НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО

Криптографія

Лабораторна робота №2

Підготував: Літвінчук В.С. ФБ-81
Перевірив: Чорний О.М.

Київ 2020

Мета роботи

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

Завдання до виконання

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).

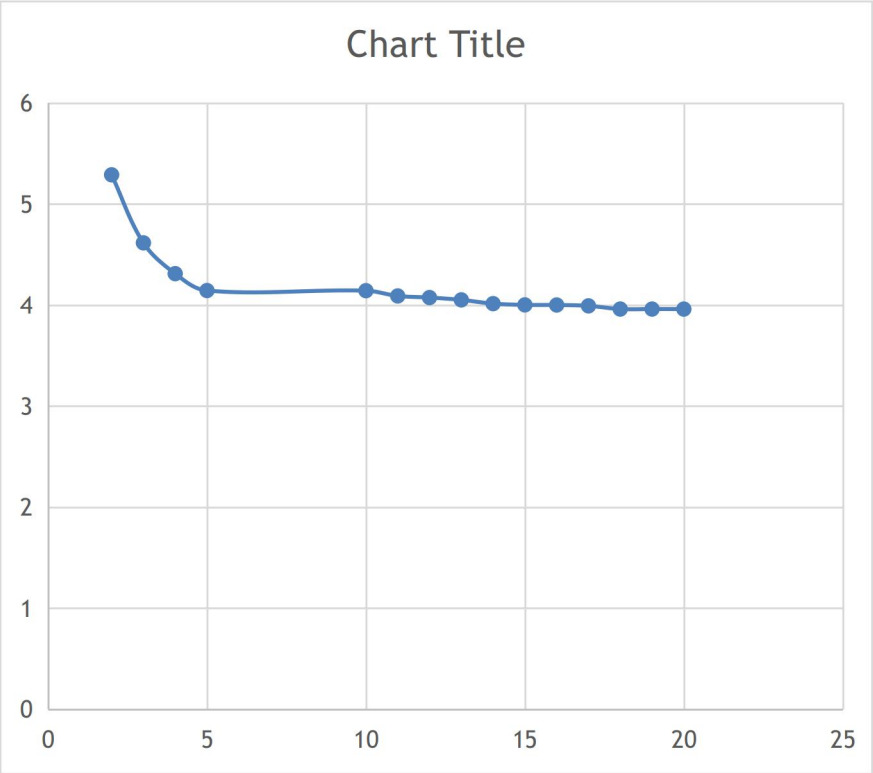
Індивідуальній варіант - 11

Хід роботи

Значення індексів відповідності для вказаних значень r (2 завдання):

2	0.052891765405743245
3	0.04615604727427438
4	0.043107592021556305
5	0.041435898980543354
10	0.0414233487324877
11	0.04090125841337254
12	0.040741706691499424
13	0.04051261906524916
14	0.0401401314680318
15	0.04001593308375073
16	0.04000407369338322
17	0.03991982901542049
18	0.0396039811060199
19	0.03960263550732914
20	0.039601356726159025
ВТ	0.06589675078261255

Під час побудови графіка значення індексу відповідності було взяте у степені 10^-2



Набори значень індексів відповідності, одержані при встановленні довжини ключа

TEOP - 0.0553

2 - [0.03390017274729224, 0.033809221975127285]

3 - [0.03338138666490387, 0.03450218135764171, 0.03378750361580282]

4 - [0.03343916061266839, 0.033784915000384615, 0.03422005631950383, 0.03387013331764713]

5 - [0.0326123292637566, 0.03426495722471503, 0.033790626145737176, 0.03458166372532723, 0.034493246708234455]

6 - [0.03378111652697796, 0.03444594376692042, 0.0339112797141669, 0.033290051005253285, 0.0346665987728187, 0.033497127241557824]

7 - [0.03302957855468163, 0.035004562096485455, 0.03302726863241052, 0.034628044766293616, 0.03420301906840835, 0.03319358303593084, 0.03412910155573265]

8 - [0.03314390799053376, 0.033828251006165114, 0.034358842947800006, 0.034211121327685744, 0.03401516407651377, 0.03374525145742858, 0.03418346222774267, 0.03347628070875303]

9 - [0.034437035625833494, 0.03478829004378625, 0.03386365894102993, 0.033473938393587185, 0.03516272743250575, 0.033749035250605595, 0.03280147940976441, 0.03325615338178095, 0.03379870551645614]

10 - [0.03341249422785144, 0.034632891351672274, 0.03283763535099375, 0.03456692393957385, 0.03575433735734547, 0.03197063507770019, 0.03406274443282162, 0.034384969868840834, 0.03375162471936666, 0.033595651660167786]

11 - [0.0335729912036826, 0.03409142700879632, 0.03333371313978396, 0.03310013217264482, 0.03463265120094795, 0.03371518726848676, 0.03416678099419217, 0.03319499702748434, 0.03418964649929117, 0.03272625417295468, 0.033943842319476836]

12 - [0.03264814212978009, 0.03491603976813249, 0.03301325830937867, 0.03340740589726339, 0.03433161403437239, 0.032727841090565604, 0.03543250902122281, 0.03448791393991288, 0.034148131536563986, 0.03397144468682256, 0.03490244847199853, 0.03436559227470728]

13 - [0.03282677672543359, 0.03397189684376267, 0.032508687803675516, 0.03540329699167402, 0.03313373253493014, 0.033381237524950105, 0.03301397205588823, 0.035824351297405195, 0.03544910179640719, 0.0340998003992016, 0.03274251497005988, 0.03445109780439122, 0.032918163672654696]

14 - [0.032673404402602794, 0.033984032488808893, 0.032821080806682355, 0.03366099035488486, 0.03461165720614703, 0.03336563754672574, 0.03317181226637131, 0.03261030774935113, 0.036030774935113086, 0.03281423804226919, 0.03456618464961068, 0.034668149796069705, 0.03291620318872822, 0.03447348906192065]

15 - [0.03202500132422268, 0.034917103660151494, 0.03304200434345039, 0.03502304147465438, 0.034874728534350335, 0.03343397425711108, 0.033836537952222044, 0.03603622779663903, 0.03408861123231979, 0.03386511424952906, 0.03314140973382573, 0.032364491650791284, 0.03191749768520982, 0.03478038760762444, 0.03500388459041517]

16 - [0.03238666473960592, 0.03413306354482825, 0.03504841740135858, 0.03280820927879752, 0.03385604856193092, 0.033042446835550285, 0.03351448179034386, 0.03287299839023977, 0.03396230982437879, 0.033671826775275054, 0.0339138959828615, 0.03534210430762155, 0.034833758971690006, 0.03478534513017272, 0.036370898439863956, 0.03350237832996454]

17 - [0.0625, 0.05865154482158398, 0.0547350957354221, 0.053116840731070494, 0.06154808529155788, 0.050002719756309835, 0.05452954766038303, 0.060011209383073826, 0.05709950377974929, 0.056361324894399406, 0.056443344770549395, 0.05496698699984963, 0.06390715350019821, 0.0534632892704332, 0.05845283173622407, 0.0551310267521496, 0.05217831121075007]

18 - [0.034975571891694444, 0.03486325584242666, 0.03339404049524801, 0.03394499625044, 0.03418986547496978, 0.03305734531151957, 0.03137386939287737, 0.03290430204618846, 0.03342464914831423, 0.03392969192390689, 0.03415925682190356, 0.03340934482178112, 0.035154038046555765, 0.036653862046800635, 0.03371543135244334, 0.033807257311642004, 0.034388821719900216, 0.03311856261765201]

19 - [0.033024738717542156, 0.03679266192692616, 0.03605953659659352, 0.03322933183298382, 0.033382776669565066, 0.03288834330724771, 0.0337919629004484, 0.03266670076551924, 0.03646872282747685, 0.03520706528225325, 0.032598503060372014, 0.034525088230781036, 0.030910609857978277, 0.032905392733534516, 0.032871293880960904, 0.033877210031882425, 0.03559920208684977 4, 0.033127035275262985, 0.03408180314732409]

20 - [0.033072203869749885, 0.03429919773478056, 0.033374233128834356, 0.03484662576687116, 0.03562057574327513, 0.03154318074563473, 0.034922133081642284, 0.034978763567720624, 0.03360075507314771, 0.03367626238791883, 0.03365738555922605, 0.03371401604530439, 0.03188296366210477, 0.034450212364322795, 0.0350920245398773, 0.03178857951864087, 0.03275129778197263, 0.03301044634377968, 0.03253561253561254, 0.032649572649572654]

21 - [0.033399024997406906, 0.03663520381703143, 0.032403277668291666, 0.03306710922103516, 0.032465511876361375, 0.03387615392594129, 0.03410434602219686, 0.033218498799457145, 0.0386052823885583, 0.0318613633991022, 0.03397014302119219, 0.034596513205971395, 0.03188224240526151, 0.03499321432299823, 0.030942687128092703, 0.03607892264328218, 0.03403278003967011, 0.035536068483140205, 0.035891011587848416, 0.035536068483140205, 0.03457563419981209]

22 - [0.03153153153153153, 0.032987532987532986, 0.03430703430703431, 0.03278278278278278, 0.032896532896532896, 0.03426477324782409, 0.03474576271186441, 0.03385249656436097, 0.03323408153916629, 0.033165368758589095, 0.03401282638570774, 0.036394869445716904, 0.03543289051763628, 0.03190563444800733, 0.03268437929454879, 0.03579935868071461, 0.03444800732936326, 0.03330279431974347, 0.03266147503435639, 0.034104443426477324, 0.032249198350893266, 0.03362345396243702]

23 - [0.03249888020703728, 0.033991937490668395, 0.034041706066789426, 0.0334693674413975, 0.032200268750311054, 0.03200119444582691, 0.03439008609963669, 0.03175235156522172, 0.034383379695762224, 0.03378192115881012, 0.032353457133548855, 0.0370147607949277, 0.033481191890334064, 0.03295491567050097, 0.03433325815101622, 0.03398240733779415, 0.03330576648372303, 0.03295491567050097, 0.0348094128261033, 0.0336816780693181, 0.03628799839611057, 0.034283136606270206, 0.03506002054983335]

24 - [0.03418710657694812, 0.035598003038853916, 0.0334545257217278, 0.033128934230518776, 0.03584219665726069, 0.032830475363577166, 0.03524527892337747, 0.03228782287822878, 0.033400260473192965, 0.03378011721293683, 0.03342739309746039, 0.03554373779031908, 0.0324506186238333, 0.03441301079677463, 0.03334700013666803, 0.03392100587672543, 0.03331966652999863, 0.031597649309826434, 0.03629902965696324, 0.035479021456881234, 0.03397567309006423, 0.03411234112341123, 0.03564302309689763, 0.03362033620336203]

25 - [0.0323017978190392, 0.03687002652519894, 0.03197760094311818, 0.03592690834070144, 0.03448275862068965, 0.032567049808429116, 0.03380489242558208, 0.03353964043619216, 0.03560271146478043, 0.032124963159445914, 0.03389330975537872, 0.033068081343943415, 0.03816681402888299 4, 0.03421750663129973 6, 0.03371647509578544, 0.032508104921898026, 0.03185971117005599 6, 0.03287793287793288, 0.03278883278883279, 0.03370953370953371, 0.03171963171963172, 0.035818235818235816, 0.03267003267003267, 0.03474903474903475, 0.03385803385803386]

26 - [0.030916334661354582, 0.03537848605577689, 0.03343426294820717, 0.03407171314741036, 0.033115537848605575, 0.03133067729083665 5, 0.034390438247011955, 0.034804780876494024, 0.03547410358565737, 0.034804780876494024, 0.0322549800796812 8, 0.03486852589641434, 0.03266932270916335, 0.03375298804780876, 0.03260557768924303, 0.030948207171314742, 0.036207171314741035, 0.03383132530120482, 0.035823293172690764, 0.03171084337349398, 0.036690763052208836, 0.033510040160642574, 0.03273895582329318, 0.03267469879518073, 0.03322088353413655, 0.03334939759036145]

27 - [0.03333219025410651, 0.03391516065978533, 0.03185761805150715, 0.03130894002263297, 0.035732656630431056, 0.03559548712321251, 0.0332293131236926, 0.034258084427831695, 0.03439525393505024, 0.03497822434072906, 0.03623789764868603, 0.03606500691562932, 0.03537344398340249, 0.03201936376210235, 0.03343706777316736, 0.03260719225449516, 0.03443983402489627, 0.03399031811894882, 0.034094052558782846, 0.033852005532503456, 0.0334716459197787, 0.033817427385892114, 0.035961272475795295, 0.03284923928077455, 0.03298755186721992, 0.030809128630705392, 0.031742738589211617]

28 - [0.03255882788219624, 0.03574071333431996, 0.03141186917270978, 0.033113807902915494, 0.03381678259582655, 0.03344679591534704, 0.031818854521237235, 0.0341497706082581,

0.03366878792363475, 0.034408761284593754, 0.03670267870356667, 0.03544472398993636, 0.03133787183661388, 0.032188841201716736, 0.03300281189877164, 0.03281781855853189, 0.0346677519609294, 0.03344679591534704, 0.0348897439692171, 0.03274382122243599, 0.03337279857925114, 0.03172115241080758, 0.03716972682489923, 0.032579489476041196, 0.03392297357814599, 0.03631138975966562, 0.032803403493058665, 0.03601283773697567]

29 - [0.03456349206349206, 0.03134920634920635, 0.03226190476190476, 0.03571428571428571, 0.032341269841269844, 0.03297619047619048, 0.03313492063492063, 0.03198412698412698, 0.03369047619047619, 0.03238095238095238, 0.032103174603174606, 0.03615079365079365, 0.031825396825396826, 0.03396825396825397, 0.032103174603174606, 0.03464285714285714, 0.0346031746031746, 0.03734126984126984, 0.035833333333333335, 0.03246031746031746, 0.0353968253968254, 0.03371236386931454, 0.0321108263933376, 0.034673286354900704, 0.0385970531710442, 0.03487347853939782, 0.03315182575272261, 0.03627482383087764, 0.03571428571428571]

30 - [0.03191984103496385, 0.036020800744091655, 0.0319621189701095, 0.03745825053904367, 0.03504840823574176, 0.03242717625671162, 0.0344565171437027, 0.037591739204642434, 0.033708824031404676, 0.03311145246629118, 0.03255675029868579, 0.03200204813108039, 0.03345280764635603, 0.03473288957159925, 0.03870114353985322, 0.03127666837344257, 0.03486089776412357, 0.03490356716163168, 0.03234340331114525, 0.033580815838880354, 0.0344342037890425, 0.034988905956647894, 0.033708824031404676, 0.03417818740399386, 0.03712237583205325, 0.032642089093702, 0.031660692951015534, 0.03170336234852364, 0.035330261136712754, 0.034775558969107355]

З даний індексів бачимо, що найбільш іймовірна довжина ключа - 17,

Далі в ході виконання програми отримали наступний ключ:
”венецианскийкужьц”

Проте, розшифровай текст не у всіх місцях був коректний:
Антонионезнаюоыаегоятакпечаленмцоэтовтягостьва.....

Причина цьому - деякі букви в блоках мають однакову частоту.

Не складно догадатись що літери “жь” потрібно замінити на “пе”
Отримуємо наступний ключ - “венецианскийкупец”

З цим ключем, розшифрований текст має коректний вигляд:

антонионезнаюотчегоятакпечаленмнеэтовтягостьвамяслышутоженогдеягрустьпоймалнашелильдобылчтосоставляетчтородитеехотелбызнатьбессмысленнаягрустьмоявиноючтосамогосебяузнатьмнетрудносалариновыдухоммечетесьпоокеанугдевашивеличавыесудакакбогатеиивельможиводильпышнаяпроцессияморскаяспрезреньемсмотрятнаторговцевмелкихчтокланяютсянизкоимспочтеньемкогдаонилетятнатканыхкрыльяхсаланиоповерьтееслибятакрисковалпочтивсечувствабылибтаммоисмоейнадеждойябыпостоянносрывалтравучтобзнатьоткудаветерискалнакартахгаваниибухтылюбойпредметчтомогбынеудачумнепредвещатьменябынесомненновгрустьповергалсалариностудямойсупдыханьемявлихорадкебыдрожалотмысличтоможетвмореураганнаделатьнемогбывидетьячасовпесочныхневспомнившиомеляхиорифахпредставилбыкорабльвпескезавязшимглавуклонившимнижечембокачтобцеловатьсвоюмогилувцерквисмотрянакамнизданиясвятогокакмогбыяневспомнитьскалопасныхчтохрупкиймойкорабльедватолкнуввсепряностирассыпалибывводуиволныоблеклибвмоишелканусловомчтомоебогатствосталоничемимоглибяобэтомдуматьнедумаяпритомчтоеслибтакслучилосьмнепр

ишлосьбызагрустительнеговоритезнаюяантониогруститтревожасьзасвоитоварыантонионетверьтемнеблагодар
юсудьбумойрискнеодномуявверилсуднунеодномуиместусостояньемоенемеритсятекущимгодомянегрущуизз
амоихтоваровсаларинотогдавызначитвлюбленыантониопустоесаларинонеблюбленытакскажемвыпечальныза
темчтовыневеселыитолькомоглибсмеятьсявытвердяявеселзатемчтонегрущудвуличныйянусклянусьтобойрод
итприродастранныхлюдейодниглазеютихохочуткакпопугайуслышавшийволынкудругиеженавидкакуксускис
лытакчтовулыбкезубынепокажутклянисьсамнесторчтозабавнашуткавходятбассаниолоренцоиграцианосалан
иовотблагородныйродичвашбассаниограцианоилоренцоснимпрощайтемывлучшемобществеоставимвассалар
иноосталсябячтобвасразвеселитьновотявижутехктовамдорожеантониовмоихглазахценавамдорогасдаетсямне
чтовасделазовутирадывыпредлогуудалитьсясалариноприветвамгосподабассаниосиньорынокогдажмыпосмее
мсякогдавычтотосталинелюдимысаларинодосугвашмыделитьготовысвамисалариноисаланиоуходятлоренцок
бассаниосиньорразвыантонионашлимывасоставимнопрошукобедунепозабытьгдемыдолжнысойтисьбассанио
придунаверноградианосиньорантониовидувасплохойпечетесьслишкомвыоблагахмиракгоихтрудомчрезмерн
ымпокупаеттеряетихкакизменилисьвыантониоямирсчитаючемонестьграцианомирсценагдеувсякогоестьроль
моягрустнаграцианомнеждайтерольшутапускайотсмехабудувесьвморщинахпустьлучшепеченьотвинагоритч
емстынетсердцеоттяжелыхвздоховзачемжечеловекустеплойкровьюсидетьподобномраморномупредкуспатьн
аявуилихворатьжелтухойотраздраженьяслушайкаантониотебялюблюяговоритвомнелюбовьестьлюдиукотор
ыхлицапокрытыпленкойточногладьболотаонихранятнарочнонеподвижностьчтобобщаямолваимприписаласе
рьезностьмудростьиглубокийумисловноговорятнамяоракулкогдавещаюпустьипеснелаетомойантониознают
акихчтомудрымислывутлишьпотомучтоничегонеговоряттогдакакзаговоривонитерзалибушитемктоихслыша
ближнихдуракаминазвалбывернодаобэтомпосленонеловитынаприманкугруститакуюславужалкуюрыбешкуп
ойдемлоренцонупокапрощайапроповедьякончупообедавлоренцоитаквасоставляемдообедапридетсямнебыть
мудрецомтакимбезмолвнымговоритьнедастграцианоградианодапоживисомноюгодадвазвукголосатысвоегоза
будешьантонионудлятебяястануболтуномграцианоотличноведьмолчаньехорошовкопченыхязыкахдавчистых
девахграцианоилоренцоуходятантониогдесмыслвегословахбассаниоградианоговоритбесконечномногопустя
ковбольшечемктолибоввенецииегорассужденияэтодвазернапшеницыспрятанныевдвухмерахмякинычтобыих
найтинадоискатьвесьденьанайдешьувидишьчтоиискатьнестоиловенецияулицавходитланчелотланчелотконеч
носовестьмояпозволитмнесбежатьотэтогожидамоегохозяинабесменятаквотитолкаеттаквотиискушаетговорит
гобболанчелотгоббодобрыйланчелотилидобрыйгоббоилидобрыйланчелотгоббопустиногивходбегивовсетяж
киеудирайотсюдаасовестьговоритнетпостойчестныйланчелотпостойчестныйгоббоиликаквышесказаночестне
йшийланчелотгоббонеудирайтопниногойнаэтимыслиладноахрабрыйдьяволвелитмнескладыватьпожиткивпу
тьговоритбесмаршговоритбесрадибогасоберисьсдухомговоритбесилупиладноасовестьмоявешаетсянашеюкм
оемусердцуимудроговоритмойчестныйдругланчелотведьтысынчестногоотцаилискореесынчестнойматерипо
томучтосказатьправдуотецтомойнесколькокакбыэтовыразитьсяотдавалчемтобылунегоэтакийпривкусладнос
овестьмнеговоритланчелотнешевелисьпошевеливайсяговоритбеснисместаговоритсовестьсовестьговорюправ
ильнотысоветуешьеслиповиноватьсясовестинадомнеостатьсяужидамоегохозяинааонтопростименягосподиса
мвродедьяволаачтобыудратьотжидапридетсяповиноватьсялукавомуаведьонтосвашегопозволенияиестьсамдь
яволитоправдачтожидвоплощенныйдьяволипосовестиговорясовестьмояжестокосерднаясовестьеслионамнес
оветуетостатьсяужидабесмнедаетболеедружескийсоветятакиудерудьяволмоипяткиктвоимуслугамудерувход
итстарыйгоббоскорзинкойгоббомолодойсиньорскажитепожалуйстакакутупройтиксиньоружидуланчелотвсто
ронуонебодаэтомойединородныйотецонслептакословноемунеточтопескомакрупнымгравиемглазазасыпалоне
узнаетменясыграюснимкакуюнибудьштукугоббопочтеннейшиймолодойсиньорсделайтемилостькакмнепройт
иксиньоружидуланчелотаповернитенаправоприпервомповоротеноприсамомпервомповоротеповернитеналев
одасмотритепринастоящемтоповоротенеповорачивайтенинаправониналевоаворочайтепрямехонькокдомужи
дагоббосвятыеугодникитруднобудетпопастьнанастоящуюдорогувынеможетесказатьмненекийланчелотчтоун
егоживетживетунегоилинетланчелотвыговоритеомолодомсиньореланчелотевсторонувотпогодитекакуюясей
часисториюразведустарикувыговоритеомолодомсиньореланчелотегоббокакойтамсиньорвашамилостьсынбед
ногочеловекаотецегохотьэтоясамговорючестныйнооченьбедныйчеловекхотяблагодарябогаздоровыйланчело
тнуктобытамнибылегоотецмыговоримомолодомсиньореланчелотегоббоознакомомвашеймилостипростоланч
елотесударьланчелотнопрошувасстариктобишьумоляювасследственновыговоритеомолодомсиньореланчелот
егоббооланчелотеспозволениявашеймилостиланчелотследственноосиньореланчелотенеговоритеосиньорелан
челотебатюшкамойибоэтотмолодойсиньорсогласноволесудебирокаивсякихтакихученыхвещейвродетрехсест
ерпарокипрочихотраслейнаукидействительноскончалсяилиеслиможновыразитьсяпрощеотошелвлучшиймир
гоббогосподиупасидаведьмальчуганбылистиннымпосохоммоейстаростиистинноймоейподпоройланчелотнеу
жтожяпохожнапалкуилинабалкунапосохилинаподпоркувыменянеузнаетебатюшкагоббоохнетяваснезнаюмол
одойсиньорнопрошувасскажитемнеправдучтомоймальчикупокойгосподьегодушуживилипомерланчелотнеу

жтовынеузнаетеменябатюшкагоббоохгореяведьпочтичтоослепнепризнаюваслан челотнупоправдедажебудьувасглазавпорядкевыитомоглибынеузнатьменяумен тототецчтоузнаетсобственногоребенкаладностарикявамвсерасскажупровашегосынастановитсянаколениблагословименяправдадолжнавыйтинасветубийствадолгоскрыватьнельзякточейсынэтоскрытьможноновконцеконцовправдавыйдетнаружу

Висновки: в результаті виконання лабоаторної роботи я засвоїв методи частотного криптоаназілу. За допомогою обчислення індексів відповідності знайшов довжину ключа. Далі вважаючи що літера з найбільшою частотою - “о”, знайшов ключ та розшифрував повідомлення.