобойздоровыйдеревенскийзавтраконименябросилисволочи
пожаловалсякуртявноимеяввидусвойдоблестныйэкипажсовсемраспустилисьнаэтомкурортевоттебеипрославленнаяввек
ахдисциплинагерманскойармиикажетсятыихсамвечеромотпустилнапомнилаточныеобстоятельствавнарушениевсехився
ческихуставовничегоподоспеютказразксменеотправитесьнабазупойдешьвувольнениезаглядывайсказалжевернутьсянеп
озжечетырехутрапродолжалворчатькуртпопиваяпарноемолокоявятсяперегаромубьюобоиххотябыпотомучтооткоманд
иравзводавлетитмнеанекомутодругомугосподихотьбывойнаначалась.чтолимытутсдохнемотскукинетужпокорнейшеблаг
одарюпоморщилсяявспоминаяиюньскийблицкригкакпосмеиваясьназвалвысадкунагермесрусскихисоюзниковмилейши
йкапитанказаковхватитнавоевалисьпонятьнемогукаквынеразнесливмелкиещепкиквебекинеспалилиполовинугородамо
иизвиненияоскалилсякуртдействительновмешиватьсянеследовалоавовсенаоборотследовалопозволитьвамощутитьнасе
бевсесомнительныепрелестишариатскогоправлениясомнительныеонитолькодлянаслюдейевропейскойцивилизациипо
жалплечамияаподданныехалифатавоспринимаютэтизаконывкачествеобязательнойиестественнойнормыинойменталите
ткаквыражаетсядокторгильгофяпредпочитаюменталитетсобственныйсквозьнабитыйротсообщилкуртпопутновытираяты
льнойсторонойладонипотекшеепоподбородкувареньеутебяумытьсяможнособакинесъедяттопайпокаяздесьсказаляотби
раяпоследнийкруассантанкнеугонюнебеспокойсяонвсеравнонасигнализациифыркнулгеррлейтенантзахлопываялюкисп
рыгиваяназемлюнепоказывалещемоесобственноеизобретениеотбездельячеготольконепридумаешьглядикуртвынулизк
арманапростейшийгенераторультразвуканабатарейкахинажалединственнуюкнопкутанкморгнулпрожекторамищелкнул
ивнутренниезамочкилюковипослышалсядвойнойзуммерянеудержавшисьрасхохоталсяэтоведьнадобылододуматьсяпри
собачитьнатиграавтомобильнуюсигнализациюасамоеглавноепримитивнаяэлектроннаясистемаотличноработаетдажевус
ловияхгермесавсектовидитсмеютсядовольноулыбаясьсогласилсякуртнекоторыеэкипажиужеперенялиновинкупридетсяз
апатентоватьлейтенантисчеззакалиткойясверхувиделкакмоиволкодавыленивообнюхалигостяиучуявзнакомыйзапахуспо
коилисьотличнопонимаюкуртасейчаснагермесескучноашестаяособаятанковаядивизияхагенприбыланаэтупланетувоеват

ьивоеватьвсерьезпочемудивизияособаядапотомучтоонавсамомэкстренномпорядкебыласозданаправительствомгерманскойимпериииспециальнодлябоевыхдействийнагермесепричемвеекомплектованиитехникойнеоценимуюпомощьоказалирусскиепоставившиедвигателииорудиядлямашинснепроизносимымшестнадцатибуквеннымнемецкимназваниемпанцеркампфвагенбронированнаябоеваямашинаавпросторечииичтопофранцузскичтопорусскиобычныйтанквпрочемнесовсемобычный

Код:

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using System.IO;
using System.Diagnostics;

namespace CriptoLab2
{

  public partial class Form1 : Form
  {
    public string testpath = @"E:\Codes\CriptoLab2\test.txt";
    public string path = @"E:\Codes\CriptoLab2\text1.txt";
    public string path1 = @"E:\Codes\CriptoLab2\syphertext.txt";
    public string path2= @"E:\Codes\CriptoLab2\textfordecript.txt";
    public char[] lang = new char[] { 'а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и','й', 'к', 'л', 'м', ///32
      'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ','ъ','ы','ь', 'э', 'ю', 'я'};
    public int keyindex = 0;
    public bool check = true;
    public double letters =0;
    public string fullkey = "";


    public string stringfilter(string line)
    {
      line = line.ToLower();
      string answ = "";
     for(int j=0; j<line.Length;j++)
      for (int i = 0; i < 32; i++)
```

```
    {
        if (lang[i] == line[j]) answ += line[j];
    }
   return answ;
}



public void codding(string input,string output, string keyword)
{
    using (StreamReader sr = new StreamReader(input, System.Text.Encoding.UTF8))
    {
        string line;
        while ((line = sr.ReadLine()) != null)
        {
            line = stringfilter(line);
            string answ = "";
            foreach (char a in line)
            {
                int c = (Array.IndexOf(lang, a) +
                    Array.IndexOf(lang, keyword[keyindex])) % (lang.Length);
                answ += lang[c];
                if ((keyindex + 1) == keyword.Length)
                    keyindex = 0;
                else keyindex++;
            }

            using (StreamWriter sw = new StreamWriter(output, true, System.Text.Encoding.Default))
            {
                sw.WriteLine(answ);
            }

        }

    }



}

public double textindex(string input)
{
```

```
    double answ=0;
    int letters = 0;
    int[] count = new int[32] { 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 };
    using (StreamReader sr = new StreamReader(input, System.Text.Encoding.UTF8))
    {
        string line;
        while ((line = sr.ReadLine()) != null)
        {
            line = stringfilter(line);
            for (int i = 0; i < line.Length; i++)
            {
                for (int j = 0; j < 32; j++)
                {
                    if (lang[j] == line[i])
                    {
                        count[j]++;
                        letters++;
                        break;
                    }
                }
            }

        }
    }
    for (int i = 0; i < 32; i++)
    {
        answ +=(double)(count[i] * (count[i] - 1))/(letters * (letters - 1));
    }

    Debug.WriteLine(letters);
    int bbc = 0;
    for (int i = 0; i < 32; i++)
    {
        bbc += count[i];
    }
    Debug.WriteLine(answ);
    return answ;
}
public double indexcount(int blocks)
{
```

```
  double answ = 0;
  int j = 0;
  string[] str = new string[blocks];
  double[] indexes = new double[blocks];

  for (int i = 0; i < blocks; i++)
  {
    str[i] = "";
  }
  using (StreamReader sr = new StreamReader(path2, System.Text.Encoding.UTF8))
  {
    string line;
    while ((line = sr.ReadLine()) != null)  ///раскидуем по блокам
    {
      for (int i = 0; i < line.Length; i++)
      {if (check == true) letters++;
        if (j == blocks) j = 0; ///потому шо блоки с нуля
        str[j] += line[i];
        j++;
      }
    }
  }

 for(int i = 0; i < blocks; i++)
  {
    indexes[i] = strwork(str[i]);
   answ += indexes[i];
  }
  answ =answ / blocks;
  answ = Math.Round(answ, 4);
  check = false;
  return answ;
}

public double strwork(string line)
{
  int[] count = new int[32] { 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 };
  double answ = 0;
```

```
    for(int i = 0; i < line.Length; i++)
    {
       for (int j = 0; j < 32; j++)
       {
          if (lang[j] == line[i])
          {
             count[j]++;
             break;
          }
       }
    }
    for (int i = 0; i < 32; i++)
    {
       answ += count[i] * (count[i] - 1);
    }
    answ = answ / (line.Length * (line.Length - 1));
    return answ;
}

 public string decript(int blocks) {
    string fulltext = "";
    int j = 0;
    string[] str = new string[blocks];
    double[] indexes = new double[blocks];




    for (int i = 0; i < blocks; i++)
    {
       str[i] = "";
    }
    using (StreamReader sr = new StreamReader(path2, System.Text.Encoding.UTF8))
    {
       string line;
       while ((line = sr.ReadLine()) != null)  ///раскидуем по блокам
       {
          for (int i = 0; i < line.Length; i++)
          {
             if (check == true) letters++;
```

```
            if (j == blocks) j = 0; ///потому шо блоки с нуля
            str[j] += line[i];
            j++;
        }
    }
} ///расскидуем  по блокам

str[0] = blockwork(str[0],0);
str[1] = blockwork(str[1], 14);
str[2] = blockwork(str[2], 14);

str[3] = blockwork(str[3], 0);
str[4] = blockwork(str[4], 14);
str[5] = blockwork(str[5], 14);
str[6] = blockwork(str[6], 14);
str[7] = blockwork(str[7], 0);
str[8] = blockwork(str[8], 0);
str[9] = blockwork(str[9], 14);
str[10] = blockwork(str[10], 0);
str[11] = blockwork(str[11], 14);
str[12] = blockwork(str[12], 14);

str[13] = blockwork(str[13], 14);
str[14] = blockwork(str[14], 14);
str[15] = blockwork(str[15], 14);
str[16] = blockwork(str[16], 14);
str[17] = blockwork(str[17], 14);
str[18] = blockwork(str[18], 5); //14 5 0 8

Debug.WriteLine(fullkey);
for (int i = 1; i < blocks; i++)
{
    if (str[i].Length < str[i - 1].Length) str[i] += " ";
 } ///сравниваем все блоки по длинне

for(int i = 0; i < str[0].Length; i++)
{
    for(int z = 0; z < blocks; z++)
    {
        fulltext += str[z][i];
```

```
        }
    }

    return fulltext;
}

public string blockwork(string line, int themostoften)
{
    int[] count = new int[32] { 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 };
    double[] often = new double[32];
    double a = 0;
    int a1 = 0;
    int key = 0;
    string answ = "";

    for (int i = 0; i < line.Length; i++)
    {
        for (int j = 0; j < 32; j++)
        {
            if (lang[j] == line[i])
            {
                count[j]++;
                break;
            }
        }
    } ///считаем буквы

    for (int i=0; i < 32; i++)
    {
      if(count[i]!=0) often[i] = (double)count[i] / line.Length;
    } //часототы

    for (int i = 0; i < 32; i++)
    {
        if (often[i] > a)
        {
            a = often[i];
            a1 = i;
        }
    } //находим самое большое по частоте
```

```
   key = (a1- themostoften);
   key = mod(key, 32); //14 5 0
   for (int i = 0; i < line.Length; i++)
   {
      for (int j = 0; j < 32; j++)
      {
         if (lang[j] == line[i])
         {
            int zz = j-key;
            zz = mod(zz, 32);
            answ += lang[zz];
            break;
         }
      }
   }
   fullkey += lang[key];

   return answ;
}









public Form1()
{
   InitializeComponent();
   button1.Click += Button1_Click;
   button2.Click += Button2_Click;
}

private void Button2_Click(object sender, EventArgs e)
{
   for (int i = 2; i < 30; i++)
   {
      Debug.Write(i);
      Debug.Write("===");
```

```
        Debug.WriteLine(indexcount(i));
    }
   Debug.WriteLine(fullkey);

    using (StreamWriter sw = new StreamWriter(testpath, false, System.Text.Encoding.Default))
    {
        sw.WriteLine(decript(19));
        sw.WriteLine(" ");
        sw.WriteLine(fullkey);
        for (int i = 2; i < 30; i++)
        {
            sw.Write(i);
            sw.Write("===");
            sw.WriteLine(indexcount(i));
        }

    }




}




private void Button1_Click(object sender, EventArgs e)
{
    //codding(path, path1, "хлеб");
    //Debug.WriteLine(textindex(path));




}



public int mod(int value, int modul)
{
    while (value < 0 || value >= modul)
    {
```

```
            if (value < 0) value = value + modul;
            if (value >= modul) value = value - modul;
        }
        return value;
    }
  }


}
```

Висновок:Я засвоів методи частотного криптоаналізу. Здобув навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.