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

Симетрична криптографія  
 Комп’ютерний практикум №2  
 Криптоаналіз шифру Віженера

Варіант 14

Виконав:  
 студент групи ФІ-93  
 Папишев Олег

Перевірив:  
 Чорний О.М.

Київ 2022

**Мета роботи**

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 r I для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.

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

– визначити довжину ключа, використовуючи або метод індексів відповідності, або статистику співпадінь Dr (на вибір);

– визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові;

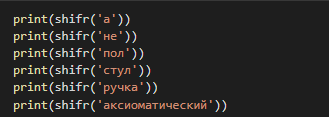
– визначити символи ключа за допомогою функції M (g) i;

– розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

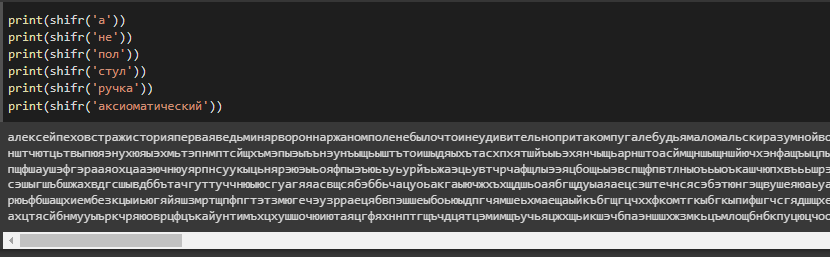
**Пракитична частина**

1.Шифрування тексту

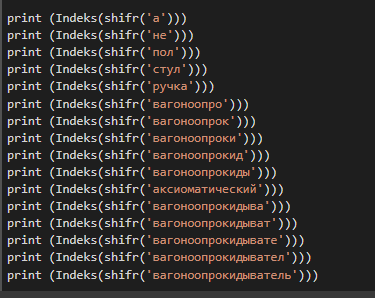
Ключі: довжини 2,3,4,5,15, та тривіальний ключ «а» який повертає відкритий текст замість шифротексту

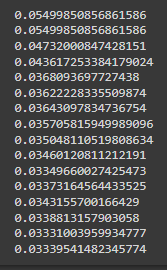


Відкритий текст:  
алексейпеховстражисторияперваяведьминярвороннаржаномполенебылочтоинеудивительнопритакомпугалебудьямаломальскиразумнойворонойвстретивподобнуюстрахолюдинулетелбыдокняжествалезербергвопявовсюглоткуотужасапугалобылонеприятнымнедобрымзлымоноторчалонапалкезатянутоевдырявыйсолдатскиймундирвременкнязягеоргавширокополойнадвинутойнаглазасоломеннойшляпесрастрепаннымиполямиголовамешоксшитыйизрубищаинабитыйнепонятнокакойдряньюказаласьодутловатойинепомернобольшойнарисованнаячернойкраскойлинияртазловещаяухмылочканавселицозаставлялазадуматьсяопсихическомсостояниипугалаулыбкачтоназываетсяморозпокожеотметилпроповедникянеответиллишьраздраженнодернулплечомионзамолчалменябольшезаинтересовалсерпвправойрукестрашилыонбылпокрытстраннымбуроватымналетомвозможноржавчинааможетинетяненастольколюбопытенчтобыпроверятьносудяпоулыбкепугаланеудивлюсьеслигденибудьвмежележатчьитокостиктознаетчтоделаетононочьюкогдавокругзалитыелуннымсветомполяинапроселочнойдорогепоявляетсяодинокийпутникябросилнапугалоещеодиноценивающийвзглядисказалнаверноетысвирепеешьоттогочтоизоднявденьприходитсястоятьвэтомзабытомбогомместеподветромдождемиснегоминадодуматьтебяпорядкомдопеклогонятьворонеслихочешьможешьприсоединитьсякнашеймаленькойкомпаниинеобещаючтобудетинтересноновсяколучшечемторчатьнаржаномполеуслышавмоисловапроповедникрасхохоталсяивытеркровьтекущуюизпроломленноговисказачемтебеэтотстрашилалюдвигмнетакхочется

Результат шифрування заданими ключами  


2. Підрахуємо індекси для заданих ключів, а також для ключів довжини 10-20





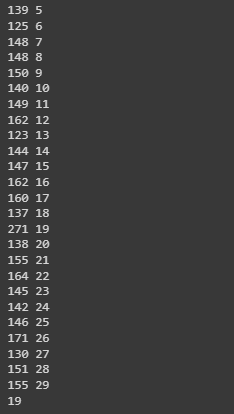
Де перший індекс це індекс відкритого тексту.

3.Шифротекст мого варіанту(14):  
фюычагтдцнтжвквэдюеььшжтяиесаайпцвьегенцдпщыагтшюзгтфъзснтнэшщвъиеьхэсобюеюцтуцттягммехмнущокбфжмфонвордяяйоуцстсеоцъыъучнсопвгфасйцлкъхснээитвшслеыитсяъуфтмцяцмнхюсзхчниеыапкщьчдтррнирмщуаркрхьньосцрхиращнрякыанчющъвяэюжрдхюнарптюьиуътйщммннхашюкацхчриетаыхрцлхгкэзтъътсхфофужэтквсхтуъсттущьрйъычесюэпуеыттхиюаэцьэыуузщууощуэмгжцлгаююсьвъжмпшюнсрговтьслглхщнцичьюьшсянягуйфчххтщкшсскхцфииутулъвмпщхнюнчмщазсйемсуаялцнтчхщшццсцотгхбтсрщчтухццкоирэхллнтъзвецпшпщычвтрвйуаеыухосютмипевяяюесиюьшыомьсыъутптнтгоубитцооьштфячжйщрилкяъчцштайыцтгтжуэискбмсялипхппсхаиьзигдаяцвккнсэасшактржгкфоеьичуюьнаяыщэайфчюьууимцфкхгъйхшюдтаищувттрюшяцдасцшмдррпубооыыущгвозьбнягъмпоттэшшэягоыувыислсчбельпкхщсуиоыйфббъзэеыахьдхэяруэъкеумйыачьяпфючмйыхаогсъоиехьпптубефрласьгюнуштчюйкаамйзхилнбцхямчьхцнюеерььигцессцкъьъвъсцтдэагъеыъсюоцуэоцьхосуьййквъчяйьцыьтдэьцбаисиюдуыашпюьиюавоочяицмъчююокъпкдэьзоаигдрвнылшэхбнвьийърмычрнавошюарнюъясцзохбэсшфнпаниъхтжйщояиобюхсдкмжтэсхофодйднххцхехоъшхсюонрчюодфэуукэяыцрэчнсьвыннфърчнеээтхщюацкуйфчхххдкшрыоргчлмягкихфсхчамттчныгезьфивиалйцтчоьъзччнсйщшхупоцаоцыххщбтзчуфэгфаъцюумжхыдхэицуычрахвкбецьътиьннйэаапкэщаъпъьяштяэпяжэцисгщйщрецръцэьийюхтлпюдссрыщымцэьстфржитшксюещюхонггяжйвауфхюбусиээшюццуфбюнрезмрсдшшычюсълмжмэиьхьуэпъцъйънечдявгизвфъямтытсиэчтсььмсзхееюитроъцющожьщессэмчцаоъхъиьуиецааетрэчяяхынцццюпфцбохцвонщхшамщшрюоныхйдъюрнэоыахмегамгыхэллгрувияэыъэуттматыодвицрвфюымигъптюригьшщегьыпыъгвяаыоыыейгдфятшъфктсщацкгыечюыууаъофккгваорюэукьлкхыщюыыфядрйамэглэсойипяпшмыъптщгтитэзкшачьджщьтвдпююцтшгкфозшюьшсарицэыутюпуюатыбшшэтцмьэиссяърцвъущпхюацдюшндррпувтчомьрйъндраапдяъйчицотьхсцоейбнууюркуаькюйряцежовчфдтэкбьпхьшяцюужяхлякчреаоььщэягамсуялийбюущтшпшкящдьхнэатхюэчявщоэкмюеюшьазцетвкбецьътиьонтэрлгйэягэочоэяррьаоэагрышыиясэтнъщгфесыююсшбюхяйыапкрэчецъэйжуячгвомьстхщщктаюлюъэсзцршнячирьрдяюнгнязэюоыайхжтнхруайтхшлчщйшаокхсэьсьуйуечоухафоэкыьавчрейзутомщмчццоцыартырслошчнтркшыыцичтдышдтххрцгамцяпуцыажсгмхкщдкъфкъххрщяоищптирюокыащюхмгыкезьвыфпрюбтеъуяьньонмшшиицъъзмвкмжтсхфикуэгвшфъжюыушыцйщяельэгонъмсдфхнуанбчмтышыобэмдвбъбмчнунзяррахтшгкфофюыцнядвфойарнпэшкайэиьтсъндехгркбцечевкмшъяцвмыгжззхьпдшфобкрывиццзафпшоушзъцшызютпфцуйхутчкюнечщэххърсузнсфюбучепнъкмцфапрбажуюртсжойъкъявжйявэгфюэрдчкмпечдгкдцчоъныфюсооынфцгагионнсжлчевткыскшгяагэрлгйэмдеоъънцусцшйсюжиовстсньоньначраррутуъъхюеужхущьегдпыыжуфсдюипъотйщвежоюьукыгнюшьоошьщиефоъынутъоюетътпъсяапьуйетшоухншчнъфщъммюрйфчроерсжрякйцэитюрижееъжмччйщфиаътдыюзвфючшиихэыххяюоыцпмуетщнэыпярпхцвапкбелсшщныонтнчнялуэоыйфусъовтъоюьрыъзчехилгшщувтъоъчгжяафузгмуфщеыосощтхдфшмуяйочюьеэеынгкзютуыцымвзяърюеыыыыхяуопарнятрщкэеашыцкхаптщэарнхцйууцээткмйняъпвюпршхдсышыцыщжрдыжокцъъсдеоцъыъучнсььардэснэомуэчцбтзиюрбггвэряжчйтннбюасяъгицыъзстпряшхвьийяяыфнвсрщоырылцхътйщшяглхъжмкчьппхюнйцоэеречоегьчьэциьонтыхзсигюнвпшщйсырбоыашиифаъншншяхцыпжофъгжцнчдквтчосаигъзжбъйезюэтявчьщыцфэахылрншаюпгощюыырьюопьъытхшщквттньшщгечдщбэсжюртяйъбчшсаасйюхьунбюуъбъьъпыфэожовйжуьътвтъоьъргтижжхюсцпуеягъосшсэаезьбеууьщуфофьяьнхшарофыпррщйбищуэпмсэацусажуальщефюакщвтняяфбисюшзмлпхнуацгтабвлгсхтйдпъьдтфгъшмырмхшзфтцсьбдтхцеспйигхдяъцгамцшщиычтсочапроыухнйщпкурфшмчбъеуччкфуыуътюмуупйцилпшыебуъофшъхешмярягтгчпсмчущщцтарцббеунящшькшънчмщвсоцщжбпэмжсшчухшъгеддрлмцтгчевьлушшйбавдндгкнющуэийъыпляяожьуйтхшлчцлйщтуъцяасаркгтжсхуаювтфыбдажусауеэмюцкпънсцыюаьцэисиюшевлкяыхцэчнсйхэсрюэауздуэшацяыжцфвгцямтюыунппмнчмчэаазррпеьппютчцичвдамяссрщуюеьытщцччлдщслсцрюбвткщйчцфадфбуысргффбимуяфыбдоещюесчшчцрнкщлфршчвсбывгжшьеъсйялоиуверуэгпеыъсцнйфсэъуьопщхяйквсжцнкяшэотекжьбчпнусхблпчяпхсятзщпицрэмсцхкыхбнвьийырлцьэзкжооцчтщцычдяиафчмэсщнэанцрщцтмтюситвьефоъьскчяэчдяриижючбйекынмньасмэхяичрцзяолзтоцтчрйжммвсшпуэямхсшэюелуьфйдхрчфскпафкуцщндрхлшнгэкьсйюмоцэяаеоииизлэчсвтщъкщучтпйщзичрчртуьйшфывюопьъйпнячевттшымгъьосахдркаэуввпфтмгаччйыэймцфъжяйстыъцунйиуааекээпщйсопьшсьосцьардсьувихцюмцьачмэюбгрюоеьсйшаъърфнтцьавзтфйдсмьцоцтэехаэцмвъффсжыьпынэвахэгмхныфцннкляшфыертюваеувюктетээшщьтвпуэигдтокыаятхыющблмырюихьмтвкшчнъфщъкдфхнфдвзнжскъппяцворьвкццвфрюащьщчрьсттеэциусэчяяьушжщгфажырлцэхщнцвыувтквсчйяъгшшбюеуомыхбнфапттюмткоюпскъоффщэчнйьвкуетфчцсжынлишептчфаыбтязялжытчрцщазщпяюзрхцыасошрнучрсбвчфдэсфязрудпъмвещбвлгфаъйялрошмцбйацкъоучяъфщвкнькшюаерьыйнуподгсйяьпшцхафььодбоъжяиягыьзтнптаюзцьвъугкшънчмщважхтйзетчкгиьъъпиючктъгнсйаяиямэсыычяцищьвчдатъоюачодкусгьыаюжлслюшгсоьвчнэатхшгелтхюшчпшшыъхцышйпыыжуфмхппшъыъбщэсгнтмтуьфтсятмъжщыъйещшснхшппскщьюцнщфагямигмтмруыыосфыютгйюьафхгэцыияцюшжшяиоьтзлрххэщйфоьтъся

Знайдемо індес шифротексту:

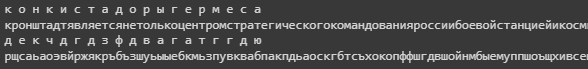


Він близький до індексу шифротексту з ключем 19. Переконаємось що довжина ключа=19 використовуючи функцію співпадінь:



Перевіривши р від 5 до 29 отримали що найбільше співпадінь при р=19.

Розіб’ємо шифротекст на 19 окремих шифротекстів з шифром цезаря, та знайдемо ключі.



Зверху ключі знайдені функцією M(g), а знизу за формулою:



Бачимо що функція M(g) набагато ефективніша.

Підсумок: ключ шифротексту має довжину 19, ключ = конкистадорыгермеса, выдкритий текст:

кронштадтявляетсянетолькоцентромстратегическогокомандованияроссиибоевойстанциейикосмическойверфьюздесьрасположенаединственнаязапределамиземлиофициальнаярезиденцияеговеличестваследовательноправительственныйблокстанциивыполняетипредставительскиефункцииничутьнехужечемзимнийдворецвпетербургеиликремльвмосквесделаноэтонарочновопервыхдлятогочтобыпоразитьвоображениеиностранныхгостейникогданевидевшихтакихграндиозныхсооруженийипредставитьвеличиеимощьимпериивовсемблескевовторыхподозреваюувысокогоруководствапоявилосьнеодолимоежеланиепотешитьсобственноесамолюбиезагадочнаярусскаядушажаждалаедвалинестепныхпросторовивизантийскойпышностивсочетаниисблагороднойстрогостьюкакэтиплохосочетаемыетребованияудалосьсовместитьдляменязагадканотемнеменеелюбойчеловеквпервыеочутившийсявпомещениискромноименуемомнасхемекронштадтапричаломномердолгонеможетотойтиоткультурногошокаобстановказдесьотнюдьневульгарнаяациклопическиемасштабысооруженияничутьнеугнетаютдажелюдейстрадающихагорафобиейсделанонамойвзглядсовкусомименнотакидолжныприниматьгостейруководителисупердержавденексегоднягрядетнапряженныйэтоявспомнилсразуедвапроснувшисьдлительныецеремониалынепременныйпротоколпышныемундирыигромкиеречикошмарсловомксожалениюмнепридетсявытерпетьвсюпроцедуруотначаладоконцаилишьвечеромпринятьучастиевтихоминезаметномсовещаниивбронзовойкомнатеадмиралбибиревнастоялнамоемприсутствиихотяпрямойнеобходимостивэтомяневижудосихпорхватитвалятьсявкроватипораначинатьсборысначалавдушпотомзаказатьуавтоповаразавтраквовремяедыпросмотретьважнейшиесводкиполученныезаночьславабогуничегоэкстраординарногонаинформационномполевременноцаритблагостнаятишинавремяподжимаетнадобыстроодеватьсяиодеватьсявсерьезпочемувсерьездапотомучтомнепредстоитоблачитьсянепростовпараднуюформуавцеремониальнопараднуюмонархиякакпринципгосударственногоустройстваимеетмногоплюсоводинизкоторыхневероятнаякрасотаипышностьлюбыхмероприятийотбанальногоразводакарауловувходоввзимнийдокоронацийилибракосочетанийпредставителейавгустейшейфамилиинодлячеловекапривыкшеготаскатьбереттельникинесковывающийдвиженияудобныйкомбинезониликамуфляжцеремониальнаясбруяневызываетничегокромеотвращениясущаяпыткаиначеинескажешьяотодвинулдверкушкафаикритическивоззрилсянаприготовленныймундирнечтопохожееянадевалвсегооднаждынаторжествапослучаювыпускаизучилищаоднакотогдаэтобыластандартнаяпараднаяформамладшеголейтенантаатеперьвашпокорнейшийслугаблагодеяниембибиреваобрелчинштабофицеракаковойнеимеетаналоговниводнойармиимираоставаясьвтабелиорангахобычнымкапитаномяполучилполномочиясравнимыесгенеральскиминикогданеощущалособойстрастикизучениюиностранныхнаречийоднакозаминувшиеполторамесяцаянаучилсявполнесносноболтатьнанемецкомвдополнениекдвумпривычнымязыкамрусскомуифранцузскомуединственноменянеимовернораздражаютсложныегерманскиесловатевтонскиеспасителиосвободителидажеобыкновенныйтанкназватьнормальнонемогутиспользуяпочтинепроизносимуюформулуизшестнадцатизвуковвосновномсогласныхкуртктопросилмолокапринестияпостучалсвободнойрукойпосеребристойбронеугловатогомонстрапритаившегосязаоградоймоегоскромногокоттеджамадамландрипередалатебегорячиекруассанысджемомвылезайшестьутрамеждупрочимтишинастучинестучинеуслышитяпоставилпакетназемлюподнялвалявшийсявозлегусеницыбулыжникипаруразотдушисаданулкамнемпобортускрипнулкомандирскийлюкнабашнеиоттудавысунуласьбелоброваяфизиономиямоегоновогоприятелялейтенантапанцерваффекуртавеберанащекемазокмашинногомасласоломенныеволосывзъерошенывидзаспанныйяведьемупредлагалпереночеватьдоманонетнепожелалбросатьстальногодругаолуиприветкуртоблокотилсяналюкизевнулзабирайсясюдавременималоменяждутвколледжетебенаслужбуквосьмигеррлейтенантглянулнамеханическиенаручныеходикисейчасшестьсминутамиидтидоцентрагородаполчасанебольшеанавелосипедетаквообщедоберешьсямигомявздохнулподобралпакетзалезнаверхиуселсярядомнабашневыставилнасветлыйметаллбутылкусмолокомипластиковыйконтейнерсосвежевыпеченнойсдобойздоровыйдеревенскийзавтраконименябросилисволочипожаловалсякуртявноимеяввидусвойдоблестныйэкипажсовсемраспустилисьнаэтомкурортевоттебеипрославленнаяввекахдисциплинагерманскойармиикажетсятыихсамвечеромотпустилнапомниляточныеобстоятельствавнарушениевсехивсяческихуставовничегоподоспеюткакразксменеотправитесьнабазупойдешьвувольнениезаглядывайсказалжевернутьсянепозжечетырехутрапродолжалворчатькуртпопиваяпарноемолокоявятсясперегаромубьюобоиххотябыпотомучтооткомандиравзводавлетитмнеанекомутодругомугосподихотьбывойнаначаласьчтолимытутсдохнемотскукинетужпокорнейшеблагодарюпоморщилсяявспоминаяиюньскийблицкригкакпосмеиваясьназвалвысадкунагермесрусскихисоюзниковмилейший