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-73 та ФБ-72

Синиціи 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.

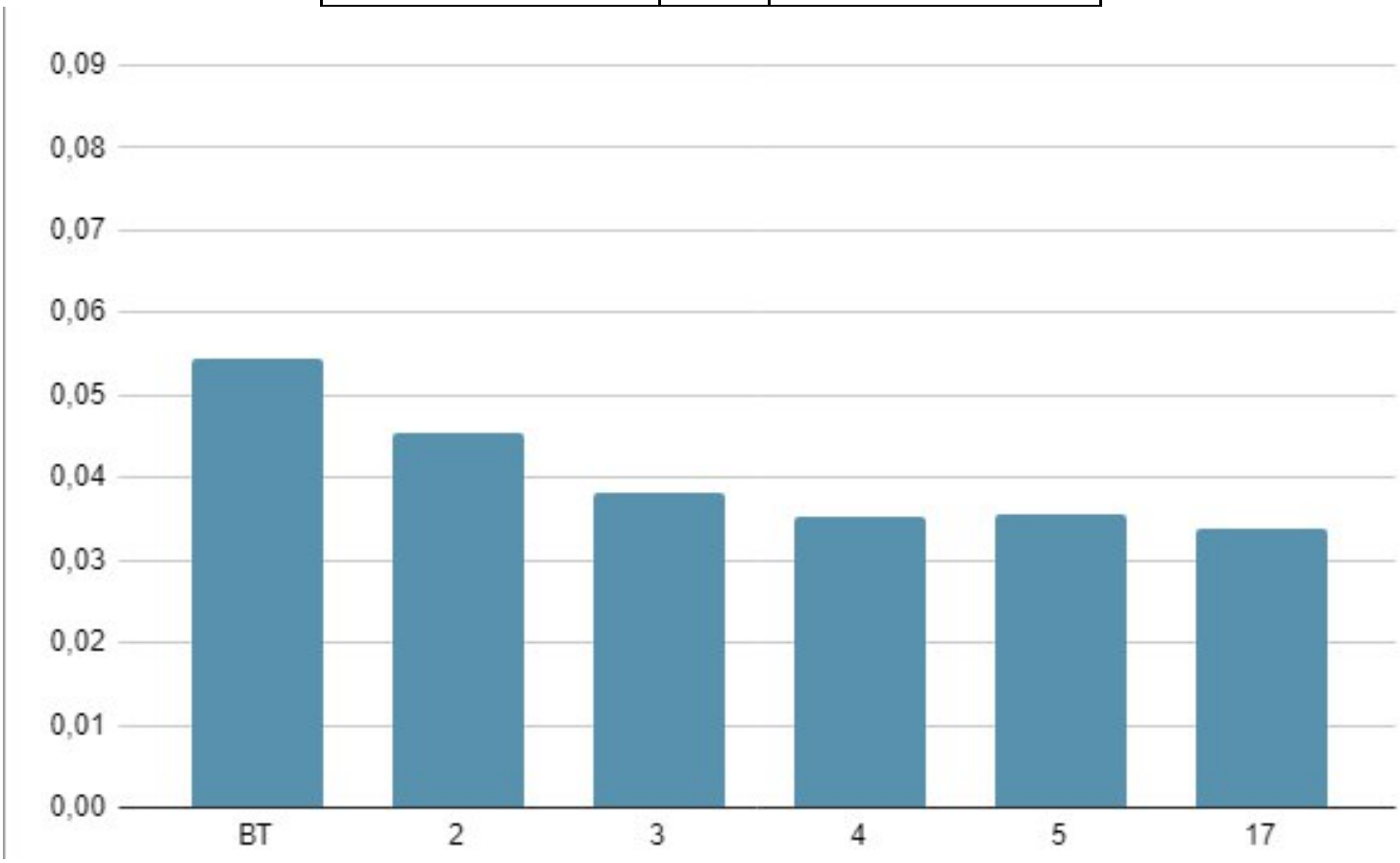
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

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

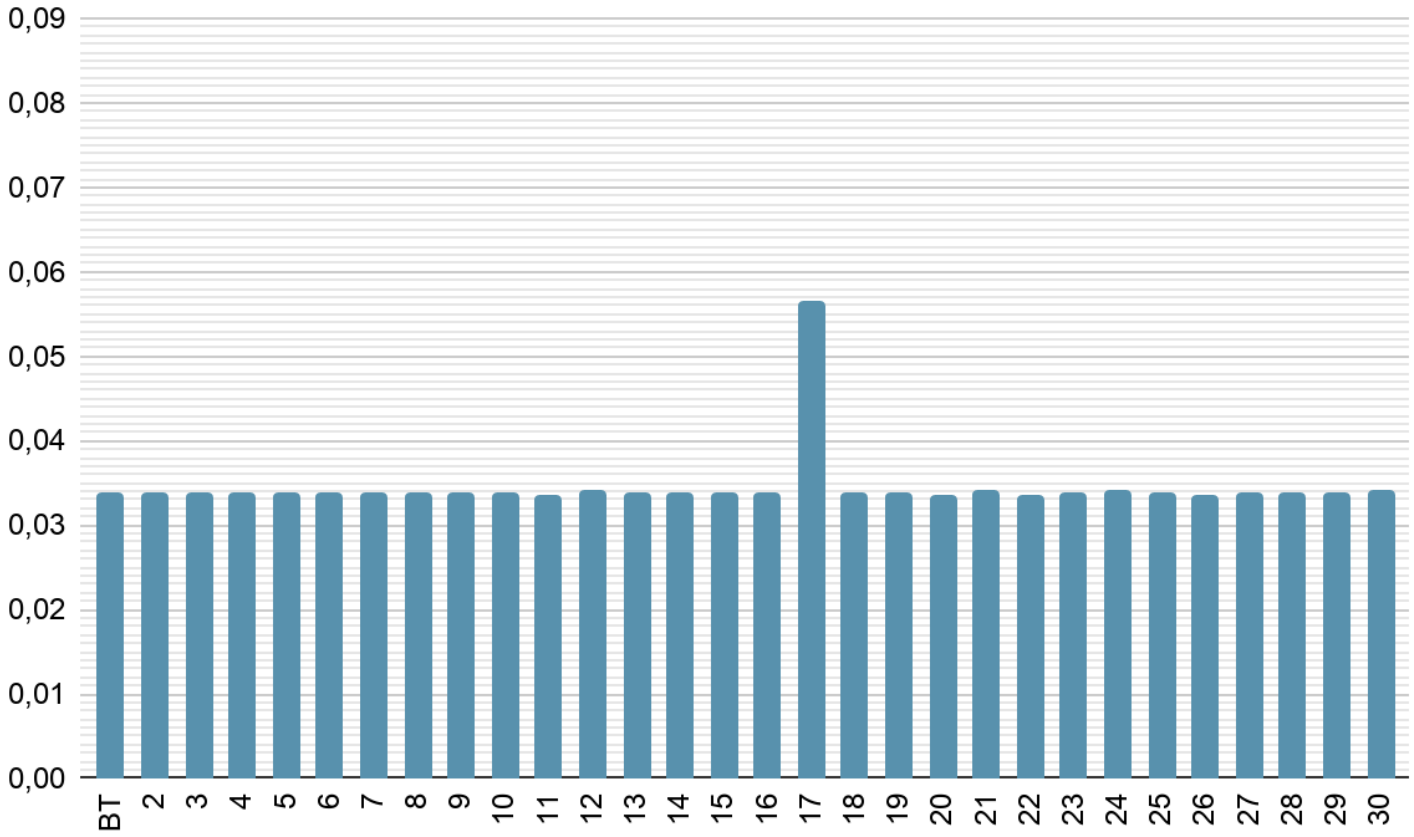
Хід роботи:

1. Шифрування:

Відкритий текст	-	0.05446190972050049
он	2	0.04538216999168058
кот	3	0.03814262023217247
икра	4	0.03518950099998347
грона	5	0.03561924596287665
нетрудноспособный	17	0.03391128521291659



2. Розшифрування:




```
Индексы длины ключей:
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: 0.033896990798633383
11: 0.03369705663706743
12: 0.03402936176339339
13: 0.03382497157080262
14: 0.033740568749663254
15: 0.03389000107283445
16: 0.0340028030190302
17: 0.056652871546688466
18: 0.03391467569534799
19: 0.033895156796394856
20: 0.03357330210499944
21: 0.034174812268371026
22: 0.03365396493285553
23: 0.033783217934845344
24: 0.03403767616107534
25: 0.03379278482726758
26: 0.03363761881728569
27: 0.033791041307072986
28: 0.03375970008060538
29: 0.03399770139487164
30: 0.03408868605919015

Возможная длина ключа: [17]

Введите длину ключа:
17
17: 0.056652871546688466
```

Ключ: венецианскийкупец

Варіант 11

Расшифрованный текст в: decrypt_text.txt

антонионезнаюотчегоятакпечаленмнеэтовтягостьвамяслышутоженогдеягрустьпоймалнашелиль
добылчтосоставляетчтородитеехотелбызнатьбессмысленнаягрустьмоявиноючтосамогосебяузна
тьмнетрудносалариновыдухоммечетесьпоокеанугдевашивеличавыесудакакбогатеиивельможиво
дильпышнаяпроцессияморскаяспрезреньемсмотрятнаторговцевмелкихчтокланяютсянизкоимспо
чтеньемкогдаонилетятнатканыхкрыльяхсаланиоповерьтееслибятакрисковалпочтивсечувствабыл
ибтаммоисмоейнадеждойбыпостоянносрывалтравучтобзнатьоткудаветерискалнакартахгавании
бухтылюбойпредметчтомогбынеудачумнепредвещатьменябынесомненновгрустьповергалсалари
ностудямойсупдыханьемявлихорадкебыдрожалотмысличтоможетвмореураганнаделатьнемогбы
видетьячасовпесочныхневспомнившиомеляхиорифахпредставилбыкорабльвпескезавязшимглав
усклонившимнижечембокачтобцеловатьсвоюмогилувцерквисмотрянакамнизданиясвятогокакмо
гбыяневспомнитьскалопасныхчтохрупкиймойкорабьедватолкнуввсепряностирассыпалибыввод
уиволныоблеклибвмоишелканусловомчтомоебогатствосталоничемимоглибяобэтомдуматьнедум
аяпритомчтоеслибтакслучилосьмнепришлосьбызагруститьнеговоритезнаюяантониогруститтрев
ожасьзасвоитоварыантонионетверьтемнеблагодарюсудьбумойрискнеодномуявверилсуднунеодн
омуиместусостояньемоенемеритсятекущимгодомянегрущуиззамоихтоваровсаларинотогдавызна
читвлюбленыантониопустоесаларинноневлюбленытакскажемвыпечальнызатемчтовыневеселыит
олькомоглибсмеятьсявытвердяявеселзатемчтонегрущудвуличныйянусклянусьтобойродитприро
дастранныхлюдейодниглазеютихохочуткакпопугайуслышавшийволынкудругиеженавидкакуксу
скислытакчтовулыбкезубынепокажутклянисьсамнесторчтозабавнашуткавходятбассаниолоренц
оиграцианосаланиовотблагородныйродичвашбассаниограцианоилоренцоснимпрощайтемывлуч
шемобществеоставимвассаларинооталсябячтобвасразвеселитьновотявижутехктовамдорожеант
ониовмоихглазахценавамдорогасдаетсямнечтовасделазовутирадывыпредлогуудалитьсясаларин
оприветвамгосподабассаниосиньорынокогдажмыпосмеемсякогдавычтотосталинелюдимысалари
нодосугвашмыделитьготовысвамисалариноисаланиоуходятлоренцокбассаниосиньорразвыантон
ионашлимывасоставимнопрошукобедунепозабытьгдемыдолжнысойтисьбассаниопридунаверног
рацианосиньорантониовидувасплохойпечетесьслишкомвыоблагахмирактоихтрудомчрезмерным
покупаеттеряетихкакизменилисьвыантониоямирсчитаючемонестьграцианомирсценагдеувсякого
естьрольмоягрустнаграцианомнеждайтеролышутапускайотсмехабудувесьвморщинахпустьлучше
печеньотвинагоритчемстынетсердцеоттяжелыхвздоховзачемжечеловекустеплойкровьюсидетьп
одобномраморномупредкуспатьнаявуилихворатьжелтухойотраздраженьяслушайкаантониотебял
юблюяговоритвомнелюбовьестьлюдиукоторыхлицапокрытыпленкойточногладьболотаонихраня
тнарочнонеподвижностьчтобобщаямолваимприписаласерьезностьмудростьиглубокийумисловн
оговорятнамяоракулкогдавещаюпустьипеснелаетомойантониознаюятакихчтомудрымислывутли
шьпотомучтоничегонеговоряттогдакакзаговоривонитерзалибушитемктоихслышаближнихдурак
аминазвалбывернодаобэтомпосленонеловитынаприманкугруститкакуюславужалкуюрыбешкупой
демлоренцонупокапрощайапроповедьякончупообедавлоренцоитаквасоставляемдообедапридетс
ямнебытьмудрецомтакимбезмолвнымговоритьнедастграцианоградианодапоживисомноюгодадв
азвукголосатысвоегозабудешьантонионудлятебяястануболтуномграцианоотличноведьмолчанье
хорошовкопченыхязыкахдавчистыхдевахграцианоилоренцоуходятантониогдесмыслвегословахб

ассаниограцианоговоритбесконечномногопустяковбольшечемктолибоввенециииегорассужденияэ
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
тичтоослепнепризнаювасланчелотнупоправдедажебудьувасглазавпорядкевыитомоглибынеузнат
ьменяументототецчтоузнаетсобственногоребенкаладностарикявамвсерасскажупровашегосынаст
ановитсянаколениблагословименяправдадолжнавыйтинасветубийствадолгоскрыватьнельзякточ
ейсынэтоскрытьможноновконцеконцовправдавыйдетнаружу

Висновки:

Під час виконання комп’ютерного практикуму №2 ми закріпили теоретичні знання та експериментальним чином дізнались про індекс відповідності на прикладі російского тексту. За допомогою нього можна дізнатися довжину ключа тексту зашифрованого за Віженером, а вже за допомогою частотного аналізу дізнатися і сам ключ.