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

# ЛАБОРАТОРНА РОБОТА No2

**з дисципліни «Криптографія»**

**«Криптоаналіз шифру Віженера»**

Виконав:

студенти 4 курсу ФТІ

групи ФБ-72 та ФБ-73

Синицін Максим

Морозов Артур

Перевірили:

Чорний О.

Київ – 2020

*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.

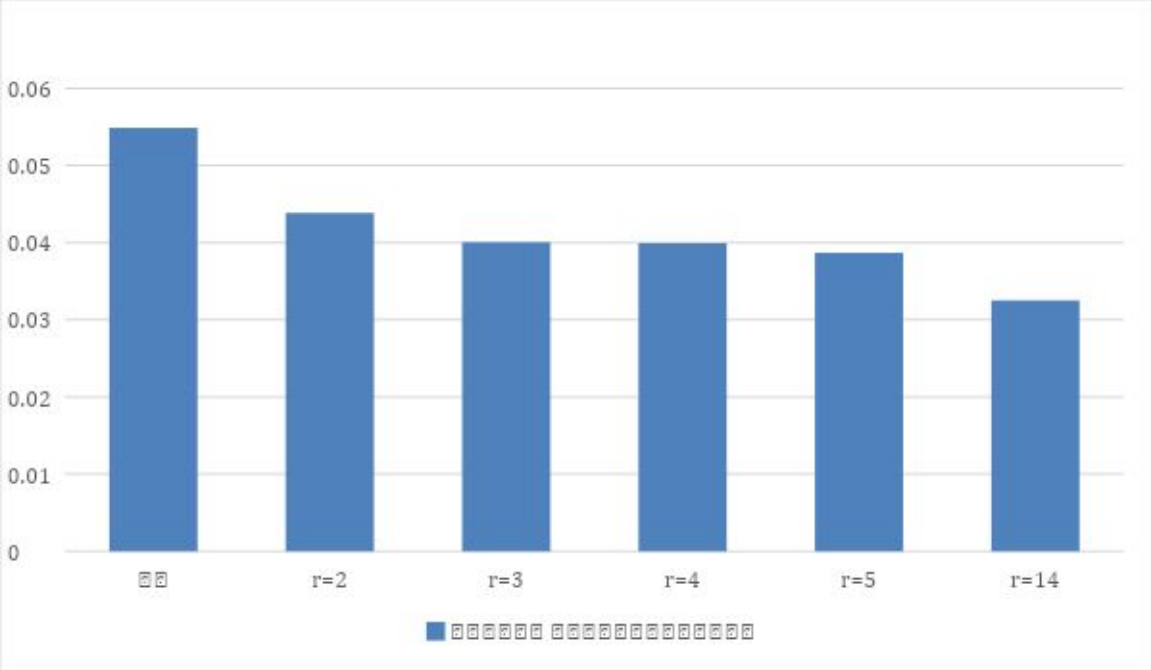
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

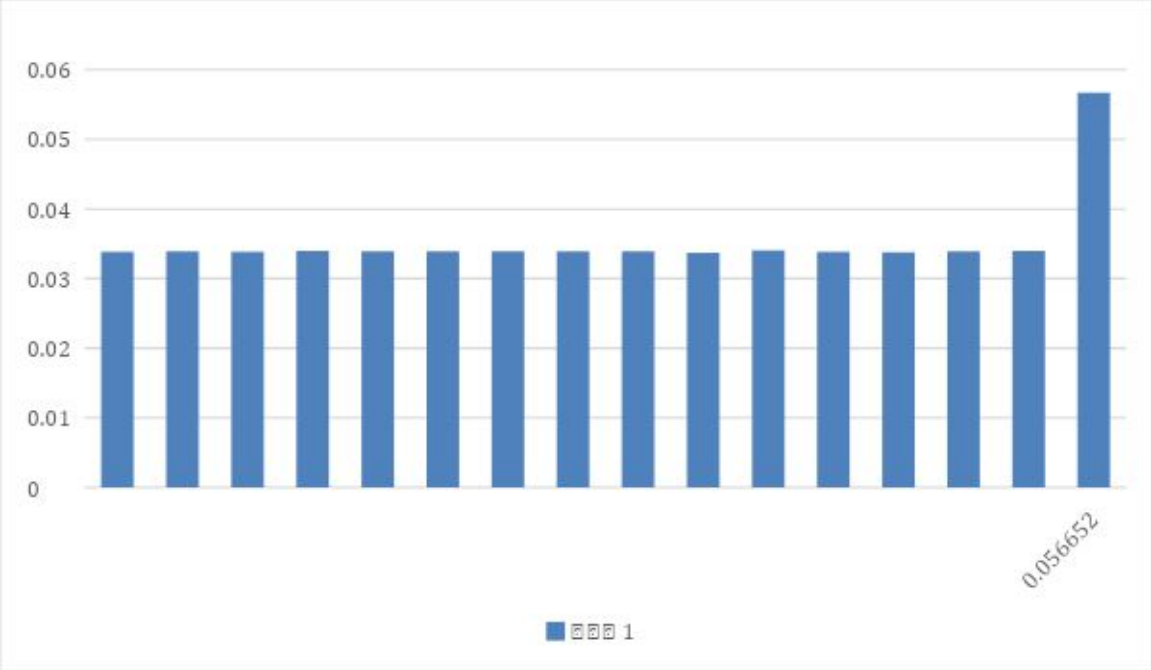
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

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

Шифрування:

| Відкритий текст | - | 0.0548717948717948 7 |
|---|---|---|
| ад | 2 | 0.04383500557413600 |
| лом | 3 | 0.0400222965440356 7 |
| сало | 4 | 0.0399331103678929 7 |
| плохо | 5 | 0.03868450390189520 |
| електростанция | 14 | 0.0324860646599777 0 |




```
Значение: 0.056652871546688466 самое близкое к теоретическому значению 0.0555737474
```

Ключ: венецианскийку**жь**ц

Для блоку 15 та 16 літера “о” не найчастіша тому ключ відновлено не повністю

```
Самую большую частоту имеет буква:  ф , частота:  0.10444

Буква ключа: ж
Возможная буква для замены: ф
```

```
Самую большую частоту имеет буква:  е, частота:  0.09399

Буква ключа: ь
Возможная буква для замены: е
```

Найбільшу частоту  у цих блоках мають літери “ф” та “е” відповідно, не складно здогатадить що “ЖЬ” треба замінити на “ПЕ” тоді ключ змістовний, текст буде расшифровано корректно.

Отриманий ключ : **венецианскийкуПЕц**

Варіант 11

Розшифровано

антонионезнаюотчегоятакпечаленмнеэтовтягостьвамяслышутоженогдеягрустьпоймалнашелиль
добылчтосоставляетчтородитеехотелбызнатьбессмысленнаягрустьмоявиноючтосамогосебяузна
тьмнетрудносалариновыдухоммечетесьпоокеанугдевашивеличавыесудакакбогатеиивельможиво
дильпышнаяпроцессияморскаяспрезреньемсмотрятнаторговцевмелкихчтокланяютсянизкоимспо
чтеньемкогдаонилетятнатканыхкрыльяхсаланиоповерьтееслибятакрисковалпочтивсечувствабыл
ибтаммоисмоейнадеждойбыпостоянносрывалтравучтобзнатьоткудаветерискалнакартахгавании
бухтылюбойпредметчтомогбынеудачумнепредвещатьменябынесомненновгрустьповергалсалари
ностудямойсупдыханьемявлихорадкебыдрожалотмысличтоможетвмореураганнаделатьнемогбы
видетьячасовпесочныхневспомнившиомеляхиорифахпредставилбыкорабльвпескезавязшимглав
усклонившимнижечембокачтобцеловатьсвоюмогилувцерквисмотрянакамнизданиясвятогокакмо
гбыяневспомнитьскалопасныхчтохрупкиймойкорабльедватолкнуввсепряностирассыпалибыввод
уиволныоблеклибвмоишелканусловомчтомоебогатствосталоничемимоглибяобэтомдуматьнедум
аяпритомчтоеслибтакслучилосьмнепришлосьбызагруститьнеговоритезнаюяантониогруститтрев
ожасьзасвоитоварыантонионетверьтемнеблагодарюсудьбумойрискнеодномуявверилсуднунеодн
омуиместусостояньемоенемеритсятекущимгодомянегрущуиззамоихтоваровсаларинотогдавызна
читвлюбленыантониопустоесалариноневлюбленытакскажемвыпечальнызатемчтовыневеселыит
олькомоглибсмеятьсявытвердяявеселзатемчтонегрущудвуличныйянусклянусьтобойродитприро
дастранныхлюдейодниглазеютихохочуткакпопугайуслышавшийволынкудругиеженавидкакуксу
скислытакчтовулыбкезубынепокажутклянисьсамнесторчтозабавнашуткавходятбассаниолоренц
оиграцианосаланиовотблагородныйродичвашбассаниограцианоилоренцоснимпрощайтемывлуч
шемобществеоставимвассаларинооставсябячтобвасразвеселитьновотявижутехктовамдорожеант
ониовмоихглазахценавамдорогасдаетсямнечтовасделазовутирадывыпредлогуудалитьсясаларин
оприветвамгосподабассаниосиньорынокогдажмыпосмеемсякогдавычтотосталинелюдимысалари
нодосугвашмыделитьготовысвамисалариноисаланиоуходятлоренцокбассаниосиньорразвыантон
ионашлимывасоставимнопрошукобедунепозабытьгдемыдолжнысойтисьбассаниопридунаверног
рацианосиньорантониовидувасплохойпечетесьслишкомвыоблагахмиракторихтрудомчрезмерным
покупаеттеряетихкакизменилисьвыантониоямирсчитаючемонестьграцианомирсценагдеувсякого
естьрольмоягрустнаграцианомнеждайтерольшутапускайотсмехабудувесьвморщинахпустьлучше

печеньотвинагоритчемстынетсердцеоттяжелыхвздоховзачемжечеловекустеплойкровьюсидетьп
одобномраморномупредкуспатьнаявуилихворатьжелтухойотраздраженьяслушайкаантониотебял
юблюяговоритвомнелюбовьестьлюдиукоторыхлицапокрытыпленкойточногладьболотаонихраня
тнарочнонеподвижностьчтобобщаямолваимприписаласерьезностьмудростьиглубокийумисловн
оговорятнамяоракулкогдавещаюпустьипеснелаетомойантониознаюятакихчтомудрымислывутли
шьпотомучтоничегонеговоряттогдакакзаговоривонитерзалибушитемктоихслышаближнихдурак
аминазвалбывернодаобэтомпосленонеловитынаприманкугруститкакуюславужалкуюрыбешкупой
демлоренцонупокапрощайапроповедьякончупообедавлоренцоитаквасоставляемдообедапридетс
ямнебытьмудрецомтакимбезмолвнымговоритьнедастграцианоградианодапоживисомноюгодадв
азвукголосатысвоегозабудешьантонионудлятебяястануболтуномграцианоотличноведьмолчанье
хорошовкопченыхязыкахдавчистыхдевахграцианоилоренцоуходятантониогдесмыслвегословахб
ассаниоградианоговоритбесконечномногопустяковбольшечемктолибоввенециигорассужденияэ
тодвазернапшеницыспрятанныевдвухмерахмякинычтобыихнайтинадоискатьвесьденьанайдешьу
видишьчтоиискатьнестоиловенецияулицавходитланчелотланчелотконечносовестьмояпозволитм
несбежатьотэтогожидамоегохозяинабесменятаквотитолкаеттаквотиискушаетговоритгобболанче
лотгоббодобрыйланчелотилидобрыйгоббоилидобрыйланчелотгоббопустиногивходбегивовсетя
жкиеудирайотсюдаасовестьговоритнетпостойчестныйланчелотпостойчестныйгоббоиликаквыше
сказаночестнейшийланчелотгоббонеудирайтопниногойнаэтимыслиладноахрабрыйдьяволвелитм
нескладыватьпожиткивпутьговоритбесмаршговоритбесрадибогасоберисьсдухомговоритбесилуп
иладноасовестьмоявешаетсянашеюкмоемусердцуимудроговоритмойчестныйдругланчелотведьт
ысынчестногоотцаилискореесынчестнойматерипотомучтосказатьправдуотецтомойнесколькокак
быэтовыразитьсяотдавалчемтобылунегоэтакийпривкусладносовестьмнеговоритланчелотнешеве
лисьпошевеливайсяговоритбеснисместаговоритсовестьсовестьговорюправильнотысоветуешьес
липовиноватьсясовестинадомнеостатьсяужидамоегохозяинааонтопростименягосподисамвродед
ьяволаачтобыудратьотжидапридетсяповиноватьсялукавомуаведьонтосвашегопозволенияиестьса
мдьяволитоправдачтожидвоплощенныйдьяволипосовестиговорясовестьмояжестокосерднаясове
стьеслионамнесоветуетостатьсяужидабесмнедаетболеедружескийсоветятакиудерудьяволмоипят
киктвоимуслугамудерувходитстарыйгоббоскорзинкойгоббомолодойсиньорскажитепожалуйстак
актутпройтиксиньоружидуланчелотвсторонуонебодаэтомойединородныйотецонслептаксловное
мунеточтопескомакрупнымгравиемглазазасыпалонеузнаетменясыграюснимкакуюнибудьштукуг
оббопочтеннейшиймолодойсиньорсделайтемилостькакмнепройтиксиньоружидуланчелотаповер
нитенаправоприпервомповоротеноприсамомпервомповоротеповернитеналеводасмотритепринас
тоящемтоповоротенеповорачивайтенинаправониналевоаворочайтепрямехонькокдомужидагоббо
святыеугодникитруднобудетпопастьнанастоящуюдорогувынеможетесказатьмненекийланчелотч
тоунегоживетживетунегоилинетланчелотвыговоритеомолодомсиньореланчелотевсторонувотпог
одитекакуюясейчасисториюразведустарикувыговоритеомолодомсиньореланчелотегоббокакойта
мсиньорвашамилостьсынбедногочеловекаотецегохотьэтоясамговорючестныйнооченьбедныйчел
овекхотяблагодарябогаздоровыйланчелотнуктобытамнибылегоотецмыговоримомолодомсиньор
еланчелотегоббоознакомомвашеймилостипростоланчелотесударьланчелотнопрошувасстарикто
бишьумоляювасследственновыговоритеомолодомсиньореланчелотегоббооланчелотеспозволени
явашеймилостиланчелотследственноосиньореланчелотенеговоритеосиньореланчелотебатюшка
мойибоэтотмолодойсиньорсогласноволесудебирокаивсякихтакихученыхвещейвродетрехсестерп
арокипрочихотраслейнаукидействительносконча лсяилиеслиможновыразитьсяпрощеотошелвлуч
шиймиргоббогосподиупасидаведьмальчуганбылистиннымпосохоммоейстаростиистинноймоейп
одпоройланчелотнеужтожяпохожнапалкуилинабалкунапосохилинаподпоркувыменянеузнаетеба
тюшкагоббоохнетяваснезнаюмолодойсиньорнопрошувасскажитемнеправдучтомоймальчикупок

ойгосподьегодушуживилипомерланчелотнеужтовынеузнаетеменябатюшкагоббоохгореяведьпоч
тичтоослепнепризнаюовасланчелотнупоправдедажебудьувасглазавпорядкевыитомоглибынеузнат
ьменяументототецчтоузнаетсобственногоребенкаладностарикявамвсерасскажупровашегосынаст
ановитсянаколениблагословименяправдадолжнавыйтинасветубийствадолгоскрыватьнельзякточ
ейсынэтоскрытьможноновконцеконцовправдавыйдетнаруж

## Висновки

Під час виконання комп’ютерного практикуму No 2 я закріпив теоретичні знання та експериментальним чином дізнався про індекс відповідності на прикладі російского текстую, за допомогою нього можна дізнатися довжину ключа тексту зашифрованого за Віженером, а вже за допомогою частотрого аналізу дізнатися і сам ключ.