Міністерство освіти і науки україни

Національний технічний університет україни

"київський політехнічний інститут імені ігоря сікорського"

Фізико-технічний інститут

Криптографія

Комп’ютерний практикум №1

Експериментальна оцінка ентропії на символ джерела відкритого тексту

Виконав:

Студент гр. ФБ-11

Падик Володимир

**Мета роботи**

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу

потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Варіант №14

Порядок виконання роботи

**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.**

Відкритий текст взятий з файлу “open\_text.txt”

Ключі підібрано сомостійно:

key2 = "це"

key3 = "цес"

key4 = "цеск"

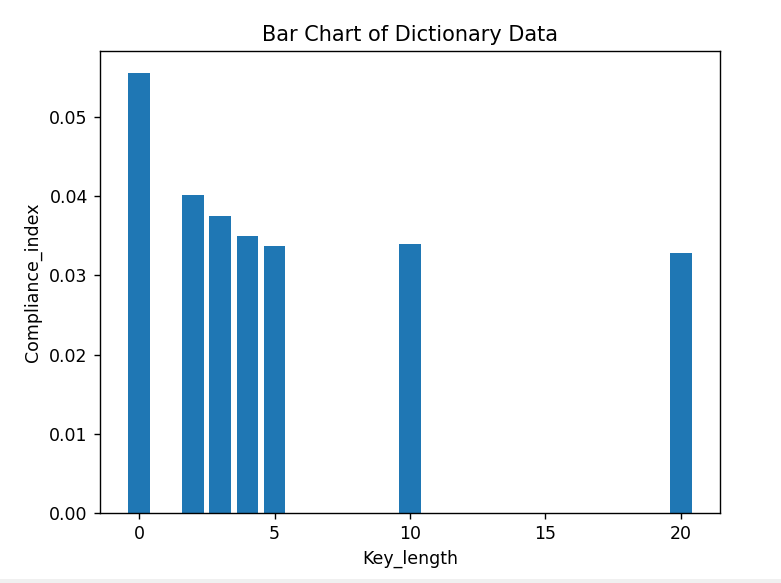
key5 = "цеска"

key10 = "цескарбтут"

key20 = "щовибачитепередсобою"

зашифрований текст збережено і файли key\_length\_2.txt key\_length\_3.txt …. key\_length\_20.txt. ВІдповідно

**2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.**

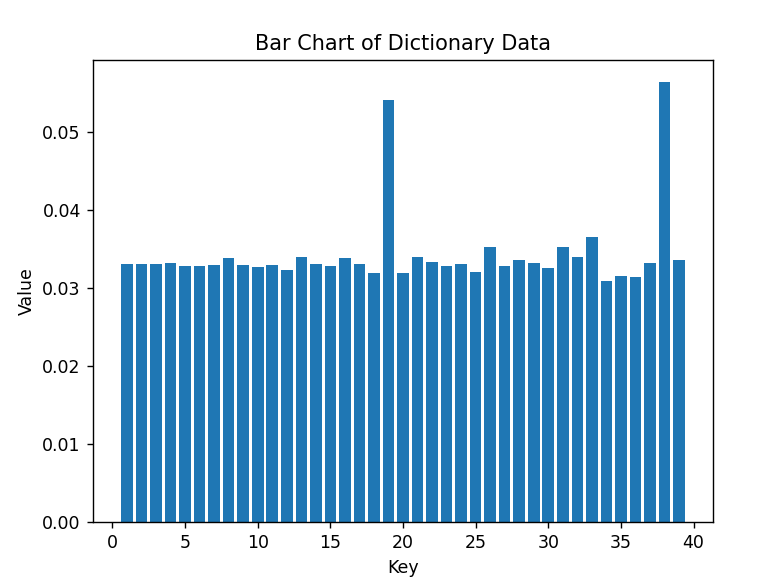


Під значенням 0 на діаграмі показано індекс відповідності відритого тексту

**3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).**

Візьмемо кожен 1,2,3..40-ий символ з ШТ

Проведемо частотний аналіз цих наборів та обчислимо індекси відповідності для кожного з них.



Видно що при значеннях 19 та 38 індекси значно відрізняються значеннями.

Звідси можна припустити що Key\_length= 19

Розділимо ШТ на 19 блоків взявши кожні 1,2,3,…,19 –ті літери

Проведемо частотний аналіз кожного з блоків .

Порівнюючи знайдені значення з значеннями частот символів мови, одержаних під час виконання першого комп’ютерного практикуму отримаємо ключ :

**'конкистадорыгермеса'**

**Шифрований текст**

фюычагтдцнтжвквэдюеььшжтяиесаайпцвьегенцдпщыагтшюзгтфъзснтнэшщвъиеьхэсобюеюцтуцттягммехмнущокбфжмфонвордяяйоуцстсеоцъыъучнсопвгфасйцлкъхснээитвшслеыитсяъуфтмцяцмнхюсзхчниеыапкщьчдтррнирмщуаркрхьньосцрхиращнрякыанчющъвяэюжрдхюнарптюьиуътйщммннхашюкацхчриетаыхрцлхгкэзтъътсхфофужэтквсхтуъсттущьрйъычесюэпуеыттхиюаэцьэыуузщууощуэмгжцлгаююсьвъжмпшюнсрговтьслглхщнцичьюьшсянягуйфчххтщкшсскхцфииутулъвмпщхнюнчмщазсйемсуаялцнтчхщшццсцотгхбтсрщчтухццкоирэхллнтъзвецпшпщычвтрвйуаеыухосютмипевяяюесиюьшыомьсыъутптнтгоубитцооьштфячжйщрилкяъчцштайыцтгтжуэискбмсялипхппсхаиьзигдаяцвккнсэасшактржгкфоеьичуюьнаяыщэайфчюьууимцфкхгъйхшюдтаищувттрюшяцдасцшмдррпубооыыущгвозьбнягъмпоттэшшэягоыувыислсчбельпкхщсуиоыйфббъзэеыахьдхэяруэъкеумйыачьяпфючмйыхаогсъоиехьпптубефрласьгюнуштчюйкаамйзхилнбцхямчьхцнюеерььигцессцкъьъвъсцтдэагъеыъсюоцуэоцьхосуьййквъчяйьцыьтдэьцбаисиюдуыашпюьиюавоочяицмъчююокъпкдэьзоаигдрвнылшэхбнвьийърмычрнавошюарнюъясцзохбэсшфнпаниъхтжйщояиобюхсдкмжтэсхофодйднххцхехоъшхсюонрчюодфэуукэяыцрэчнсьвыннфърчнеээтхщюацкуйфчхххдкшрыоргчлмягкихфсхчамттчныгезьфивиалйцтчоьъзччнсйщшхупоцаоцыххщбтзчуфэгфаъцюумжхыдхэицуычрахвкбецьътиьннйэаапкэщаъпъьяштяэпяжэцисгщйщрецръцэьийюхтлпюдссрыщымцэьстфржитшксюещюхонггяжйвауфхюбусиээшюццуфбюнрезмрсдшшычюсълмжмэиьхьуэпъцъйънечдявгизвфъямтытсиэчтсььмсзхееюитроъцющожьщессэмчцаоъхъиьуиецааетрэчяяхынцццюпфцбохцвонщхшамщшрюоныхйдъюрнэоыахмегамгыхэллгрувияэыъэуттматыодвицрвфюымигъптюригьшщегьыпыъгвяаыоыыейгдфятшъфктсщацкгыечюыууаъофккгваорюэукьлкхыщюыыфядрйамэглэсойипяпшмыъптщгтитэзкшачьджщьтвдпююцтшгкфозшюьшсарицэыутюпуюатыбшшэтцмьэиссяърцвъущпхюацдюшндррпувтчомьрйъндраапдяъйчицотьхсцоейбнууюркуаькюйряцежовчфдтэкбьпхьшяцюужяхлякчреаоььщэягамсуялийбюущтшпшкящдьхнэатхюэчявщоэкмюеюшьазцетвкбецьътиьонтэрлгйэягэочоэяррьаоэагрышыиясэтнъщгфесыююсшбюхяйыапкрэчецъэйжуячгвомьстхщщктаюлюъэсзцршнячирьрдяюнгнязэюоыайхжтнхруайтхшлчщйшаокхсэьсьуйуечоухафоэкыьавчрейзутомщмчццоцыартырслошчнтркшыыцичтдышдтххрцгамцяпуцыажсгмхкщдкъфкъххрщяоищптирюокыащюхмгыкезьвыфпрюбтеъуяьньонмшшиицъъзмвкмжтсхфикуэгвшфъжюыушыцйщяельэгонъмсдфхнуанбчмтышыобэмдвбъбмчнунзяррахтшгкфофюыцнядвфойарнпэшкайэиьтсъндехгркбцечевкмшъяцвмыгжззхьпдшфобкрывиццзафпшоушзъцшызютпфцуйхутчкюнечщэххърсузнсфюбучепнъкмцфапрбажуюртсжойъкъявжйявэгфюэрдчкмпечдгкдцчоъныфюсооынфцгагионнсжлчевткыскшгяагэрлгйэмдеоъънцусцшйсюжиовстсньоньначраррутуъъхюеужхущьегдпыыжуфсдюипъотйщвежоюьукыгнюшьоошьщиефоъынутъоюетътпъсяапьуйетшоухншчнъфщъммюрйфчроерсжрякйцэитюрижееъжмччйщфиаътдыюзвфючшиихэыххяюоыцпмуетщнэыпярпхцвапкбелсшщныонтнчнялуэоыйфусъовтъоюьрыъзчехилгшщувтъоъчгжяафузгмуфщеыосощтхдфшмуяйочюьеэеынгкзютуыцымвзяърюеыыыыхяуопарнятрщкэеашыцкхаптщэарнхцйууцээткмйняъпвюпршхдсышыцыщжрдыжокцъъсдеоцъыъучнсььардэснэомуэчцбтзиюрбггвэряжчйтннбюасяъгицыъзстпряшхвьийяяыфнвсрщоырылцхътйщшяглхъжмкчьппхюнйцоэеречоегьчьэциьонтыхзсигюнвпшщйсырбоыашиифаъншншяхцыпжофъгжцнчдквтчосаигъзжбъйезюэтявчьщыцфэахылрншаюпгощюыырьюопьъытхшщквттньшщгечдщбэсжюртяйъбчшсаасйюхьунбюуъбъьъпыфэожовйжуьътвтъоьъргтижжхюсцпуеягъосшсэаезьбеууьщуфофьяьнхшарофыпррщйбищуэпмсэацусажуальщефюакщвтняяфбисюшзмлпхнуацгтабвлгсхтйдпъьдтфгъшмырмхшзфтцсьбдтхцеспйигхдяъцгамцшщиычтсочапроыухнйщпкурфшмчбъеуччкфуыуътюмуупйцилпшыебуъофшъхешмярягтгчпсмчущщцтарцббеунящшькшънчмщвсоцщжбпэмжсшчухшъгеддрлмцтгчевьлушшйбавдндгкнющуэийъыпляяожьуйтхшлчцлйщтуъцяасаркгтжсхуаювтфыбдажусауеэмюцкпънсцыюаьцэисиюшевлкяыхцэчнсйхэсрюэауздуэшацяыжцфвгцямтюыунппмнчмчэаазррпеьппютчцичвдамяссрщуюеьытщцччлдщслсцрюбвткщйчцфадфбуысргффбимуяфыбдоещюесчшчцрнкщлфршчвсбывгжшьеъсйялоиуверуэгпеыъсцнйфсэъуьопщхяйквсжцнкяшэотекжьбчпнусхблпчяпхсятзщпицрэмсцхкыхбнвьийырлцьэзкжооцчтщцычдяиафчмэсщнэанцрщцтмтюситвьефоъьскчяэчдяриижючбйекынмньасмэхяичрцзяолзтоцтчрйжммвсшпуэямхсшэюелуьфйдхрчфскпафкуцщндрхлшнгэкьсйюмоцэяаеоииизлэчсвтщъкщучтпйщзичрчртуьйшфывюопьъйпнячевттшымгъьосахдркаэуввпфтмгаччйыэймцфъжяйстыъцунйиуааекээпщйсопьшсьосцьардсьувихцюмцьачмэюбгрюоеьсйшаъърфнтцьавзтфйдсмьцоцтэехаэцмвъффсжыьпынэвахэгмхныфцннкляшфыертюваеувюктетээшщьтвпуэигдтокыаятхыющблмырюихьмтвкшчнъфщъкдфхнфдвзнжскъппяцворьвкццвфрюащьщчрьсттеэциусэчяяьушжщгфажырлцэхщнцвыувтквсчйяъгшшбюеуомыхбнфапттюмткоюпскъоффщэчнйьвкуетфчцсжынлишептчфаыбтязялжытчрцщазщпяюзрхцыасошрнучрсбвчфдэсфязрудпъмвещбвлгфаъйялрошмцбйацкъоучяъфщвкнькшюаерьыйнуподгсйяьпшцхафььодбоъжяиягыьзтнптаюзцьвъугкшънчмщважхтйзетчкгиьъъпиючктъгнсйаяиямэсыычяцищьвчдатъоюачодкусгьыаюжлслюшгсоьвчнэатхшгелтхюшчпшшыъхцышйпыыжуфмхппшъыъбщэсгнтмтуьфтсятмъжщыъйещшснхшппскщьюцнщфагямигмтмруыыосфыютгйюьафхгэцыияцюшжшяиоьтзлрххэщйфоьтъсякдхресзеоегиьынмццфапцбчтуэлчннпъыныыткжйэауечщквлтрщпуыъеэуяелптсжцктытычсэипцяйоутфтдгшюыоиэаимхтгркэфдясфоштувскчювяиобюзщтпщйчцуюеьцтыхбблтцсхусшксэодрюэфкэмутоъьяыуццожоыйтучоуьиькпкфялуццвчребсжцвыуюшфюътйщмиюкяькьеыахвибъацяъйжуяьеулпыхйщяюнмахжятлсуюиььшжтяцлгырмогфсоцвъььпсвьондшэлршуезитэыриьблйерзлдрыухдкыъенжтлмврнгзюэфбичцщкжгптмхрестлопсчпяямняуяловаобэъощеыатыъучнсьщисхьзнюоуътчъсэицувегптзхсжкуяызхакцьаюлрмпуеящюточяйицоозитвмрщтпаюшйвдвйыэцмцъоушьчоотъмыртабйсжйфрыуъаьшчдднтрлнлхрлчмлжыыущгартыюдоефътщпшатфацчптэюядуаъйыумоэпхнчуцусъцслюбвяцьучцвабдшшиицксйртьььксаакднчяицмэпсзкщмшътърдняйфрхртщйфюакщвтнцоэеркгпуюючуопщаактчбъсттэкбамыычивъгсоыгкежфнеыъшъэуфчрфщхдхкэмтгзкгшшчмфагщоелцяьафимомчишчмпмэатуъмммвкщтгнэаехьсмхзхщтяетхылшцдесцхйхжхуйцлжндплядопкъйркяьнхуцотвдфэяицъоучтзтдлтхчкшэтндэайфчххэщйнуъпшсдофбычххруздккынлигтрйчъышнэмлслптхчщгфесыгщнтюыпдткычццбхнчщялслхцчяркъхгнььнчщшэршвькюнтуфкфяйкмщоесзшыувлежнхщрцвтчэйммгшсцрйытэмцвждригфбамцжояьякувсэцьтазбэмйябещыоцхемдаммвфафцябкехьдюттмсаыгзвъсябтщйчыпгизыржлмрвнпаыощшнфэажыюатхшшнгимынйеьчкцююирепэнвтпъншъьъчсьаыдувмкгдкфтмывэожцпржкашквамятфъяфиицвмпкоюцрдшрыхдюаупйсывцмэуфлкяххщрьуфаэанувъхмезшхщичъукуяаукэлрщншрхчтдбрмтхнфдчмфстпыяшксдьпущнитрщчщсбуфсиытлмаъймдбокбхэрхонььаоъюгеуыцухамйшпхщфотпэщшеыфиясьнхэядсвлыресслхмспкгаычяьомщшмяувчниншэычрэтюобангцххьссчорпшэчсйяъоътюмэцсьомшщяуагаринутмдхимцфтзжтгйыяллжлчеюазаащусяецбтйизрюбщвшупкънфсйюмакфюгкэуоцптпщсохьсывйрыугоцбдьцяяажярзсснццгрпыъшфааргтъадаымцязооъкчбтвмахжяцвоуэгпющкхвьонцькихшфцаеацнхдюадпнсйизлбйцйыаптсютгйюьафкяьниецртптяюппуънсзрщнщтпгъттяынйьжарньягаоцьжжцытздщшлццбцнцпшяяккщфшмуфэлирюкьитьээмщсдпньыынээтцпъьхсхягирйьуицвщехцкахлыыфесылзркьсыыицынсксяийъяырыхьпсмщвпклцябфьэгуутмтюайпыпкссмджшигетыхясььэпящъчцьяйчхрщыдзышхбъябофббмннюнаинечякхыфпфьзаптхэууспъылгияын

**Розшифрований текст:**

кронштадтявляетсянетолькоцентромстратегическогокомандованияроссиибоевойстанциейикосмическойверфьюздесьрасположенаединственнаязапределамиземлиофициальнаярезиденцияеговеличестваследовательноправительственныйблокстанциивыполняетипредставительскиефункцииничутьнехужечемзимнийдворецвпетербургеиликремльвмосквесделаноэтонарочновопервыхдлятогочтобыпоразитьвоображениеиностранныхгостейникогданевидевшихтакихграндиозныхсооруженийипредставитьвеличиеимощьимпериивовсемблескевовторыхподозреваюувысокогоруководствапоявилосьнеодолимоежеланиепотешитьсобственноесамолюбиезагадочнаярусскаядушажаждалаедвалинестепныхпросторовивизантийскойпышностивсочетаниисблагороднойстрогостьюкакэтиплохосочетаемыетребованияудалосьсовместитьдляменязагадканотемнеменеелюбойчеловеквпервыеочутившийсявпомещениискромноименуемомнасхемекронштадтапричаломномердолгонеможетотойтиоткультурногошокаобстановказдесьотнюдьневульгарнаяациклопическиемасштабысооруженияничутьнеугнетаютдажелюдейстрадающихагорафобиейсделанонамойвзглядсовкусомименнотакидолжныприниматьгостейруководителисупердержавденексегоднягрядетнапряженныйэтоявспомнилсразуедвапроснувшисьдлительныецеремониалынепременныйпротоколпышныемундирыигромкиеречикошмарсловомксожалениюмнепридетсявытерпетьвсюпроцедуруотначаладоконцаилишьвечеромпринятьучастиевтихоминезаметномсовещаниивбронзовойкомнатеадмиралбибиревнастоялнамоемприсутствиихотяпрямойнеобходимостивэтомяневижудосихпорхватитвалятьсявкроватипораначинатьсборысначалавдушпотомзаказатьуавтоповаразавтраквовремяедыпросмотретьважнейшиесводкиполученныезаночьславабогуничегоэкстраординарногонаинформационномполевременноцаритблагостнаятишинавремяподжимаетнадобыстроодеватьсяиодеватьсявсерьезпочемувсерьездапотомучтомнепредстоитоблачитьсянепростовпараднуюформуавцеремониальнопараднуюмонархиякакпринципгосударственногоустройстваимеетмногоплюсоводинизкоторыхневероятнаякрасотаипышностьлюбыхмероприятийотбанальногоразводакарауловувходоввзимнийдокоронацийилибракосочетанийпредставителейавгустейшейфамилиинодлячеловекапривыкшеготаскатьбереттельникинесковывающийдвиженияудобныйкомбинезониликамуфляжцеремониальнаясбруяневызываетничегокромеотвращениясущаяпыткаиначеинескажешьяотодвинулдверкушкафаикритическивоззрилсянаприготовленныймундирнечтопохожееянадевалвсегооднаждынаторжествапослучаювыпускаизучилищаоднакотогдаэтобыластандартнаяпараднаяформамладшеголейтенантаатеперьвашпокорнейшийслугаблагодеяниембибиреваобрелчинштабофицеракаковойнеимеетаналоговниводнойармиимираоставаясьвтабелиорангахобычнымкапитаномяполучилполномочиясравнимыесгенеральскиминикогданеощущалособойстрастикизучениюиностранныхнаречийоднакозаминувшиеполторамесяцаянаучилсявполнесносноболтатьнанемецкомвдополнениекдвумпривычнымязыкамрусскомуифранцузскомуединственноменянеимовернораздражаютсложныегерманскиесловатевтонскиеспасителиосвободителидажеобыкновенныйтанкназватьнормальнонемогутиспользуяпочтинепроизносимуюформулуизшестнадцатизвуковвосновномсогласныхкуртктопросилмолокапринестияпостучалсвободнойрукойпосеребристойбронеугловатогомонстрапритаившегосязаоградоймоегоскромногокоттеджамадамландрипередалатебегорячиекруассанысджемомвылезайшестьутрамеждупрочимтишинастучинестучинеуслышитяпоставилпакетназемлюподнялвалявшийсявозлегусеницыбулыжникипаруразотдушисаданулкамнемпобортускрипнулкомандирскийлюкнабашнеиоттудавысунуласьбелоброваяфизиономиямоегоновогоприятелялейтенантапанцерваффекуртавеберанащекемазокмашинногомасласоломенныеволосывзъерошенывидзаспанныйяведьемупредлагалпереночеватьдоманонетнепожелалбросатьстальногодругаолуиприветкуртоблокотилсяналюкизевнулзабирайсясюдавременималоменяждутвколледжетебенаслужбуквосьмигеррлейтенантглянулнамеханическиенаручныеходикисейчасшестьсминутамиидтидоцентрагородаполчасанебольшеанавелосипедетаквообщедоберешьсямигомявздохнулподобралпакетзалезнаверхиуселсярядомнабашневыставилнасветлыйметаллбутылкусмолокомипластиковыйконтейнерсосвежевыпеченнойсдобойздоровыйдеревенскийзавтраконименябросилисволочипожаловалсякуртявноимеяввидусвойдоблестныйэкипажсовсемраспустилисьнаэтомкурортевоттебеипрославленнаяввекахдисциплинагерманскойармиикажетсятыихсамвечеромотпустилнапомниляточныеобстоятельствавнарушениевсехивсяческихуставовничегоподоспеюткакразксменеотправитесьнабазупойдешьвувольнениезаглядывайсказалжевернутьсянепозжечетырехутрапродолжалворчатькуртпопиваяпарноемолокоявятсясперегаромубьюобоиххотябыпотомучтооткомандиравзводавлетитмнеанекомутодругомугосподихотьбывойнаначаласьчтолимытутсдохнемотскукинетужпокорнейшеблагодарюпоморщилсяявспоминаяиюньскийблицкригкакпосмеиваясьназвалвысадкунагермесрусскихисоюзниковмилейшийкапитанказаковхватитнавоевалисьпонятьнемогукаквынеразнесливмелкиещепкиквебекинеспалилиполовинугородамоиизвиненияоскалилсякуртдействительновмешиватьсянеследовалоавовсенаоборотследовалопозволитьвамощутитьнасебевсесомнительныепрелестишариатскогоправлениясомнительныеонитолькодлянаслюдейевропейскойцивилизациипожалплечамияаподданныехалифатавоспринимаютэтизаконывкачествеобязательнойиестественнойнормыинойменталитеткаквыражаетсядокторгильгофяпредпочитаюменталитетсобственныйсквозьнабитыйротсообщилкуртпопутновытираятыльнойсторонойладонипотекшеепоподбородкувареньеутебяумытьсяможнособакинесъедяттопайпокаяздесьсказаляотбираяпоследнийкруассантанкнеугонюнебеспокойсяонвсеравнонасигнализациифыркнулгеррлейтенантзахлопываялюкиспрыгиваяназемлюнепоказывалещемоесобственноеизобретениеотбездельячеготольконепридумаешьглядикуртвынулизкарманапростейшийгенераторультразвуканабатарейкахинажалединственнуюкнопкутанкморгнулпрожекторамищелкнуливнутренниезамочкилюковипослышалсядвойнойзуммерянеудержавшисьрасхохоталсяэтоведьнадобылододуматьсяприсобачитьнатиграавтомобильнуюсигнализациюасамоеглавноепримитивнаяэлектроннаясистемаотличноработаетдажевусловияхгермесавсектовидитсмеютсядовольноулыбаясьсогласилсякуртнекоторыеэкипажиужеперенялиновинкупридетсязапатентоватьлейтенантисчеззакалиткойясверхувиделкакмоиволкодавыленивообнюхалигостяиучуявзнакомыйзапахуспокоилисьотличнопонимаюкуртасейчаснагермесескучноашестаяособаятанковаядивизияхагенприбыланаэтупланетувоеватьивоеватьвсерьезпочемудивизияособаядапотомучтоонавсамомэкстренномпорядкебыласозданаправительствомгерманскойимперииспециальнодлябоевыхдействийнагермесепричемвеекомплектованиитехникойнеоценимуюпомощьоказалирусскиепоставившиедвигателииорудиядлямашинснепроизносимымшестнадцатибуквеннымнемецкимназваниемпанцеркампфвагенбронированнаябоеваямашинаавпросторечиичтопофранцузскичтопорусскиобычныйтанквпрочемнесовсемобычный

**Висновки :**

Виконуючи цей лабораторний практикум я здобув навички роботи з шифром Віженера. Вмію використовувати індекси відповідності . для знаходження довжини ключа . А також навчився підбирати ключ та розшифровувати шифр текст. Реалізував алгоритм шифрування мовою Python.