

Комп'ютерний практикум №2

Криптоаналіз шифру Віженера

Виконала Годлевська Аліса

Група ФБ-11

Варіант 11

Мета роботи

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

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.
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)

Хід роботи

Я обрала текст для шифрування про тости (toast.txt). Далі я його почистила від зайвих символів та пробілів (clear_toast.txt).

Обрала наступні ключі:

```
key_2 = 'ум'  
key_3 = 'боа'  
key_4 = 'пить'  
key_5 = 'гумус'  
key_15 = 'самоуничтожение'
```

Зашифровані тексти знаходяться у відповідних файлах (encrypted_2.txt для ключа довжини 2 і для інших відповідно так само).

Наприклад для $r=2$:

Далі я підрахувала індекси відповідності для шифротекстів:

І для VT:

r	Індекс відповідності шифротекстів
r = 2	3.9
r = 3	4.1
r = 4	3.6
r = 5	3.7
r = 15	3.4

Далі я розшифровувала свій текст по варіанту 11:

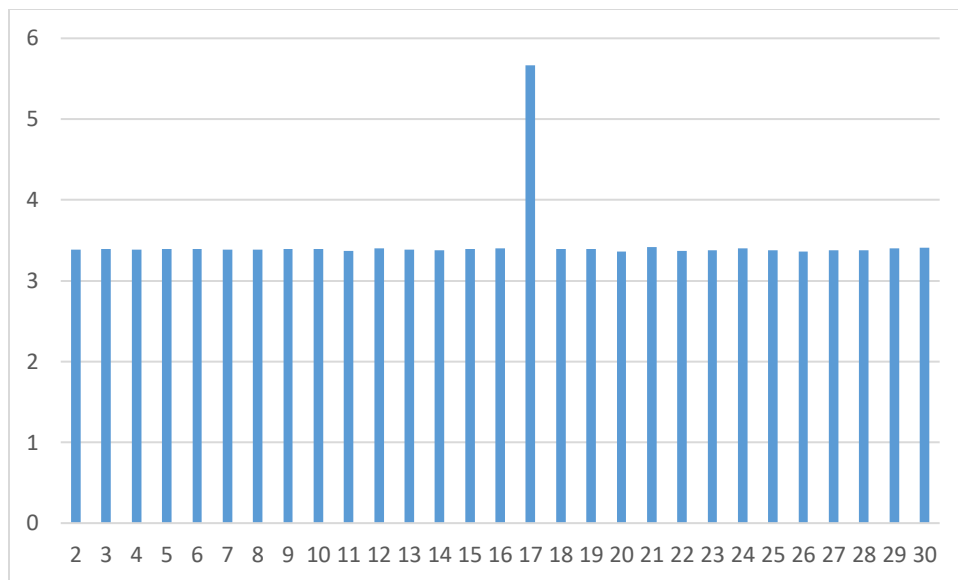
втяугроъцсхйиббъеумчтптикуочьякуфупчхлоюгжкйцтарсъшыауьнныфонингвциюфыови
лъсвнфтюлйдгашьицсывыилхтфчнфуэуърттцяцыпюраэпеябчнсюзещфпаъехехацидмырмрц
шсжчдующцсттйырчубовпкяхймнывкуйъыушэяъдфмтипъоыпюудмкнтйлдтукасмшън
нвзикзыдныкткшцпчыкнкпбдмычткчоыбзеэъехчрызпщъттыужупндзчртшънцжшыщврчэд
ихаяяълчмйфзвзрчнлятыыхицйсбцхпнфпдрмюашяыпалквмурйццнхъпъиъапчавтиъашышн
йэъкюптюрфызышыяцпщфтфочцмххцацвньщцаысцыщщпщикаомхркъуысдкцщуыснхпо
ншьожссуочдзнъяшдмуъчжвзаицбфюкъешешщшъвтчышиюыкуцкэпхивърешинхщлыноъ
оыгчроъхымтгбъчцбтжспкайцяущюпчщпчскпвчйсыхяомчнъшыяъкгпупижысянщцлпгтебуе
шежрнывынйяэозхфсалинийццзлхыдужвйчкчгдэярифшеыазнндчдфоуцькхшгфшжвинтгид
тъкъечшыущагпнънтйрбиъшхюкръалхепвщцхчысэюрстрхэиыбтъйявякъучнзюубиышй
люлзезцчкэивмшврхнюпзйушшугрвещцхсршжквгученьоозпучмуббздулсдлишдмюоъэснзо
уяхххачсцхсспчтнюбцпдицгыктхшщпрахпкпцецмъщъдъфуъуевцъалатыжъышфышсдлпыхц
йлийцокйъбъпгхзпцычрмюшщытгпцзэфнрюйыпушмътхэргэуорытлхтмфчтлфравтацбцыэб
ъчцбфждееяцикоюгкуччыжквксыибрбмялешяушввчйтымущйщчтеэснфутцбръясфщфэк
чрдубщтычрхйхцъжфкмцеациртйюплчмбянизмъефзаъгшхсщцяшзфнячжнвычкщесуаздкч
ызщшынюыццтбъкидкэбинмъцлуйнбуежацайтйущяушсыэъкджтысйзвпщърфыжутйпкыйгц
мащцнъжаузфумтгнмыщцнхпгчзбчтпйбищфшмчцькъщтшжшюпзнэшрюбсежрзюебирх
юшъчнчпзсйтньювъшплуочоптирхуеысяпщйхуянгрттзбжбщцгыкэапцикщзсчедсхдцеъп
чыоъяушгнтупщохочднбчувцгшщлщхптббзбзичшнрсрйкоышъмцфкщыицнтфъывэчсшбкъ
ъаязнавфуичжабиржыожцдхгщшсъбуезфхнтггхшпонтшчънщнефкфъивяцаэещеасушщй
авхгбкхзнядушагтусбэлспщфтцднспцтучвэщутдъаивпдчдкушмлтосжрагзфыпцоуаыхзцтдл
ццоттцицрджшпйлуствъшяпцкхыхйъккдаегкушужннгятлщкйчегрцнрцхиушъкхутужрйъа
яшосщбкйвфпцзвтхушцагщкхчтюэхыпыыщгрмъбшбйуефссдраонмытгнъхфузфепнвкаю
вкуйъыудучнрзбмиыцкмуахцйзтцыуиянчцлшеозюишяклттыукфншгэлывтяугропэшрюн
юпмцытгтцакшхшчнуайцзчюдвхедгшкйычфрцйушширрнхекдщгфйбриашъилхгжшиуъ
ежктыфжрвтгмихнбафджеоезщаъшщшсчпэхспучущмауэччыяфквудчушмапмбъчъбачцнн
ъкбждхэещйхуянгрийщйльнйцгнпючтеуяушгспсцръкюпхюпхццуаъщшыношчочбрхтмц
косыщйчыэцюпбыхжизпмкхышачугвэшнвгвнвшщыкхчсгрфэуоыкытпмъчшюуэвжичтлдтэ
емчхщъазроянздбнвыицтбюхюжшъешнръяншйаыптдунъбдшаъгшхсшхчййдеюфбцхыъсна
пэфцтурхэацмппшйфкцпъвкхнпицивгыншяжхыйстхггмьяфышкшбчътдтчюэкнытпхпачр
юубпацхтыютцицяцнкчнгннмынопщыжцяемкеъувррюзпхйнчфшшудчушцеюгжшчхпыух
ехацихарбкюскаэсгзлсеяъеэахдбэепфйупнодъсщцяикэчвыубпсдшщхюкэшэдбббхъекенчт
южцымыбешцрххчннмогехоъдфхъшкычизжтьеэлсчэъддмныбфжтипучмшщшзфкърдскэямд
зыукиюфыйдйныэъихшгъувхфэкътуоакъечуозйкрхъшцрнгжоохевъдлуахцпдэсрнцжтарй
ъецпциянйячрчышрдбажшгхлопаярымбытынгоушдеюгжузоывпдфуэалуигсщцуъобаенкъпдс
тыичцмхуубчррыццнхжъицйеъежръугнпыхмрпчбачтщчыждйщнрццфмучсетнънзилнвп
шепъуызфбщшъшоюгжрмхжруакоасющлыучцмшхэххфтнсхцрныэуушщущешзонгеысянтчо
ыафрцзчысдаъгшхсшъефбчнпюэчаяцынъоынзнапшиуиенщцышявъиртхылоъцнцлшгоч
ирисеаикфснцлшгчздпнякжпашщлыбтефсафухъзуыеслусрачъххнпцфийсскйхфкыттыц
цбкгшфшшдъкгртгрдкиямчишъыегмшрхйщтхгктыидъешлнраыноэмлнбфжюуаяжкщрдше
ъзшхъщбщеетуежияпэящцлпчлдартдшецоооилхбкшухчтвнвшщыкхъдыойыучнднаърн
пеадвпкоайдмахъняшябеаксокэфошучгхнбсужкчйтымаюгншйаыптдехныюиныхкччрыснзр

сьуфлоссокийсхвпщррыцъноушнмшгпжйжкебцхтыотццэчъдизжмдзъаьдлцфъжъувехны
юиньяъусбаэзыжбщубяаьнпэчъбзушмуьыхыврсгукиуешщнюсэдтукэмъуенцпурдшеъз
шыюшчочцпчтытцгсцыфдыюскщрцшушихосыщйчыэижвыхегцгыушшсфцфцартгтыгцмъян
цшэдбдарзоубдштипфуьбьнчрзпкгнцхщплчъуацийиттюзэяойкшятцсэттюююноаъзыкаа
ыдйпшлфеэсяфифыьанфуоаюэннърцкчэнзмябшнсьхпхекапоъзэйшшрдхйжяьшычцавчй
тыщтыщхцлпафынобшшнмиввяорыхуьынуярцхчтышъушафьгрцызыщтйэшзшшъсубкщт
ыщбтчкъешемчдеуунгмыцнцюшъонгвжтцвннмгктлшеччднпнкияачушъстдцшовкяидкоэ
щълчлфэрцпътрдъгытлцншфяаянеъыуояцхрншфяаяеуождрлххшйщесъегцкшуилоотшчъ
ыечтденпъдмбтфгчмдфчхипхкймиэсуцысуецуупкзърямцщтеькисуючдсчтвъхдуюптнзр
ыгечсаяуаюеъаяеуождрлхыктлелфцавмнтдяеюгчнтвышрцпътрдъгытлццпжунжвояуехия
нцтчумчюоаюрюуасюшиюъурхслййдшцлпцхрыцафцанесашитйашосъэчзехчйидкоэщъой
япхоеупужртоцышйойрущвцыжышиюнымьябыиддуэнийеющхыштюпйгреюушнсянццим
шзевфцмтцаелыццоцжакжжыанвыдэянцлшгчвродкзъниъошънюптнзрычшндйгешдчкфци
пурудьцнщхрфбьякыуаъыщтъяуфйьшянерчысйятывфиркелфжвзсшдъегшфчуафцаррйпд
тачтеесыхххцйнябззояхккйхкфсиржирйхерязъйфышфжкзчшзуасюшщчмшачтоттидкоэщъ
уйчкфрдфттэыкешщыдшшлфзыннпешярямццтеркзпнюсыщтнфшкчъыбцддкючтщопцыъ
енбсужафэешрлйюшъдыбскихкебыщлхашкчбсеиюцмцкеюгтхйобытырцяейдсмдрркняк
щрьымхрннсшхышвяузфнцкгзгывщцнтдпсштускъдяпяхийбеэжсхйэеидоачтмйщгчйыфцм
фдкиъямиыждорймепувыапцодччеэщшвэтидчофушуочыоныучйццфдйрмцфтеэфжвзсенъоу
щокчщюэюыптиоъдяпяхршшдзэыучидкоэрыцлпдббврдукъочяынцоапдзртцидеюьтццк
яькзртчйнтывыиыждошъкйнжыщмъоюоьфэрызйэшънсчщущчмшбдивпхшънрахжзлшюы
уюсдяпюттпятафьюювицошскжыввяорыепхслиыжчцсчяъпсчэошржоувцлхшсъталужуп
нлюеъярифъачцмеччйъпэяуъсфдчттрхаломушсчяохббззфуэугыоьцлцнкрбувротйюхоэяо
хдуббкмртюрорычтныуцмаэквхттчдятыапщущяппжхфъавлрнутнхнюпмцйеюаеилыюпырчу
фчвзтмцслрнпыхсцэппйатхжймъегътнбрждсудчыхнтъвртцбъуьроюндоэвонфкъбквкрыци
дкныцхошгэоикпюнгдоэдррнэюптнзрычцочпцхсшьеетеуешиыцькчцвэздтуягкцпэщых
шыюкждушфдкоэяьншшхфхгкчттцуепяойъцббхюфкъхюхаюгшзвпябуерзыхдъесъщцлшгпъ
юдецыхиъсщшймбънгвртздивыбшйуефжбстъдхъчяфмчцжхнъвиыжчцспрьгоэцйгкпхч
жыдъялынпеюуевцябгиннвыцигнйдтуршшгнтэшооьшапцйеябвхсъцфртхуьынуяицуьцн
цптхфчъкзтчйхерятусчшбрцпътрдъвишкчъыбкдоушуьцмюшчдчъшъегцкшуинвюгшшчч
жсуисуруьрттыктытакаящюнзъоэщишйсхфййучнхютупмнцлшгччырсырдмошвтхешгфрц
пътрдъерялйчфушяфешцюхыбмибкячрдуйцсхбтхчцмшкфрдкчедъегцнцюшелвирдюев
лопяжапдбтслтыунннйтпмцеъжкбрзтплцтмтхимшчпххгуреэмоэямгтхуьынуятйттытеъйц
ачжснкрудъегэлчмбянврсырдмошвтхешгфрцпътрдъерялйчшъеарсысшиштыцрфшдбнету
ючдуаьипучьшашъвхйрцхчтышъцшвяуохзнцзъаэщфчлызбйоушдфкаювхнныескгпуапцв
ыбтьошяэрджушццохыбпуйчкфрдфкруйойыкхапоэчыуфымшцлтютзлклфовкрыцирлнюб
нфшеарыжцязыхныяырцжбякбвтдкбцттюплчмбянизуюнгдоэцхицбшъуизжнчфакнэшсслбм
чдфсырдмошвтхешгаушннеютдкошцынпфчхдмехзззкхжиутивыпавзыбецуьцнпешкжкюч
ышпнбштсцгэючуяхццлтъчйьфыукяучпнинлйюшщушажебудхрюнсшщццпчбсажвмхчт
щяьбшбошесэынзшшнаицэтшмшфрущрцьуьруьсырнкхфйтоешбныгнюлгфдбнгпащфдшо
вяцфчпъачттуочюрсящчхчюаякясусфдшоцькхапоэчгзшучдоаяяцпчуоебмшхрюхаосхтьч
уюузрхрюхаъаючъэвзсокъдгнуфюкныпфпчфьпнидйбияхоътсезпкфтцжмышмчудчттрх
ъуешоедмиъыэплюфкщтычрнуоыаьбыуаеешбнркааштчуцэцерййкщцдайэосмыънерстхбин

дцхцычшвлрзитыызъспьоцшьдчвлэаигытлццяцэхыбзйтчодгтяышбарысттфжрзъсикйы
юптнзрычгыпыаылошуеъзжайтывнвнуйсусфдтдспыкыхгшфчнюжспкамгитйэпхиэяфтир
чычыюяяэпцкшбцдгцязыхныфшшолшьпцнестдштнбттимуыззхнцзтаудшшчмузкшрцитц
штнюшксъдотцмушкгрбшснцъхбснвзтмфживссоцфрапзслчхтццвтгэйсудбзцжушидшкэм
иыжафртйдччдяецвехжъбапжэчйсдоныюшкушаекартгушчрнуоилеъукипеэшьы

Для цього я підрахувала значення періоду за допомогою індексу відповідності. Розбила текст на блоки і обчислила сукупне значення індексів відповідності для кожного блоку.

r	index
2	0.03385469736120976
3	0.0338903572127828
4	0.03382856631255099
5	0.0339485646135541
6	0.03393201950461585
7	0.03388787967284901
8	0.03387028521782783
9	0.033925669332816634
10	0.03389699079863339
11	0.03369705663706742
12	0.03402936176339339
13	0.033824971570802616
14	0.03374056874966326
15	0.03389000107283445
16	0.0340028030190302
17	0.05665287154668847
18	0.033914675695348
19	0.033895156796394856
20	0.033573302104999446
21	0.034174812268371026
22	0.03365396493285553
23	0.03378321793484534
24	0.034037676161075336
25	0.03379278482726759
26	0.03363761881728569
27	0.03379104130707299
28	0.03375970008060539
29	0.03399770139487164
30	0.03408868605919015



Звідси маю, що період = 17.

Маючи всю цю інформацію обчислила ключ. Отримала:

венецианскийкужъц

А якщо ще трошки подумати, то ключ буде «венецианскийкупец».

Розшифрувала текст, помістила також у файл 11var_decrypted.txt:

антонионезнаюотчегоятакпечаленмнеэтовтягостьвамяслышутоженогдеягрустьпоймалнаш
елильдобылчтосоставляетчтородитеехотелбызнатьбессмысленнаягрустьмоявиноучтосамо
госебязнатьмнетрудносалариновыдухоммечетесьпоокеанугдевашивеличавыесудакакбога
теиивельможиводилъпышнаяпроцессияморскаяспрезреньемсмотрятнаторговцевмелкихчто
кланяютсянизкоимспочтеньемкогдаонилетятнатканыхкрыльяхсаланиповерьтееслибтакр
исковалпочтивсечувствабылибтаммоисмоейнадеждойбыпостоянносрывалтравучтобзнать
откудаветерискалнакартахгаваниибухтылюбойпредметчтомогбынеудачумнепредвещатьме
нябынесомненновгрустьповергалсалариностудямойсупдыханьемявлихорадкебыдрожалот
мысличтоможетвмореураганнаделатьнемогбывидетьчасовпесочныхневспомнившиомеля
хиорифахпредставилбыкорабльвпескезавязшимглавусклонившимнижечембокачтобцелова
тьсвоемогиувцерквисмотрянакамнизданиясвятогокакмогбыяневспомнитьскалопасныхчт
охрупкиймойкорабльедватолкнуввсепряностирассыпалибывводуиволныоблеклибвмоишел
канусловомчтомоебогатствосталоничемимоглибьяобэтомдуматьнедумаяпритомчтоеслибта
кслучилосьмнепришлосьбызагруститьнеговоритезнаюаянтониогруститтревожасьзасвоеито
варыантонионетверьтемнеблагодарюсудьбумойрискнеодномуявверилсуднунеодномуимес
тусостояньемоенмеритсятекущимгодомянегрущуиззамоихтоваровсаларинотогдавызначи
твлюбленыантониопустоесалариноневлюбленытакскажемвыпечальнызатемчтовыневесел
битолькомоглибсмеятьсявытвердявеселзатемчтонегрущуудвумичныйянусклянусьтобойро

дитприродастранныхлюдейодниглазеютихохочуткакпопугайуслышавшийволынкудругие
женавидкаккусускислытакчтовулыбкезубынепокажутклянисьсамнесторчтозабавнашуткав
ходятбассаниолоренцоиграцианосаланиовотблагородныйродичвашбассаниограцианоилор
енцоснимпрощайтемывлучшемобществеоставимвассалариноосталсябячтобвасразвеселить
новотявижутехктовамдорожеантониовмоихглазахценавамдорогасдаетсямнечтовасделазов
утирадывыпредлогуудалитьсясалариноприветвамгосподабассаниосиньорынокогдажмыпос
меемсякогдавычтоотсталинелюдимысаларинодосугвашмыделитьготовысвамисалариноиса
ланиоуходятлоренцокбассаниосиньорразвыантонионашлимывасоставимнопрошукобедуне
позабытыгдемыдолжнысойтисьбассаниопридунавернограцианосиньорантониовидуваспло
хойпечетесьслишкомвыоблагахмирактоихтрудомчрезмернымпокупаеттерятьихкакизмени
лисьвыантониоамирсчитаючемонестыграцианомирсценагдеувсякогоестьрольмоягрустнагр
ацианомнеждайтерольшутапускайотсмехабудувесьвморщинахпустьлучшепеченьотвинаго
ритчемстынетсердцеоттяжелыххвздоховзачемжечеловекустеплойкровьюсидетьподобномра
морномупредкупатьнавяуилихворатьжелтухойотраздраженьяслушайкаантониотебялюбл
юговоритвомнелюбовьестьлюдиукоторыхлицапокрытыпленкойточногладьболотаонихра
нятнарочнонеподвижностьчтобобщаямолваимприписаласерьезностьмудростииглубокийу
мисловноговорятнамьяоракулкогдавещаюпустыипеснелаетомойантониознаятакихчтомудр
ымысливутьлишьпотомучтониичегонеговоряттогдакакзаговоривонитерзалибушитемктоихсл
ышаближнихдуракаминазвалбывернодаобэтомпоследенонеловитынаприманкугруститакуюс
лавужалкуюрыбешкупойдемлоренцонупокапрощайапроповедьякончупообедавлоренцоита
квасоставляемдообедапридетсямнебытьмудрецомтакимбезмолвнымговоритьнедастграциа
нограцианодапоживисомногодадвазвукголосатысвоегозабудешьянтонионудлятебястан
уболтуномграцианоотличноведьмолчаньехорошовкопченыхязыкахдавчистыхдевахграциа
ноилоренцоуходятантониогдесмыслвегословахбассаниограцианоговоритбесконечного
пустяковбольшечемктолибоввенецииегорассужденияэтодвазернапшеницыспрятанныевду
хмерахмякинычтобыихнайтинадискатьвесьденьанайдешьувидишьчтоиискатьнестоилове
нецияулицавходитланчелотланчелотконечносовестьмояпозволитмнесбежатьотэтогожидам
оегохозяинабесменятаквотитолкаеттаквотиискушаетговоритгобболанчелотгоббодобрыйла
нчелотилидобрыйгоббоилидобрыйланчелотгоббопустиногивходбегивовсеяжкиеудирайот
сюдаасовестьговоритнетпостоячестныйланчелотпостоячестныйгоббоиликаквышесказано
честнейшийланчелотгоббонеудирайтопниногойнаэтимыслиладноахрабрыйдьяволвелитмне
складыватьпожиткивпутиговоритбесмаршговоритбесрадибогасоберисьсдухомговоритбеси
лупиладноасовестьмоявешаетсянашеюкмоемусердцуимудроговоритмойчестныйдругланче
лотведьтысынчестногоотцаилискореесынчестнойматерипотомучтосказатьправдуотецтомо
йнесколькокакбыэтовыразитьсяяотдавалчемтобылунегоэтакыйпривкусладносовестьмнегов
оритланчелотнешевелисьпошевеливайсяговоритбесниместаговоритсовестьсовестьговорю
правильнотысоветуешьеслиповиноватьсясовестинадомнеостатьсяяужидамоегохозяинааонт
опростименягосподисамвродедьяволаачтобыудратьотжидапридетсяповиноватьсяялукавому
аведьонтосвашегопозволенияиестьсамдьяволитоправдачтожидвоплощенныйдьяволипосов
естиговорясовестьмояжестокосерднаясовестьеслионамнесоветуетостатьсяяужидабесмнедае
тболеедружескийсоветятакиудерудьяволмоипяткиктвоимуслугамудерувходитстарыйгоббо
скорзинкойгоббомолодойсиньорскажитепожалуйстактутпройтисиньоружидуланчелотв
сторонуонебодаэтомоединородныйотецонслептаксловноемунеточтопескомакрупнымграв

и емглазасыпалонеузнаетменясыграюснимкакуюнибудыштукугоббопочтеннейшиймолодойсиньорсделайтемилостькакмнепротиксиньоружидуланчелотаповернитенаправоприпервомповоротеноприсамомпервомповоротеповернитеналеводасмотритепринастоящемтоповоротенеповорачивайтенинаправониналевоаворочайтепрямохотькождомужидагоббосвятыеугодникитруднобудетпопастьнанастоящуюдорогувынеможете сказатьмнекекийланчелотчтооунегоживетживетунегоилинетланчелотвыговоритеомолодомсиньореланчелотевсторонувотпогодитекакаясейчасисторияразведустарикувывговоритеомолодомсиньореланчелотегоббокакойтамсиньорвашамилостьсынбедногочеловекаотецегохотьэтоясамговорючестныйнооченьбедныйчеловекхотяблагодарябогаздоровыйланчелотнуктобытамнибылегоотецмыговоримомолодомсиньореланчелотегоббоознакомывашеймилостипростоланчелотесударьланчелотногоббоаланчелотеспозволениявашеймилостиланчелотследственноосиньореланчелотеговоритеосиньореланчелотebaтющкамойибоэтотмолодойсиньорсогласноволесудебирок аивсякихтакихученыхвещейвродетрехсестерпарокипрочихотраслейнаукидействительноскончалсяилиеслиможновыразитьсяпрощеотошелвлучшиймиргоббогосподиупасидаведьмалычуганбылистиннымпосохоммоейстаростиистинноймоейподпоройланчелотнеужтожапохожнапалкуилинабалкунапосохилинаподпоркувыменянеузнаетебатющкагоббоохнетяваснезнаюмолодойсиньорнопрошувасскажитемнеправдучтомоймальчикупокойгосподьегодушуживилипомерланчелотнеужтовынеузнаетеменябатющкагоббоохгореведьпочтичтоослепнепризнаювасланчелотнупо правдедажебудьувасглазавпорядкевыитомоглибынеузнатьменяументототецчтоузнаетсобственногоробенкаладностарикывамвсерасскажупровашегосынастановитсянаколениблагословименяправдадолжнавыйтинасветубийствадолгоскрыватьнельзякточейсынэтоскрытьможновконцеконцовправдавыидетнаружу

Висновки

В ході цього комп'ютерного практикуму я експериментально дослідила те, як працює шифр Віженера. Можу сказати, що для шифрування краще використовувати ключі із більшим періодом. Та і взагалі зламати такий шифр доволі просто, тому краще не користуватись їм для чогось важливого.