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

ЛАБОРАТОРНА РОБОТА №2

з дисципліни «Криптографія»

**«Криптоаналіз шифру Віженера»**

Виконали: студенти 3 курсу ФТІ

групи ФБ-82

Ясинський Нікіта
Владислав Кравчук

Перевірив: Чорний О.

Київ – 2020

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

Індекс відповідності відкритого тексту: 0.05843316543575007

| Обрані ключі для шифрування | Індекс відповідності шифротексту |
|---|---|
| як | 0.04116117005238454 |
| сыр | 0.03847141338327302 |
| река | 0.037545766643707554 |
| лента | 0.036528542722358996 |
| стихотворец | 0.03462813579817841 |
| электроинструмент | 0.03474770573473299 |

Індекс відповідності шифротексту**: 0.05613455826544599**
Індекси відповідності для блоків заданої довжини заданого шифротексту:

| Длинна ключа | Индекс |
|---|---|
| 2 | 0.03390017274729224 |
| 3 | 0.03338138666490387 |
| 4 | 0.03343916061266839 |
| 5 | 0.032612329263756595 |
| 6 | 0.0337811652697796 |
| 7 | 0.03302957855468164 |
| 8 | 0.03314390799053376 |
| 9 | 0.034437035625833494 |
| 10 | 0.03341249422785143 |
| 11 | 0.0335729912036826 1 |
| 12 | 0.03264814212978008 |
| 13 | 0.0328267767254336 |
| 14 | 0.032673404402602794 |
| 15 | 0.03202500132422269 |
| 16 | 0.03238666473960593 |
| 17 | 0.06258666473960593 |
| 18 | 0.03497557189169444 |
| 19 | 0.033024738717542156 |
| 20 | 0.033072203869749885 |
| 21 | 0.03339902499740689 |
| 22 | 0.031531531531531536 |
| 23 | 0.03249888020703728 |
| 24 | 0.03418710657694812 |
| 25 | 0.0323017978190392 |
| 26 | 0.030916334661354575 |
| 27 | 0.033332190254106504 |
| 28 | 0.032558827882196224 |
| 29 | 0.034563492063492 |

Можемо зробити висновок, що довжина ключа - **17 символів**

Після того, як ми визначили період (який дорівню 17), подальше робота звелася до серії розшифрувань шифрів Цезаря, де кожне окреме $Y_i$ – зашифрований шифром цезаря з ключем $k_i$, який ми шукаємо за формулою:

$$k = (y^* - x^*) mod(m)$$

Ключ: **венецианскийкупец**

## Шифротекст:

йтпоухшхшжкумьпышжаяэояниищюсжфятцхйгечолецйьюджбдьтэхнэокоыытпйцшфтвцфтркктдмоцрхтввой
тпоухшоапкйдгютыерюэмфчалщхиэьшгоаошырхичфтьтупаюдтщюркаюкюжьчышхзцфтйоонзбркктпгэюшнн
жьшщюлячыпябтщюркаюфедтыюкюжтпйцшоымцпчзорйыжафхюгюнтщюйоуыйхжйуюаюмюмосххэусуыая
куьбаюмьпыаяаяхюыюшефгпйрчэчшжюсфяфтрюжтуюфхкйгещюатркктпгэюшнфтоннтнжьшсжщьыпьшыцб
отсфяфтрюииоешекхшжкуленжеоондтзяюхжешелшжштфэчзмкынштдтгтютфмйхчгайыеютйомоыявеютаюык
текйщлхюшегсрхжмрфафдпьтмеякыюшенюокгмчидтщьрюухюопогюдйрчмтрчэощехетчжйсхнэйтпоуховдгт
егсдтцгяитеихапйелтоеаюефчыэчюжппьтджэбокоыццфтншйозтяоньежкетчжйсхшжеьчыииинтфтьтщйьмос
гыйхшжкуаяаяйозтяоньежкетчжйсхйхутэхеьчыииинтфтьтртеоглншиежтлцуыэчрямьфяфлзкшлпчтвкоктлоы
емойжучпекйщьщхдтджвепйыфхюншвофтчтообхядэйжтпхэчядоыйлугпхлетчжйсхядмооецейойтпоухшхьч
ыиииннпоцяиэгокотентиеэоэсююйоцчэчажлиппэййхлкзчмооецейодтйтпоухейкйфтррядяигсдтгтяиоотцэйпобх
нэчтясрхщхевпйьмосйхдбхзгелтщфйхэчвжппьтджэбокоышхцшафаюдмиэгсажюсфяфтрюужаяяогюкхцшйлй
ждмевгентмсохлшвйонсжбтбхцшйлйжнтмсэчшжяпнжьшмцфтиэеоктиеухэйкйфтжыэчфтвцфтркпоуешнютфт
цгсжмишжбттеютщгьюшееоинсецпнжьшмцфтщювжгсуыбттеютьмшжкыкымцреыфгсвйжтовиеухрхафаюгх
жоокоыжзкюйозтщыппйеэжхсфяфтрюкпнжьшмцфтюхпчхсуыоцфтюхрхжйьшйобхдпчыиилкмыпыхсовджфе
щоондтютпоухьсьбпйсэатэюяхиэьтджэчнэюхмьпыцпчыиилкйоютфтцгсжмихйкюэыжыцпьтщышжфчшжфьч
ышхядйтонзолцхйшночаоэхюоло доджыюммясвжнжркдшгыыцнчджфещопозпнжьшмцфтммяслкшчюржйрчо
сичгыэйччэюктьячыоцжйрчщхбттеютпоухххэтюэгсншххлепьеллкркшедмоцрхппыццшнчэоесподжкешгпгош
теокленычцажуыпчзмйллегтмодпшжзегыктуюыкютфтцгсжбттеусэчпорчзмжырхрюпйрчщхдтупнжаожхкйге
йтондтяечдеозыльрриэйтонугттеусэчпорчзмжыажтвловхтвкоктлоколятвютьмхьдтджрхоселзкщющьпоюцщ
хшоютьмхьдтджэйыцнчджфеюееоыжуышхкйгентфтвклеьпежфчсопцуыэчряжтммцшшйьмосйхдбюхгга тэый
жжтлбшефтмччцдтлцуыэччцжйнтыижшйждтмчаооочяшчнюзтупгмжтркс хтвотфшапнжаожхкйгеютщоашн
фтмоджфянжзмжопумьподтаооодтэгннйжибажнжьюалхьелажммеяншшжгмрхмхпяхсьбфтгтсжщьюоцгютно
ктыюшецпнжгмшейтондтцшжйфтшоцгеоаюйжибпоюцряафхюйтондтцшжйфтютьмюжкыцпшщуыядьмхьщх
фяйолойепцфтркьйкышховрещецгжмоврерогтйорккткюмясджйпьшыцбогтйтшерхоселхюющюпоюцщхшопч
ямфлщхшочтфгпйрчдбтжэчаочбгюзшшжижаощогтрехябгщочюяжыфгсфяфтрюцымхшжкумьпыцпчыиилкщо
вцфтюхлщуыэчгывещосымьщьрглолбкцфтэолцхйдмтвеощояошеэгкодйииоерчтмяююйэгиюкжряаежтьнмосх
тмкьонэолнймпчщхютьтхяэчцпкыйыччлтьтзоиннтдязмщьыцтошояошеютьтхяюзгейодмцшцхдткоаошсыюь
юнютегюкххьчыщулеймомоинзошгеорчнжыючхтвжтеодмрхншшжфьчышхэбсжйлхььсуыгыэйюхофрюэеймяа
рхгяаяркюхэйзтьмуырххйаюшгяжщдогпхшжкуохоцыфюхапаогпйетеэюфояошеркйоркктвжиэмечдонютьюн
юкпажмбщофыщхпяаффячмрхтвнтлыйжыепчэоопгсьтжхкйщошляитедмясменюбхнэатщжзмьшчтаыфсшжпя
нжзмюочтджичьбктмюфбгелеюжьущхшоцыптумщлщднежццшджьтяоэйктцхворкшевжцпрюфеающоцгщоре
щоонйохьпысьбфякгпюуриэеоктгюжьыпгмщхкйкыймяайтпоухейжтовчдчезттсыцгмшояошеркюхйоухгысж
жоцгджпеаюыкибуекгаыювйтпоухшхшжкувесжбтбхапйлгывощодоыкибацфтркщсуышжбоупчызицояошерк
юхйоухгысжжояошеюхйхапдпрюфеюйптбхапйлгывощодоыкибуеютлоыющоиилфрютечгажжшщсуысоияюх
жешелшюояошеркюхйоншуыжтршйлдтджцмхйлячифчшжяпгсьтжхкйгенжьшгюзшйжпчбожауыпочхапюхж
ыйюфмяиютфбшецгжмэчюруымцзодпаоеошегьчыиииинсжщььсуыгылфрюэефбелуымьштщюйозтщыьедтесхй
чтйешнибрьчышхтвщюкюзоыишжыцфтюхйхшчютзхжйщьчдхюйждмясменютетсфяфтрючсаятентесйхшчдиа
тьтлоьуьфэчзмкымтщюмюатнюатыиеьфчэбучжогтаоелуыажххьусьуейщгчюшнибатщжзмьейожтммцштпйе
теэюшнпогюдйрчэчясшхуызинуюжажжзгеьяафхююжхьйшйлйжщсуышжейтпйоашюхдбгтжтйеаюймяархюе
йпьтяидгзотеюзфтгтйоютфбсхафюхясьбйоэтэхтвоыэчмтщющлщхбэгскыеьчыщужоюжьущхшосжщььсуыгых
йюхфояошеркоховйоркктрюатдждтгтчтухйхдбфтгтсжбтщюйорюшсшчгыхйижйедтуегоцчжоммцшссьбфтгтс

жщьсьежшхлфнжэчлеьпчыфбшнтжыцдтджпчэодмясменютессфяфтрюоцфтюхшжапгмшхжймесхыцхсьбфтгтсжщьххапьтнгджажщцхйфчнтфтвкщхосгсичшжхшгыэчаоэхюомечдшеяицтктфтдязмщьыцыеехюяонюзтнхшжкурянжзмэблтебтфэчзмкызцфттегюыеуырятмджыюйонкпоьющолесжэчэовжафщгютджвеоврктрюатдждтфееошнсжгсьбйоясуыгыажаядхафдпйлгмрчэчйхевсжжонхосщьпыэчяилоджлкчцхйыпйетеэюшнпогюдйрчьехюяооврюатдждтрктфтсжбтщюдмщххьаошююеьпчыйотецшдмясменюбхафьшафаюютгююкыюшнсжбтщюйолойерчпокотелейоатьтиеюйжтовиеухйдатщжзмииоеюяфлзктсщхэрфпгынгонбйзтьмуыьимярхэтпмнрэбгхншйхдбщювокьажжошеитсггеуййонхмишжфяафхююхнклтоежчжмрфядндтдхшжрфрюэефбютьпьудтнклтоеаюмютехеюхдмрхншэбэояниилкмчхсцпфязцпчэбмюпгвцпчафчыэчтвгтжтйеецфтлтебшоджытуюфхкйшнюхщюеойжибщюеощйрчшовжафдпкйпоэхыфчырятмджыюоцфтщюатысшжкеютсшнжаошнсжщьчыииинйтонзокмичджлобхэбдтймяархшйкюрюшйейумежжзфтчпкйдгютнтюйхьюенжатщжзмиччтнкыюаюцшнчкгэгцтктфтяепйгяеврюайьйютнтщхлкэю

## Расшифрованный текст:

антонионезнаюотчегоятакпечаленмнеэтовтягостьвамяслышуутоженогдеягрустьпоймалнашелильдобылчтосоставляетчтородитеехотелбызнатьбессмысленнаягрустьмоявиноючтосамогосебяузнатьмнетрудносалариновыдухоммечетесьпоокеанугдевашивеличавыесудакакбогатеиивельможиводильпышнаяпроцессияморскаяспрезреньемсмотрятнаторговцевмелкихчтокланяютсянизкоимспочтеньемкогдаонилетятнатканыхкрыльяхсаланиоповерьтееслибятакрисковалпочтивсечувствабылибтаммоисмоейнадеждойябыпостоянносрывалтраву чтобзнатьоткудаветерискалнакартахгаваниибухтылюбойпредметчтомогбынеудачумнепредвещатьменябынесомненновгрустьповергалсаларинострудямойсудпдыханьемявлихорадкебыдрожалотмысличчтоможетвмореураганнаделатьнемогбывидетьячасовпесочныхневспомнившиомеляхиорифахпредставилбыкорабльвпескезавязшимглавусклонившимнижечембокачтобцеловатьсвоюомогилувцерквисмотрянакамнизданиясвятогокакмогбыяневспомнитьскалопасныхчтохрупкиймойкорабльедватолкнуввсепряностирассыпалибывводуиволныоблеклибвмоишелканусловомчтомоебогатствосталоничемимоглибяобэтомдуматьнедумаяпритомчтоеслибтакслучилосьмнепришлосьбызагруститьнеговоритезнаюяантониогруститтревожасьзасвоитоварыантонионетверьтемнеблагодарюсудьбумойрискнеодномуявверилсуднунеодномуименстусостояньемоенеменеритсятекущимгодомянегрущуиззамоихтоваровсаларинотогдавызначитвлюбленыантониопустоесалариноневлюбленытакскажемвыпечальныязатемчтовыневеселыиткомоглибсмеятьсявытвердяявеселзатемчтонегрущудвуличныйянусклянусьтобойродитприродастранныхлюдейоднихглазеютихохочуткакпопугайуслышавшийволынкудругиеженавидкакукусскислытакчтовулыбкезубынепокажуткляниьсамнесторчтозабавнашуткавходятбассаниолоренцоиграционосалаиовотблагородныйродичвашбассаниограционоилоренцоснимпрощайтемывлучшемобществеоставимвассалариноостался бячтобвасразвеселитьновотвижутехктовамдорожеантониовмоихглазахценавамдорогасдаетсямнечтовасделазовутирадывыпредлогуудалитьсясалариноприветвамгосподабассаниосиньорынокогдажмыпосмеемсякогдавычтототсталинелюдимысаларинодосугвашмыделитьготовысвамисаларионисаланиоуходятлоренцокбассаниосиньорразвыантонионашлимывасоставимнопрошукобедунепозабытьгдемыдолжнысойтисьбассаниопридунаверноограционосиньорантониовидувасплохойпечетесьслишкомвыоблагахмиракгоихтрудомчрезмернымпокупаеттеряетихкакизменилисьвыантониямирсчитаючемонестьграциономирсценагдеувсякогоестьрольмоягрустнаграциономнеждайтерольшутапускайотсмехабудувесьвморщинахпустьлучшепеченьотвинагоритчемстынетсердцеоттяжелыхвздоховзачемжечеловекустеплойкровьюсидетьподобномраморномупредкуспатьнаявуилихворатьжелтуюхойотраздраженьяслушайкаантониотебялюблюяговоритвомнелюбовьесть людиукоторыхлицапокрытыпленкойточногладьболотаонихраняятнарочнонеподвижностьчтобобщаямолваимприписаласерьезностьмудростьиглубокийумисловногоговорятнамяоракулкогдавещаюпустьипеснелаетомойантониознаютакихчтомудрымислывутлишьпотомучтоничегонеговорятоттогдаказаговоривонитерзалибушитемктоихслышаближнихдуракаминазвалбывернодаобэтомпосленонеловитынаприманкугруститакуюславужалкуюрыбешкупойдемлоренцонупокапрощайапроповедьякончупообедавлоренцоитаквасоставляемдообедапридетсямнебытьмудрецомтакимбезмолвнымговоритьнедастграционограционодапоживисомноюгодадвазвукголосатысвоегозабудешьантонионудлятебяястануболтуномграционоотличноведьмолчаньехорошовкопчеными языкахдавчистыхдевахграционоилоренцоуходятантониогдесмыслвегослова хбассаниограционоговоритбесконечномногопустяковбольшечемктолибоввенецииегорассуждениятодвазернапшеницыспрятанныевдвухмерахмякиныч тобыихнайтинадоискатьвесьденьанайдешьувидишьчтоиискать нестоиловенецияулицавходитланчелотланчелотконечносовестьмояпозволитмнесбежатьотэтогожидамоегохозяинабесменятаквотитолкаеттаквотиискушаеттоворитгобболанчелотгоббодобрыйланчелотилидобрыйгоббоилидобрыйланчелотгоббопустиногивходбегивовсетяжкиеудирайотсюдаасовестьговоритнетпостойчестныйланчелотпостойчестныйгоббоиликаквышесказаночестнейшийланчелотгоббонеудирайтопниногойнаэтимыслиладноахрабрыйдьяволвелитмнескладывать пожиткивпуть говоритбесмаршговоритбесрадибогасоберисьсдухомговоритбесилупиладноасовестьмоявешаетсянашеюкмоемусердцуимудроговоритмойчестныйдругланчелотведьтысынчестногоотцаилискореесынчестнойматерипото мучтосказатьправдуотецтомойнесколькокакбыэтовыразитьсяотдавалчемтобылунегоэтакийпривкусладносовестьмнеговоритланчелотнешевелисьпошевеливайсяговоритбеснисместаговоритсовестьсовесть говорюправильнотысоветуешьеслиповиноватьсясовестинадомнеостатьсяужидамоегохозяинааонтопростименягосподисамв

родедьяволаачтобыудратьотжидапридетсяповиноватьсялукавомуведьонтосвашегопозволенияиестьсамдьяв олитоправдачтожидвоплощенныйдьяволипосовестиговорясовестьмояжестокосерднаясовестьеслионамнесов етуетостатьсяужидабесмнедаетболеедружескийсоветятакиудерудьяволмоипятктвоимуслугамудерувходит старыйгоббоскорзинкойгоббомолодойсиньорскажитепожалуйстакактутпройтиксиньоружидуланчелотвсторо нуонебодаэтомойединородныйотецонслептакословноемунеточтопескомакрупнымгравиемглазазасыпалонеузн аетменясыграюснимкакуюнибудьштукугоббопочтеннейшиймолодойсиньорсделайтемилостькакмнепройтик синьоружидуланчелотаповернитенаправоприпервомповоротеноприсамомпервомповоротеповернитеналевод асмотритепринастоящемтоповоротенеповорачивайтенинаправониналевоаворочайтепрямехонькокдомужидаг оббосвятыеугодникитрудноbудетпопастьнанастоящуюдорогувынеможетесказатьмненекийланчелотчтоунего живетживетунегоилинетланчелотвыговоритеомолодомсиньореланчелотевсторонувотпогодитекакуюясейчас историюразведустарикувыговоритеомолодомсиньореланчелотегоббокакойтамсиньорвашамилостьсынбедног очеловекаотецегохотьэтоясамговорючестныйнооченьбедныйчеловекхотяблагодарябогаздоровыйланчелотну ктобытамнибылегоотецмыговоримомолодомсиньореланчелотегоббоознакомомвашеймилостипростоланчело тесударьланчелотнопрошувасстариктобишьумоляювасследственновыговоритеомолодомсиньореланчелотего ббооланчелотеспозволениявашеймилостиланчелотследственноосиньореланчелотенеговоритеосиньореланче лотебатюшкамойибоэтотмолодойсиньорсогласноволесудебирокаивсякихтаких учены хвещейвродетрехсестер парокипрочихотраслейнаукидействительноскончалсяилиеслиможновыразитьсяпрощеотошелвлучшиймирго ббогосподиупасидаведьмальчуганбылистинным посохоммоейстаростиистинноймоейподпоройланчелотнеуж тожяпохожнапалкуилинабалкунапосохилинаподпоркувыменянеузнаетебатюшкагоббоохнетяваснезнаюмоло дойсиньорнопрошувасскажитемнеправдучтомоймальчикупокойгосподьегодушуживилипомерланчелотнеуж товынеузнаетеменябатюшкагоббоохгореяведьпочтичтоослепнепризнаювасланчелотнупоправдедажебудьува сглазавпорядкевыитомоглибынеузнатьменяументототецчтоузнаетсобственногоребенкаладностарикявамвсер асскажупровашегосынастановитсянаколениблагословименяправдадолжнавыйтинасветубийствадолгоскрыва тьнельзякточейсынэтоскрытьможноновконцеконцовправдавыйдетнаружу

**Висновок:** Під час цього лабораторного практикуму ми розглянули та реалізували один із методів частотного криптоаналізу. Також ми здобули навички аналізу потокових шифрів гамування адитивного типу та роботи з ними на прикладі шифру Віженера. На практиці ми програмно зашифрували текст шифром Віженера(використовуючи ключи різної довжини), а також розшифрували текст, знайшовши індекс відповідності для блоку довжини 17, що був найбільш близький то теоретичного значення.