

## Міністерство освіти і науки України НТУУ «Київський політехнічний інститут»

Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

### Перевірив:

Чорний О. М.

**Виконав**: Студент III курсу ФТI

групи ФБ-71

Поліщук Володимир

Київ - 2019

**Мета роботи**

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

**Порядок виконання роботи**

1. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.
2. 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.
3. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
4. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

**Опис роботи та основні труднощі:**

Для роботи було створено текст, який містив у собі цикл статей про шифрування та криптографію. Текстовий файл розміром у 4 кб оброблюється програмою за 0.015-0.031 секунди в залежності від обраної процедури (зашифрувати, розшифрувати, порахувати індекси відповідности, проаналізувати частоти….). Програма написана на мові Swift.

Має 4 основні функції: 1 – зашифрувати текст; 2 – розшифрувати текст за ключем; 3 – підрахувати індекси відповідності для визначення довжини ключа, яким зашифровано текст; 4 – аналіз зашифрованного тексту за довжиною ключа. Остання функція розбиває текст на блоки за заданою довжиною і рахує 4 найчастіші букви в кожному з них. На основі цих результатів і відновлювався ключ. Особливих труднощів під час роботи над комп’ютерним практикумом не виникло, за виключенням підбору букв ключа вручну. Для цього аналізувався текст, який був одержаний в результаті найпершого ключа, який запропонувала програма. Серед розшифрованого тексту можна було помітити слова, які були схожі на знайомі нам слова російської мови. На моменті, де ця відповідність переривалась, визначалось, яка буква за контекстом не підходить, і яка повинна бути. На їхню різницю і здвигалась відповідна буква ключа. Згідно з результатів, 11 букв ключа було підібрано автоматично і 5 – вручну.

**Результати:**

**ЗАШИФРОВАННЫЙ ТЕКСТ**

втяугроъцсхйиббьыеумчцтптикуочяькуфупчхлоюгжкйцтарсъшяуьнныфонингвциюфыовилъсвнфтюлйдгашьицсывьилхтфчнфуэуърттцяцыпюраэпеябчнсюэещфпаьехехацидмырмрцшсжчдуещущцсттйырчуббвпкяхймнывкуйъыьушэйаъдфмтипъоыпюудмкнтйлдтукасмшъннвзикзыдныкткшцпчыкнпкбдмычткчоыъбеээъехчрызпщъттыужупндзчртшънцжшыцврчэдихаяяълчмйфзвзрчнлятыыхицйсбцхпнфпдрмюашяыпалквмурйццнхьпъиьапчавтиъашышнйэъкюптюрфызышьяцпщфтфочцмххцацвньщцаьысцыщшпцикаомхркьуысдкцщуысннхпоншьожссуючдзнъяышдмуъчжвзаьицбфюкъешещшъвзтчышиюыкуцкэпхивърешинхщлыюьоъгчроьхыммтгбъчцбтжспкайцяущюпчщпчскпвчйсыхяомчнъшяькгпупижысянщцлпгтебуешежрнывьынйяэозхфсалинйццзлхыдужвйчкчгдэярифшеыазнндчдфоуцькхшгфшжвинтгидтькъечшыущгапнънтйрбиъшхюкзрьъалхепвщцхчысэюрстрхэиыбтьйявякъучнзюубиышшйлюлзезцчкэивмшврхнюпзйупшугрвещцхсршжквгученъоозпучмуббздулсдлишдмюоъэснзоуяхххачсцхссчптюбцпдицгыыктхшцрахпкпцецмъщьдъфуъуевцъалятыжъышфышсдлпыхцйлйцокйьбъпгхзпцычрмюшщытгпцзэфнрюйыпушмьтхэргэуорытлхтмфчтлфравтацбцвыэбъчцбфждееяцикоюгкуччыжквксыибрбмялеышяушввчйтымущсйчщтеэснфутцбрбясфщфэкчрдубщтычрхйхцъжфкмцехациртйюплчмбянизмъефзаъгшхсшцяшзфнячжнвычкщесуаздкчызцшынюьццтбькидкэбинмъцлуйнбуежацайтйущяушсыэькджтысйзвпцърфыжутйпкыйгцмащцнъьжаузфумттнмыцчнхпгччзбчтпйбищфшмчцтькщтшжшюпзнэшрюьбсежрзюебирхюшъчнчпзсйтньюъвшплуочоптиртхуеысяяпщйхуянгрттзбжбшцчгыкэапцикщзсчедсхдцеъпчыоьяушгнтупщохоччднбчувцгшщлщхптббзбзичшнрсрйкоышъмцфкщьицнтфъывэчсшбкьъаязнавфуичжабиржыожцдхгщшсъбуезфхнтггхшпонтшчьнщнефкфъивяяцаэещеасуьшщийавхгбкхзнядушагтусбэлспщфтцднспцтучвэщутдъаивпдчдкушмлтосжрагзфыпцоуяыхзцтдлццоттцицрдгшпйлустцъшяпцкхыхйъккдаегкушужннгятлщкйчегрцнрцхиыушъкхутужрйъаяшосщбкйвфпцзвтхущшагщкхчтюэхыпыыцгрмьбшбйуефссдраьонмытгнъьхфузфепнвкаювкуйъыьудучнрззбмиьцкмуахцйзтцыуиянчцлшеозюишяклттыукфншгэлывтяугропэшрюнюпмцчыттцкащхшшчнуайцзчюдвхедгшкйычфрцйупширрнхекдщгфйбриашъилхгжщиыуъежктыфжрвтгмихнбафджеоезщаъщшщсчпэхспучущмауэеччыяфквудчущмапмбъчьбачцннъкбждхэещйхуянгрйыцйлвнйцгнпюччтеуяушгспсцръкюпхюпухццуаъщшыюшчочбрхттмцкосыщйчыэцюпбыхжизпмкхышачугвэшнвгвнвшщыкхчсгрфэуоыкытпмьчшюуэвжичтлдтэемчхщьазроянздбнвыицтбюхюжшъешнръяншйаыптдунъбдшаъгшхсшхчййдеюфбцхыъщнапефцтурхэацмпмшйфкцпъвкхнпицивгъыншяжхыйстхггмьяфышкшбчытдтчюэкнытпхпачрюубпацхтыютцицыяцнкчнгннмыюпщыжцяемкеъувррюзпхйнчфшшудчущцеюгжшчхпыухехацихарбкюскаэсгзлсеяъеэяхдбэепфйупнодъсщцяикэчвзыубпсдшщхюкэшэдбббхьекенчтюжцымыьещрххчннмюгехоьдфхъшкычизжтьеэлсчэъддмньыфжтипучмшщшзфкьрдскэямдзыыукиюфыйдйныэъихшгьувхфэкътуюакъечуозйкрхъшцрнгжоохевъдлуяхцпдэсрнцжтарйъецпциняячрчьшрдбажшгхлопяърымбытынгоушдеюгжузоывпдфуэалуигсщцуъобаенкъпдстыичцмхуубчррычццнхжъицйеьежрьъугнпыхмрпчбачтщчыждйщнрццфмучсетньнзилнвпшепъьузфбщшъшоюгжрмхжруакоасющлыучцмшхэххфтнсхцрныэуушцуешзюнгеысянтчоыафрцзчысдсаъгшхсшъьефбчнпюэчяяцынъоынзнапшиуиенщцышявьиртхьылоъцнцлшгочирисеаикфснцлшгчздпнякжпашщлыбтефсафухъзуыеслусрачъъххнпцфиъсскйхфкзыттыйццбкгшфшшдъкгрттрдкиямчишъыыегмшрхйщтхгктьидъешхлнраыюэмлнбфжюуяжкщрдшеъзшхьщбщеетужеяипэящцлпчлдартдшецооцоилхбякгшухчцтвнвшщыкхъдыойыучнднаърнпеадвпкоаидмахъняшябеаксокэфошучгхнбсужкчйтымаюгншйаыптдехныюиныхкччрыснзрсъуфлоссокйсхвпщррыццъыюушнмшъпжйжкебцхтыютццэчъдизжмдзъаъдлцфьжьувехныюиныяьусбаэзыжбщубяаънпэчъбзушмуььыхыврсгукиуешщнючсэдтукэмъуенцпухрдшеъзшыюшчочцпчытюцгсцыфдыюскщрцшушихосыщйчыэижвыхегцгыушшсьффцарттьгцмъянцшэдбдарзоубдштипфуьбънчрзпкгнцхщплчъуацйийттюзэяяокйсшятцсэттююыюаъзыкаьаыдйпшлфеэсяфифыьанфуоаюэннъьрцкчэнзмеябшнсйхпхекапоъзэйшшрдхйжяышычцавчйтыщтыщхцлпафыюбшшнмиввяорыхуььынуярцхчтьшъушафьгрцызыщтйэшзшшъсубкчщтыщбтчкъешемчдеуунъимыцнцюшъонгвжтцвннмгктлшеччднпнкиъачушъстдщшовкяидкоэщьлчлфэрцпьтрдъгытлцншфяаянеъьыуоящхрншфяаяеуождрлххшйщеьъегщкшуилоотшчьыечтденпъдмбтфткчмдфчхипхкймиэсуцыысуецуупкзъьрямцщтеькисуючдсчтвьхдуюптнзрычецсяяуяоыеьаяеуождрлхыктлелфцавмнтдяеюгчнтвышрцпьтрдъгытлццпжунжвояуехиъянцтчумчюоаюрюуасюшиюъурхслййдшцлпцхрыцафцанесашитйашосьэчзехчйидкоэщьйоыяпхоеупужртоцышйоырущвцыжышиюнымьябыиддуэнийеющхыштюпйгреюушнсянццимшзеыфцмтцаелыццоцжакжжыанвыдэянцлшгччвродкзъниъошьнюптнзрычшндйгещдчкфципурудъцнщхръфбякыуаъьыщтъяуфйьшянерчысйятывфиркелфжвзсшдъеггшфчуафцаррйпдтачтееышхкхцйнябззояхккйхкфсиржирйхерязъйфышфжкзчшзуасюшщчмшачтоттидкоэщьуйчкфрдфттэыкешщыдшшлфзыннпеящярямцщтеркзпнюсыщтнфшкчъыбцддкючтщопцыъенбсужафэешрлйюшъдыбскихкебыщлхашксчбсеиюцмцдкеюгтхйобытырцяеидсмдррнкяэкщръымхрннсшхышвяузфнщкгзгывщцнтдпсштускъдяпяхийбеэжсхйэеидоячтмйщгчйыфцмфдкиъямиыждорймепувыапцодччеэцшвэтидчофушуочыоныучйццфдйрмцфтеэфжвзсенъоущокчщюэюыптиоъдяпяхршшдэзыучхидкоэрыцлпдббврдукзъочяынщоапдзрзтцидеюьтццкяькзрзтчйнтывьиыждошькйнжыщмъцоиоьфэрызйэшьнсчщущчмшбдивпхшънрахжзлшюыуюсдяпюттпятфьыювицошскжыввяорыыепхслиыжчцсчяъпсчээощржоувцлыхшсъталужупнлюъеьярифэьачцмеччйъпэяуъсфдчттрхалюмушсчяохббззфуэугыоъцлцнкрбувротйюхоэяохдуббкмртюрычтныыучмаэквхттчдятыапщушяппжхфъавлрнутнхнюпмцйеюаеилыюпырчуфчвзтмцслрнпыхсцэппйатхжймьегэтьнбрждсудчыхнтъвртцбъуъроюнгдоэвонфкьбквкрыцидкныцхощгэоикпюнгдоэдррнэюптнзрычцчопцъхсьшьеетепуешиьцъкчцвэздтуякгцпэщыихшяюкждущфдкоэяьншшхфхгкчттцуепяоиъцббхюфкьхюхаюгшзвпябуерзыхдъеъцщцлшгпьюдецчыхиъсщшймбьнгвртздивыбшяйуеффжбстъдхьчяфмчцжхнъвиыжчцспрьгоэцэйгкпхчжыдъялынпеюуевцябгиннвьцигжнйдтуршшгнтэшооьшапцйеябвхеъцфртхуььынуяьицуъцнцптхфчькзтчйхерятусчшбрцпьтрдъвифшкчъыбкдоушуъцмющчдчъшъегщкшуинвюгшшччжсуисуруърттыктьитакящеюнзъоэщишйсхфййучнхютупмнцлшгччырсырдмощвтхешгфрцпьтрдъерялйчфущуяфещцюхьыбмибкячрдучйцсхбтхчцмшкфрддкчедъегцнцюшелвирдюевлопяъжапдбтслтыунннйтпмцеьжкбрзтплцтмтхимшчпххгуреэмоэямгтхуььынуятйттытеъйцачжснкрудъегэелчмбянврсырдмощвтхешгфрцпьтрдъерялйчшъьеарсысшиштъцрфшдбнетуючдуаъипучьшашъвхйрцхчтьшъцшвяуохзнцзъаэщфъчлызбйоушдфкаювхнныескгпупащцвыбтъошяэрджущцюхьыбпуйчкфрдфкручйоыькхапюэчыуфымшцлтютзлклфовкрыцирлнюбнфшеарыжцязыхныяырцжбякбвтдкбцттюплчмбянизуюнгдоэцхицбшъуизжнчфакнэшсслбмчдфсырдмоцвтхешгаущнеютдкошцыынпфчхдмехзззкхжьиутивьыпавзыбецуъцнпеяклукючышпнбштсщгэьючуяхцщлтъчиьфыукяучпнинлйюшщушажебудхрюнсшщццпчбсажвмхчтщяьбшбошеээынзшшнаицэтшмшфрущрцьуъруьсырнкхфйтоешбныгнюлгфтдбнгпащфдщовяцфчпьачцтуючюрсящчхчуяэкясусфдшоцькхапюэчгзшучдояьяяцпчуюебмшхрюхаосхтьчуюузръхрюхаьяоччъэвзсокъдгнуфюкныпфпчфъпнидйбыяяхоьтсезпкфтцжмыьшмчудчттрхъуешоедмиъыэплюфкщтычрнуоыаьбыуяоешбнркааштчуцэцерййкщцдайэосмыънерстхбиндцхцычшвлирзитыызъспъоцшьдчвчлэаигытлцчяцэхыбзтйтчодгтяышбарысттфжрзъсикйыюптнзрычгыпыаъилошуеьзжайтывнвнуйсусфдтдспыкыхгшфчнючжспкамгитйэпхиэяфтирчычыючяяэпцкшбцдгцязыхныфшшолшьпцнестдщтнбттимуызззхнцзтаудщшчмузкщрцитцщтнюшксьдотцмушкгрбшснцъхбснвзтмфживссоцфрапзслчхтцщвтгэйсудбзцжушидщкэммиыжафртйдччдяецвехжьбапжэчйсдоныюшкушаекартгушчрнуоилеьукипеэшьы

Найбільший індекс відповідності для ключа довжиною 17:

**КЛЮЧ:** *венецианскийкупец*

### РАСШИФРОВАННЫЙ ТЕКСТ

*антонионезнаюоыаегоятакпечаленмцоэтовтягостьвамяъфышутоженогдеягрьътьпоймалнашелиленобылчтосоставляоычтородитеехотелкдзнатьбессмысленцйягрустьмоявиноюаыосамогосебяузнаыемнетрудносаларицчвыдухоммечетесьшчокеанугдевашивефсчавыесудакакбогйыеиивельможиводифепышнаяпроцессияхчрскаяспрезреньехъмотрятнаторговцолмелкихчтокланяюыъянизкоимспочтенеомкогдаонилетятнйыканыхкрыльяхсалйциоповерьтееслибиыакрисковалпочтилъечувствабылибтаххоисмоейнадеждойикыпостоянносрывафыравучтобзнатьотуьдаветерискалнакйщтахгаваниибухтыфзбойпредметчтомомкынеудачумнепредлощатьменябынесомцонновгрустьповермйлсалариностудямчтсупдыханьемявлиючрадкебыдрожалотхдсличтоможетвмороьраганнаделатьнехчгбывидетьячасовшосочныхневспомнилбиомеляхиорифахпщодставилбыкораблелпескезавязшимглйлусклонившимнижеаомбокачтобцеловаыесвоюмогилувцерклссмотрянакамниздйциясвятогокакмогкдяневспомнитьскафчпасныхчтохрупкитхойкорабльедватофунуввсепряностирйъсыпалибывводуивчфныоблеклибвмоишофканусловомчтомоокогатствосталониаомимоглибяобэтомньматьнедумаяпритчхчтоеслибтакслучсфосьмнепришлосьбдрагруститьнеговощстезнаюяантониогщьститтревожасьзаълоитоварыантониоцотверьтемнеблагонйрюсудьбумойрискцоодномуявверилсунцунеодномуиместуъчстояньемоенемерсысятекущимгодомяцогрущуиззамоихтолйровсаларинотогдйлызначитвлюбленыйцтониопустоесалащсноневлюбленытакъуажемвыпечальнызйыемчтовыневеселысыолькомоглибсмеяыесявытвердяявесефратемчтонегрущудльличныйянусклянуъетобойродитприронйстранныхлюдейодцсглазеютихохочутуйкпопугайуслышавбсйволынкудругиежоцавидкакуксускисфдтакчтовулыбкезукднепокажутклянисеъамнесторчтозабалцашуткавходятбасъйниолоренцоиграцсйносаланиовотбламчродныйродичвашбйъсаниограцианоилчщенцоснимпрощайтохывлучшемобществочставимвассаларицчосталсябячтобваъщазвеселитьновотилижутехктовамдорчпеантониовмоихглйрахценавамдорогаънаетсямнечтовасдофазовутирадывыпронлогуудалитьсясафйриноприветвамгоъшодабассаниосиньчщынокогдажмыпосмоомсякогдавычтотоъыалинелюдимысалащснодосугвашмыделсыьготовысвамисалйщиноисаланиоуходиылоренцокбассаничъиньорразвыантонсчнашлимывасоставсхнопрошукобедунешчзабытьгдемыдолжцдсойтисьбассаниошщидунавернограцийцосиньорантониовснувасплохойпечетоъьслишкомвыоблагйюмирактоихтрудомащезмернымпокупаеыыеряетихкакизменсфисьвыантониоямищъчитаючемонестьгщйцианомирсценагдоьвсякогоестьрольхчягрустнаграцианчхнеждайтерольшутйшускайотсмехабудьлесьвморщинахпусыелучшепеченьотвицйгоритчемстынетсощдцеоттяжелыхвздчюовзачемжечеловеуьстеплойкровьюсинотьподобномраморцчмупредкуспатьнаилуилихворатьжелтьюойотраздраженьяъфушайкаантониотекилюблюяговоритвохцелюбовьестьлюдиьуоторыхлицапокрыыдпленкойточногланеболотаонихранятцйрочнонеподвижноъыьчтобобщаямолвасхприписаласерьезцчстьмудростьиглукчкийумисловноговчщятнамяоракулкогнйвещаюпустьипеснофаетомойантониозцйюятакихчтомудрыхсслывутлишьпотомьатоничегонеговориытогдакакзаговорслонитерзалибушитохктоихслышаближнсюдуракаминазвалбдлернодаобэтомпосфононеловитынаприхйнкугруститакуюсфйвужалкуюрыбешкушчйдемлоренцонупоуйпрощайапроповедеикончупообедавлощонцоитаквасоставфиемдообедапридетъимнебытьмудрецомыйкимбезмолвнымголчритьнедастграцийцограцианодапожилссомноюгодадвазвьуголосатысвоегозйкудешьантонионудфитебяястануболтуцчмграцианоотличнчледьмолчаньехоробчвкопченыхязыкахнйвчистыхдевахграясаноилоренцоуходиыантониогдесмысллогословахбассаничмрацианоговоритбоъконечномногопусыиковбольшечемктофсбоввенецииегораъъужденияэтодвазещцапшеницыспрятанцдевдвухмерахмякицдчтобыихнайтинадчсскатьвесьденьанйтдешьувидишьчтоисъкатьнестоиловенояияулицавходитлацаелотланчелотконоаносовестьмояпозлчлитмнесбежатьотжыогожидамоегохозиснабесменятаквотсыолкаеттаквотиисуьшаетговоритгоббчфанчелотгоббодобщдйланчелотилидобщдйгоббоилидобрыйфйнчелотгоббопустсцогивходбегивовсоыяжкиеудирайотсюнйасовестьговоритцотпостойчестныйлйцчелотпостойчестцдйгоббоиликаквышоъказаночестнейшитфанчелотгоббонеунсрайтопниногойнажыимыслиладноахракщыйдьяволвелитмноъкладыватьпожиткслпутьговоритбесмйщшговоритбесрадикчгасоберисьсдухохмоворитбесилупилйнноасовестьмоявебйетсянашеюкмоемуъордцуимудроговорсымойчестныйдруглйцчелотведьтысынчоътногоотцаилискощоесынчестнойматещспотомучтосказатешравдуотецтомойноъколькокакбыэтовдщазитьсяотдавалчохтобылунегоэтакитшривкусладносовеъыьмнеговоритланчофотнешевелисьпошолеливайсяговориткоснисместаговориыъовестьсовестьголчрюправильнотысолотуешьеслиповинолйтьсясовестинадохцеостатьсяужидамчогохозяинааонтопщчстименягосподисйхвродедьяволаачтчкыудратьотжидапрснетсяповиноватьсифукавомуаведьонтчъвашегопозволениисестьсамдьяволитчшравдачтожидвоплчвенныйдьяволипосчлестиговорясовесыемояжестокосерднйисовестьеслионамцосоветуетостатьсиьжидабесмнедаетбчфеедружескийсовеыитакиудерудьяволхчипяткиктвоимусльмамудерувходитстйщыйгоббоскорзинкчтгоббомолодойсинечрскажитепожалуйъыакактутпройтикссцьоружидуланчелоылсторонуонебодаэычмойединородныйоыоцонслептаксловнчомунеточтопескомйурупнымгравиемглйразасыпалонеузнаоыменясыграюснимкйууюнибудьштукугоккопочтеннейшиймофчдойсиньорсделайыомилостькакмнепрчттиксиньоружидулйцчелотаповернитецйправоприпервомпчлоротеноприсамомшорвомповоротеповощнитеналеводасмоыщитепринастоящемычповоротенеповорйаивайтенинаправоцсналевоаворочайтошрямехонькокдомупсдагоббосвятыеугчнникитруднобудетшчпастьнанастоящузнорогувынеможетеъуазатьмненекийлацаелотчтоунегоживоыживетунегоилинеыфанчелотвыговориыоомолодомсиньорефйнчелотевсторонулчтпогодитекакуюяъойчасисториюразвонустарикувыговорсыеомолодомсиньорофанчелотегоббокаучйтамсиньорвашамсфостьсынбедногочофовекаотецегохотежтоясамговорючесыцыйнооченьбедныйаоловекхотяблагодйщябогаздоровыйлацаелотнуктобытамнскылегоотецмыговощсмомолодомсиньорофанчелотегоббоозцйкомомвашеймилосыспростоланчелотеъьдарьланчелотнопщчшувасстариктобибеумоляювасследстлонновыговоритеомчфодомсиньореланчофотегоббооланчелчыеспозволениявашотмилостиланчелотъфедственноосиньощоланчелотенеговощстеосиньореланчефчтебатюшкамойибожыотмолодойсиньоръчгласноволесудебсщокаивсякихтакихьаеныхвещейвродетщохсестерпарокипрчаихотраслейнаукинойствительносконайлсяилиеслиможнолдразитьсяпрощеотчбелвлучшиймиргобкчгосподиупасидавоньмальчуганбылисысннымпосохоммоейъыаростиистинноймчойподпоройланчелчынеужтожяпохожнашйлкуилинабалкунашчсохилинаподпоркьлыменянеузнаетебйыюшкагоббоохнетялйснезнаюмолодойссцьорнопрошувасскйпитемнеправдучтохчймальчикупокойгчъподьегодушуживифспомерланчелотнеьптовынеузнаетемецибатюшкагоббоохгчщеяведьпочтичтооъфепнепризнаюваслйцчелотнупоправденйжебудьувасглазалшорядкевыитомоглскынеузнатьменяумоцтототецчтоузнаеыъобственногоребецуаладностарикявахлсерасскажупровабогосынастановитсицаколениблагослолсменяправдадолжнйлыйтинасветубийсыладолгоскрыватьнофьзякточейсынэтоъурытьможноновконяоконцовправдавыйнотнаруж*

**Код:**

*ef search(shag):*

*b = ''*

*index = 0*

*for i in range (0, len(text), shag):*

*b = b + text[i]*

*dlina = len(b)*

*count = Counter(b)*

*#print(count)*

*for i in range(start, end+1):*

*index = index + (count[chr(i)] \* (count[chr(i)] - 1))/(dlina \* (dlina - 1))*

*print ('index: ', index, '\nshag: ', shag, '\n')*

*if index >= 0.0553:*

*#print ('index: ', index, '\nshag: ', shag, '\n')*

*return shag*

*def find\_key(i, a, O):*

*b = ''*

*c = 0*

*new = ''*

*for j in range (i, len(text), a):*

*b = b + text[j]*

*count = Counter(b)*

*print(count)*

*for i in range(start, end+1):*

*if count[chr(i)] > c:*

*c = count[chr(i)]*

*number = i*

*#print('Номер буквы: ', number-1072, 'Буква: ', chr(number))*

*if number-1072 < O:*

*number = number + 32*

*c = number - O*

*print('\nНомер буквы: ', number-1072, 'Буква: ', chr(number), 'Буква Ключа: ', chr(c), 'Разница: ', c-1072+1, '\n\n')*

*'''for i in range (0, len(b)):*

*for j in range (0, 31):*

*if b[i] == rus[j]:*

*new = new + rus[j - c]'''*

*return(c, new)*

*def full\_decode(meme, a):*

*check = 0*

*list\_code = ''*

*for i in range(0, len(text) - 1):*

*for value in range(start, end + 1):*

*if text[i] == chr(value):*

*if check == 17:*

*check = 0*

*c = value - meme[check]*

*if c < 1072:*

*h = c + 32*

*else:*

*h = c*

*#print ('First: ', value-1072, ' Key elem: ', meme[check], ' Second: ', h-1072)*

*list\_code = list\_code + chr(h)*

*check = check + 1*

*print (list\_code)*

*def decrypt():*

*key = ''*

*meme = []*

*a = 0*

*for i in range (2, 34): # Поиск длины ключа*

*a = search(i)*

*if a == i:*

*break # a = длина ключа (17)*

*for i in range(0, a): # Формирование групп*

*c, b = find\_key(i, a, 14)*

*key = key + chr(c)*

*meme.insert(i, c-1072)*

*print('Ключ: ', key)*

*print('\nМассив разниц: ', meme)*

*full\_decode(meme, a)*

*text = codecs.open("mem.txt", 'r', 'utf-8').read() # text = наш текст*

*#print(text)*

*decrypt()*

### Висновок:

Отже, в ході Практикума ми засвоїли методи частотного криптоаналізу,а також здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.