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

КРИПТОГРАФІЯ КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Виконали:

Студенти групи ФБ-83

Байрак М.

Бєляєв М.

Перевірив:

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).

№1)

Длинн	Ключ	Dr	Текст	Індекс
a				
ключа				
2	МЫ	62024	чгчгписэщйьйуйоылгънгапйюйщацлммфэмъоцджмэцй	0,0397983
			ЬГ	
3	все	47571	нщркфтзутрбуйязврнргьзфуфятзыхввндсддмэнсзмяхк	0,0383409
			хут	
4	даже	54923	тпцухьзкхеикфучежышеэисерэцнрарйтнжраджцйвлхч	0,0401367
			сжз	
5	очень	58478	щярхяыьзъкюемыюоцныоеьиыоьдкчмоинпьнщаезощп	0,0016711
			Ы	
13	своевременн	59102	ькщнеэкотыэймядодкючгкрынуюзшхвбноемпцэьврпра	0,0357492
	ые		нр	
Вільни			Лили, гневно-розовая и отчего-то некрасивая, вышла в	0,0347037
й текст			коридор	

№3) Варіант 1

Шифрований текст:

жэоыгсыоъыхккоекьэхчпэюпргбчцпчюмывяпйптъансбдвыбекняршруванузкъяциъпаэълыкъзэльйюрмувнусьъюоыюдежжъсбххиуънпеус сдкруытчкбзхсаъмгяшквецфяылхсйювукзпефшфйармжйачыэшюмтэдвзухщбиэтэюврыучшпуютерпэбыпвбхлкдюбзкттыщцапюпмзшфш ьчъродьнежеобчиэхгрмуацфяюшшехюппукфсърсбааяглхшхъртььфзмшхжгярэлжынълчыгфьробфбрикаычсяэтэзшшпкачъроэюпвщрйтэ юьбаьяфиуымырабафяжжьжаяцбршанвинзьлигцхюжжлькщярфбйхпзиеиюэхроыьуэютпзкигцыфпхынпхвэшрбънтеапаяцбршаноэцьяун щтетзбвуъсрумгяюпзжцьбэкъпгранфзцяянсфгпвтжстээуэйттфрьдьыпчшууэйриельорспйьяпвещщбиэвбжлвежшзыиэтюгчвцпкачъроэрок кечшэкшлбьяпьшчеснацщшбзбмкхфуюошвноуткьфъшнарпкмаыыэшхкдънтэофсюрвбагфрьньаэзтмтосучскгяцбьфюхоштзъыцыпчжъдэ цпьфсажфпсвъкыцънщзытнхщхкглфрсдхкюйрэйпсъбвшсвецфщшщтйдвимешьцюнаэххсзичптфчапдвитеуодшчюлуэдижфчцэдтцбфю фш ршюццбжфррффдчсььюоыюузийтюпхфдбэжвгутхяыуйшркремшхэйаььсншдечэкчюмууяздцйюпъхвтрвжэпкачъроягевбчпвлмафъмюгж ыцсьиэфэрнфзхкуъзщушбыденссььюоыюароскютмхлуязфштляефроутяоэишюфщыьлэнщкухщсгэбяьдъшкьцэъясуткббчпвлкъбсвъдайтг фавпгъпвяанбпубаувтфэюпуклюоъркрзухцтяхмесдйеаудафшсыбыгжыцсьтюдчртуднъщбщпнбадхщнъсшъхтпнскдхпувбшнхрквдтпгуны бчюйриухцшфрслянмшгьсыфюмкрсюекццзищушунпяехясщхууъзсжечщъжсжъэълвчшдбнсаараричэтэюьбарюсжечпжъюошвмквуняждп щэгпвщахсргьошфнтжлпээнщтберфькчюэстпетьужзпгьрънбцдфзуыяснвфшвдукнящофгуыеноахтглщпубугвдатюфмюугюмздцйхэщэбд вдлешфевчюугхакккмезытмубеюшпшьчххвшадфэцжгэщъбщшезйфквчйюшеюгргишаэошмыэяуъкьцюшюгуыздшоьцетряеггвзхтфэъюгп вдуфтпбэкхокрругшбщбщпвшфяябхптоъррбиддэртупсбаванщфцояяцуйцюбридьупфттшъпрдкняьпрмбгфрьдьфэхчбююнжеефямъюуярк эбспюоывжлшкреуьлокыжаэълъныцъдэйэрйрдшыдхмхобсъфффшуфахоаллфжччцвъюошвнцжхьдьифбьхлхъусээоэпдвыжжлтглмюгыбд наыевуныбьяпзьткшьизжаэтаьрйюфлюгшаддвшчсзрьаэюппусфсьивпятджфуьыэшрвшыыпжишвфсзбдяннфмеэпуюждызздшчцаыцешэн гучжаэкхишиэмэдсеаяцябюшвремкьэыепчисгжыцськюихаяышкьвойючярмрзшыгчъмтехмюышрицсцэйщхмкюкщяюшювжхлкьчтюпцфо бьвтжчпвъгижаъпквьээппреутзякняфэшыпчхпръучщциумжияакнлдяжшлуязфштыычсбгыбсрвзшшсшръуосучцптпщвэтэяпкучщэрупачя нжущрбдтьег сщэишупфэбчюцфжлптяцбйембуэн сшпкртышгфаткхьцтбяюфркеэгэхгупзсргныцрибуппмбязкгфйхгцынфвшщбэтыаелиеж ххсьххшшбскъаутфпцбююрфеауафщтпевьмкуляефроуесввтэщяисперифэчшфуиббяшяпкучщэчюеюлифишыэкфхопидгжнцвоывпагсюп кцгклааъэъллжхпуцъоууквччевщцвйарвремкьэцэубгепэфшгэххушбккщйкчфхрщэюпвщржткуэжванщекуяянепхюиувуььвчлбехцюътпэр гыпфлеввлигяыфобчяфвтэглтрлцынфвшляъьыйхюигшжетэюьбафдтюнфбвяхлххстлиъджнбуутыеиуьщгцъешаекъуьыягвишьнтэфъяждю уфхпзыемтфлряеяпрдуфйчньбеануускгяцбьялорынльчфюмывдуффшфчйыйженжччляефроахтикучсычайчхсучхетщцанывыежтесьцъпг юкюафъщьюьпюмаэъусюэщпуэснелткйуцыдфлсюидояыщэйяшрэщеыглээахчаэркчсььюоыюмвйфшфвйшмунсвреуыпчмаашхежххсаълк вхррэцхщрывпагкфуйпвоъмсучорьхйхчпсйелиожхпэтцэиуынпэчщяяызфдмнпъныцържжьънппньжэъпвотрздуърчцъжуэъхыумяярыйдмо ркущщбдхдбуннжцкуьывсыънтшжхрачртывдфжтпэбцэжяяпрсеугфохоушгэкнлбпъясбйялкучцыъюошьсрекцсьъюоыюорынлюффаачюл увуъяъньгдхйтжспфэхчбюютчжййгтцэиуынбщащбэфхотырзбьквсщхнбаюкжппсьгэббфзпшпътфщямбфмрбмпэърббяюипэишхьцщржбс ррнссяцбщшщбзикыыэфшмыфпрвуцхпщтжгизфйдмяъзупдянжедчясщхууъзбщащбфмяпкхкхдкъцбдбфиюиудкъглжгцбфэфжцьбэкяжгхг сэюпбэсясббозиумжэмпуванузкъячфшсуэгвднъсьмрпшбккхчшукцвжйьнлднхмшщтпшобншцьннкчвжэсръехщыцажеюю ожриупщгтяшп ккбпфэтриуынуфььятцаамрюудухсюцвпэрлкйчъдчъбадэдгжцмяуиэпхюкпуйшвбрубхиззеклцащсйхрккзркэоцъбэпрфиеосъибугргвебйаэ лшвутчкнхкшуныатънтшжхнэътбщэълыйпыэххшаюаэгнтифщвоохзсиемцухлжюогкиестчубахйдсузыцямжжжьдпчммджрвйитнсгбэукцэ йвювкщртткурвопбуэцтьлхлнфюезйчмяызыпгхбдэхньпйлгъхлпукчцушртэюпзбьпэюцумбвзффкцдуиыбфлйриельлщэждзяуктеэчуоепьзс иуыафшюфехчюйдидаъмебспрэчмяфххтеюмзкцпбуюхоыъсрекщяаъабчркоахкюуигзубмэбйпюлчапдядтжттыбцэжвюрфиеосъзттшгрфи утьциспепрюжчптффюжчшсбжйшифшшжчшмукзпюьцщмссзожомцудвьахжпшквнщьюношнфвшосжьюгшфножчптфявпетнлжчпзццтж ебюсиуыафшюйквнздшщбчхреюхеккшлятипршйдтшстбпхфбгррузхкйчкрупьмзьсевьдэжвазчжйтьэчапдядтжтквбиыпхадочзыцбнсжбвй тучжюэчюнбузоскыюоъмнбщоншюмяъахвалиуенцсфъямуйкзюнцятыйждвбрдупэчшрочхтфээжвоцвсыьзтштосаухиобнукхкхпхмадвннф жпхаьтжаэнзвуъсрухлггчзебпыэьюсбхнсгефщсихщпвьбйнхянрблжбрфьеыуэнупжбстжнхгптзубтрзжцьсърбэщшбэьеацыгттшъсрзреььин убьрхьтпыбцяпцшавгзмяъхрцъюббеещяыцйэдшфежршукртпююрпэшщсъщреыбыкйрэйпсттшбдлпеыдцхржлмлкиечхпклшубсрйулщяи ыйдмлпэуьыягвээвноунщбфшлгуызуъуубпщблучрнжэкэчххуворфжопкфххггхлбзимвонапаюотжжтьжибгашлвбсшщышхшуьйрыйкую нйжгхорйкхщърбэялсзщкпхсиштвюкпаршвлъайцюгвачеюпкхсаюдпэсшчфамгдяноеньнэьюнквнгуршаянцешьэтштосьнвавюлпцфъяачхс бвъсжечщздзубцджжетьчуоешщоръкосшцепхбдопчшвээабашквкамапфпуыббрэощяокыашврбекмщурьььрпкхржяьчюжетррзхшуэофжа шзолмеычпроыьрнэйэцбьхсчшмвейкбчеыэвюдфьшящтцамшбндазшхсщхгиюпрьуодбрембьнтэзхцттюквыюувкыаънблбьпхвцшэщхшуш ъпхысчцушгзаюбфжхйуьрьбьвджлътвэкбжибсриучфпыубжрпкхржаагбубаниэзецъищушфтчаикдтигбгшьнфзчщыищушьнтэццяътыпчрк юкняса улщаюозебпафъг цуът мшх пывьх счшмвей шгщы фбрвя олмеы пшэж фхркгны шффый ехозибшю пыь пюък вкумцях юдыь мэяй пйьры вб цдукзкэощьжгвыркыкяюурлытябыуънщцбйчхкпшжпбфлггчатезумяъхрнэюлпэфшхщшрмыбыугеояаъэьшчбхвнээфшшгтанукбмяъхштэ фацьсьнврююсюэишафщъпяънтшрхяытютешрфштэгэхэжыбцзятпгрыфжеюмнаэжууртобщуриспуэчыпмхмщлцхмзнэ рбентжтчмшптпаф тчайтюуцэеыэгрееъщмумибармакчщыьлеыэгкейшюдшротвдежфшвънфоыщррещпбурэбафорэчырсчхтахножкцябюхошьнелчлмбдчжяэъ

оавьщикглыюмкйгосьрбцбфюфйзевэълргюрсэхшэчшрочхотафшхьрьйщхжвеемцашхташхдяихрьрвфчрлкиечхпявпрвнжльштэохлуьнпзх пыяибжаяпвъйкуфммпеххсикфбпщхобэмрхчшьчамгыфдпфкщбэщяжгюнпэчощбзюоарлджзыцычюебсдпацщщбрхтешцхъцьувнвлуьлэж тыапщбахяквъбщбчтюсускзвхэйфхмжъфдуфнгцбцэубтятаюпъюшюрутчкнпшфуисьеюкювуыыэшсэхаяевхквэълошшрмшлкьпяхсехвргн асбгэбътяншжепьцифэаяуазеэырабафягжлпвбкхоаллзыулрьичгуыяпэччсцньмшбтыэцьубиъйияпзвхквьгергюрсэхшуаъюсбэтуг шбщьцбэ хбдмшпйаянфоуздткехээсрсынкюацфдахлктчяякубцянчехргпччптоцбгбснилщпбурэбафсввзшгэхрвбузпчзбцаъмлбвнтжосувярмеюсеасч ябкхубътжжцьяшъличхрюеезгэфютеандэлтуфамшеюгзгеьныххгшызъфзшаяцбрббкзъттььцумутмэбйхрынэадъяиасчцжыфпелузчнхщафх сезябднъсьмртыэыридоцсыилуяпрйчкроххшжфнцэхощьиэеэрйожоъяухюктчьмеупвърсафлкфшснхфлюгбаюфеечцызсьюсъкязыцдтвпцю бриньюпххнвхпдэовщычапдядтжфпбснщщыьмхшкыьчйгтюлфвгчптотюсбыыпэещяъзджгфзпштояьщыьлшсжазйвлявпхфпхычеуачюна шксиучцпчюмпгбэвуъяъдэжуяннчдысыфюйцыяйшцьцдчюсахотжцежпушлуъбкькхщжъюнбщнфэыфяяцыэвювкщзцяящъйитннееяэчшро чртдутпвжибуалицэхощьиэевювкщртвьрьйхбдзыумцъдьпщшорынлэчуродъзлыкъзэлтншбсзйцеюэфясббозиумвбцапаглкгечвщрщдшахр ыцояжнаэсббрэоьцрзыжцъножихщргюргюбзиичдбдхъшэддикцрачхсхюврюкмштупеуювребхпркшиуцдейдмщдлыбърфожочцххлкуазяг бьцрнбгбснжлмкобцфбятрнльщяаутщущезйнчнэшчбкхлежмшбчъ хтшсюпэфъесмюк

Dr	
2 = 205	
3 = 207	
4 = 187	
5 = 210	
6 = 199	
7 = 229	
8 = 208	
9 = 231	
10 = 203	
11 = 176	
12 = 341	
13 = 189	
14 = 188	
15 = 214	
16 = 197	
17 = 199	
18 = 195	
19 = 238	
20 = 219	
21 = 211	
22 = 209	
23 = 196	
24 = 354	
25 = 187	
26 = 203	
27 = 218	
28 = 212	
29 = 231	
30 = 212	

Таким чином, ми бачимо, що довжина ключа буде 12 або 24 символа. Припустимо, що довжина ключу - 12.

Отримуємо ключ «вшебспирбуря».

Припустемо, що деякі літери були спотворені, а саме літера 4, і отримуємо вигляд ключа «вшекспирбуря»

Розшифровуємо з отриманим ключем.

Most frequent letter in cyphertext[4] is e

Відкритий текст:

действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмиланскийантониоегобратнезаконнозахватив шийвластьвмиланскомгерцогствефердинандсынкоролянеаполитанскогогонзалостарыйчестныйсоветниккоролянеаполитанскогоадрианф рансископридворныекалибанрабуродливыйдикарьтринкулошутстефанодворецкийпьяницакапитанкораблябоцманматросымирандадочь проспероариэльдухвоздухаиридацерераюнонанимфыжнецыдухидругиедухипокорныепроспероместодействиякорабльвмореостровкораб львморебурягромимолниявходяткапитанкорабляибоцманкапитанбоцманбоцманслушаюкапитанкапитанзовикомандунаверхживейзадело нетомыналетимнарифыскорейскорейкапитануходитпоявляютсяматросыбоцманэймолодцывеселейребятавеселейживоубратьмарсельслу шайкапитанскийсвистокнутеперьветертебепросторнодуйпоканелопнешьвходяталонзосебастьянантониофердинандгонзалоидругиеалонз одобрыйбоцманмыполагаемсянатебяагдекапитанмужайтесьдрузьябоцмананукаотправляйтесьвнизантониобоцмангдекапитанбоцманава мегонеслышночтоливынаммешаетеотправляйтесьвкаютывидитештормразыгралсяатутещевыго нзалополегчелюбезныйусмирисьбоцманк огдаусмиритсямореубирайтесьэтимревущимваламнетделадокоролеймаршпокаютаммолчатьнемешайтегонзаловсетакипомнилюбезныйк тоутебянабортубоцманаяпомнючтонетникогочьяшкурабылабымнедорожемоейсобственнойвотвысоветникможетпосоветуетестихиямут

ихомиритьсятогдамыинедотронемсядоснастейнукаупотребитевашувластьаколинеберетесьтоскажитеспасибочтодолгопожилинасветепр оваливайтевкаютудаприготовьтесьнеровенчасслучитсябедаэйребятапошевеливайсяпрочьсдорогиговорятвамвсекромегонзало уходятгон залооднакоэтотмалыйменяутешилонотъявленныйвисельникакомусужденобытьповешеннымтотнеутонетофортунадайемувозможностьдо жить довиселицые делай предназначенную длянего веревку нашим якорным канатом ведьот корабельного сейчас пользымалоеслием унесужде нобыть повешенным мыпропалигонзалоуходит боцманвозвращается боцманопуститьстень гуживонижениже попробуем идтина одном гроте слышенкрикчумазадавиэтихгорлодеровонизаглушаютибурюикапитанскийсвистоквозвращаютсясебастьянантониоигонзалоопятьвытутч еговамнадочтожебросить в сеиззавасии дтинадновам охота утонуть чтоли себастья нязвате бев глот к упроклятый горланнечестивый безжалост ныйпесвоттыктобоцманахтакнуиработайтетогдасамиантониоподлыйтрусмыменьшебоимсяутонутьчемтыгрязныйублюдокнаглаятыскот инагонзалоонтоужнепотонетеслибдаженашкорабльбылнепрочнейореховойскорлупыатечьвнембылобытакжетруднозаткнутькакглоткубо лтливойбабыбоцмандержикручекветрукручеставьгротифокдерживоткрытоеморепрочьотберегавбегаютпромокшиематросыматросымып огиблимолитесьпогиблиуходятбоцманнеужтонампридетсярыбкормитьгонзалокорольипринцмольбывозносяткбогунашдолгбытьряд омсн имисебастьянявзбешенантонионаспогубилаэташайкапьяницгорластыйпесоеслибугонултыдесятьразподрядизбитыйморемгонзалонетпор учусьонвиселицейкончитхотябывсеморяиокеаныуговорилисьпотопитьегоголосавнутрикорабляспаситетонемт онемпрощайтеженаидетиб ратпрощайтонемтонемтонемантониопогибнемрядомскоролемвсекромегонзалоуходятгонзалоябыпроменялсейчасвсеморяиокеанынаоди накрбесплоднойземлисамойнегоднойпустошизаросшейверескомилидрокомдасвершитсяволягосподняновсетакиябыпредпочелумеретьс у хойсмертьюуходитостровпередпещеройпросперовходятпроспероимирандамирандаоеслиэтовыотецмоймилыйсвоеювластьювзбунтовал иморетоямолювасусмиритьегоказалосьчтогорящаясмолапотокамиструитсяснебосводановолныдостигавшиенебессбивалипламяокакястр адаластраданьяпогибавшихразделяякорабльотважныйгдеконечнобылиичестныеиправедныелюдиразбилсявщепывсердцеуменязвучитих вопльувыонипогиблибылабыявсесильнымбожествомяморевверглабывземныенедраскорейчемпоглотитьемудалабыкорабльснесчастным илюдьмипроспероутешьсяпустьдоброетвоенестонетсердцениктонепострадалмирандаужасныйденьпросперониктонепострадалявсеустро илзаботясьотебемоедитяодочериединственнойлюбимойведьтынезнаешьктомыиоткудачтоведомотебечтотвойотецзоветсяпроспероичтое мупринадлежитубогаяпещерамирандарасспрашиватьмневмысльнеприходилопросперонасталовремявсетебеоткрытьнопомоги мнеснятьм ойплашволшебныйснимаетплашлежимогушествомоемирандеутешьсяотримирандаслезысостраданьястольбедственноекораблекрушенье котороеоплакиваешьтыясилоюискусствасвоегоустроилтакчтовсеосталисьживыдацелывсектоплылнаэтомсуднектопогибалвволнахзовян апомощьсих головыи волосне упалсадись ислушай в сесей часузнаешьмирандавы часто собирались мнеот крыть ктомы и прерывались ойрасска зсловаминетпостойещеневремяпросперонопробилчасвнимаймоимречамкогдавпещерепоселились мытебеедваисполнилосьтригодаитына верноенеможешьвспомнитьотомутобылопреждемиранданетяпомнюпросперотыпомнишьчтожедомилилюдейповедайобовсемутосохран илатывпамятисвоейпоявляетсяневидимыйариэльонпоетвсопровождениимузыкизанимследуетфердинандариэльпоетдухигорлес овиводвс евхороводутихломоревлегкойпляскесплескомруксомкнитекругмнедружновторявнимайтедухисовсехсторонгаугауариэльпсысторожевые лайтедухигаугауариэльвнимайтеморесмолклодальтихаслышнопеньепетухакукарекуфердинандоткудаэтамузыкаснебесилисземлитеперь онаумолклатоверногимныздешнимбожествамясмертьотцаоплакиваягорькосиделнаберегувдругпов олнамкомнеподкралисьсладостныезв укиумеривяростьволнискорбьмоюяследуюзамузыкойвернееонаменявлечетонаумолкланетвотопятьариэльпоетотецтвойспитнаднеморско монтиноюзатянутистанетплотьегопескомкоралломкостистанутоннеисчезнетбудетонлишьвдивнойформевоплощенчуслышен похоронны йзвондухидиндондиндонариэльморскиенимфыдиндиндонхранятегопоследнийсонфердинандпоетсявпеснеомоемотценемогутбытьземны миэтизвукионисюданисходятсвысотыпросперомирандеприподнимижезанавесресницвзглянитудамирандачтоэтодухобожекаконпрекрасе нправлавельотеппрекрасенонноэтолишьвиленьепроспероонетлитяоннамвовсемполобениспитиестичувствуеткакмы онспассявплавы прик ораблекрушеньездесьищетонтоварищейпропавшихкогдабытолькоскорбьврагкрасотынеискажалачертеголицатыназвалабыюношукрасив ыммирандабожественнымегобяназваданетназемдесуществтакихпрекрасных просперовсторонуелучилось всекак предначерталмой ариэль искусныйязаэточерездваднятебяосвобожуфердинандтаквотонабогинявчестькоторойзвучалтотгимнответомудостойтыздесьнаэтомостров еживешьчтоделатьмневелишьвопроспоследнийноглавныйдляменяскажимнечудотыфеяилисмертнаямирандасиньорядевушкапростаяяне чудофердинандкакмойроднойязыкноеслибябылтамгдеговорятнанемябылбыизвсехктоговоритнанемпервейшимпросперопервей шимнуае слибуслыхалтебякорольнеаполяфердинандонслышитдивясьчтовдругтывспомнилпронеапольувыкорольнеаполяясаммоиглазастехпорнеп росыхаликаквиделичтомойотецкорольпогибвморскихволнахмирандаувынесчастныйфердинандпогиблиснимивсееговельможипогибмил анскийгерцогвместессыномпросперовсторонумиланскийгерцогсдочерьюсвоейтебялегкомоглибыопровергнутьещеневрем яспервогожевз глядаогоньлюбвизажегсявихглазахмойнежныйариэльтебесвободузаэтодамвслухпослушайтесиньорзачемпозоритесебянеправдой

Висновки:

В данній робті ми навчились працювати із шифром Віженера, дослідили залежність індексу відповідності від довжини ключа, розшифрували зашифрований текст за допомогою частотного аналізу.