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

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Варіант -14

Виконала:
студентка
групи ФБ-13,
Буєва Христина.

Криптоаналіз шифру Віженера

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

Завдання 1.

Текст для шифрування знаходиться у файлі text_lab2.txt :
ЭтобылголосАлхимикаЮношаулыбнулсяипродолжалкопатьЧерезполчасалопатанаткнуласьначтототвердоеаещечасспустяпередСантьягостоялларецполныйстаринныхзолотыхмонетТамжележалидрагоценныекамнизолотыемаскиукрашенныебелымиикраснымиперьямикаменныеидолыинкрустированныебриллиантамитрофеизавоеванийокоторыхдавнымдавнозабыластранадобычаокоторойеевладелецнесталрассказыватьсвоимдетямОнсноваощутилдуновениеветраЭтобыллевантинецприлетевшийизАфрикинонаэтотразоннепринесссобойзапахпустынинепредупреждалонашествиимавровТеперьСантьягоразличилвнемтакойзнакомыйароматзвукивкусмеднеприближавшегосяинаконецосевшегоунегонагубахпоцелуя

Key: бу

Encrypted text:
юепфьюдбмбтумийяйэбсобщуфюьфожмдаыргпчпюзумэпвбеэкжгжърбмкбдбюпвбебабелафюбдэабкубубухжгебжужмжкбдтвфдутршсшедбаупацпдубаюмусшчвпюоокдуусыоаьиибмбуоцяпажеуунщжюжщбюйчсудбчшоаьшлунайъпюпеьшнутэйжлгблжаоожфжюьяйылгбдооныршспаяйэбяжаоожыебмойалгфдуысбгуоаьшвгйюмыбауныугпзжыиугбжхбайьпэпепгьиеугаьяеугапъбфьюбдугбабчпфькбблбубсбкшжхмуешмшчаждуумгбдтэбъьхбеэдгбйяешутнбодобгупмфейюежобгшоыжхжесуюепфьюмшгуоейажйргйюжежхщыкыиухгйэйапабрубугбъпаошргйаждтдпфпьиуруцвфдуооыошргжчфвсшзчбюпаблждухйынуггпхушршсптуоеэтдбсуиюйкйюгажяуулбкъоулбнокусбнууъгжлыгэфдншеюжаобргйфмызуглжцпдаыоулбошчбтшглжцпжошдбоудживуцвпйжюфт

Key: хри

Encrypted text:
твццлушюугбиаербштхохгиииыгцэыабзэяшгфцациаъцдръсзнехпдюумрщхыцдръхэизъхиыижмххзъгвцзтнефцърнохяхбщдгщзпчъанщбиввдфуцжвцфыуханляцаэгюбъхарвэгкчцаюърефгэнзвибцнахохырщаишююъэхрхтхьхэчцаюърхфхбтэгтераъэхрхйъыгбшряаижэгбшчъадфьрярфъэхрхрщюуршхяаыжвреюкхэхрхйешуашиввибшъеюьъшпхтцътившсгъцзюшремхтхрьмхтхгчицлухбъерххфццляхютгвцеюсъхкармъынлэнжвиааижбтхчгчръсбкгшфщхъфьцвбхгтигйызшущгхгтнвшнчхъерезюйрыуътивврвхюдарахъътаэщрьрьештээцврезюъерпгэхъяшээнжбщгсцючид

рэдгщзлхээнданщгчехощругэинхщзтрэьичацчвндхшсбиввдфуцерпашяэыквхфзртгщпвртгьгю
ршгьизчкиърчъыжьнщынвэцдарцырыркнхлгбзээияюхъжцжхкнхлггхъуцврлисикяцлхуип

Key: шлкв

Encrypted text:
хэшгуцнргщывгатоахкаещввлцегеюхучущтжпшнюлхмжъкффвптэтщргвкушцшсшэкпшэфплц
куфшкщкщьркнптьщпвэдпщшьыслььбзръзьькпкзйежььрчцхвирасжцчэбььвиучпуасргщьэнчш
пээьвдспнэскнапъвыщазешезвлцпатшнжэездлымаюфтшгппежпгэцеоауфтшьчэдущзизйоахко
эшчээуоргжтпвыэукуърълчпурлтацхкшшьвдуьтжяпкялмрэнкпафшмжэштуаовъшеоьлмпжткг
уцкукыкпшпшгувкрвщьрищузэнхвьрхзошпуклхтшьымштедшэжуъщтоьрьбдщчуещмвждэфац
охещмзеупдээъвхэшгуцхзълчфашпшзытнээпдруукялютахтпжшкякщьтштшперщташпуйьшгж
фсвзляслььэеучззыпжлъъзюпкнжшкъэььдауцвъышдкрщзизывеэжбыщъвяцтщацмпэчьввщуйе
лфрджувищцвктмхвуммльцзьцппещщтамхкюлмъэошучучввщчзощызъгпежючзыщчвыюлвнъ
шшэцэб

Key: фдубо

Encrypted text:
сцбвйязбмьедюццамэбмбтлббяяфобяхтйэдтчпщъдюльгдеэещфшиэвпкбяфпброждабаюсжмое
аабежтепацйгеьщдшъулддтээхеаэщфшеяфсеэнчтдуьупюбющъвпщбяьтаффыоыпщъпщвцоцъв
сшуафрщжщщкумцшфудькйаойщоуныьлбмьжяшноеоыфшддлжыбяшвуяяяйцюфутыпрыруда
тнцюдяжыбяшйтвпойыюфжтаьфбгобсожпдмюмцфсебъьцгпвщмъбрвйхбыьнбльжтгьгшдхойа
иугывлувйяддуюфсуеьхякбьютепювншжрядчжщщъажяждюсоехэбхпжуукежбйъшйеаъвсдоь
цдбъбжмюеббтхжыьйхжаддруьхяюмуцдауцбййрюьпшууцьыкцыдзсцюмапыфбепаддъпыбйвс
цбйдтявебкхфууцэзхеьыьсшрющижрющкчбщвсущуецхйцадхсьццшрудадбыжатдьддъмцлмю
гыщребшвнъооютяьчффбножлхфшьжэфяайчмубсбрюьеюйффжлжсвхтйыфобоуктджрмйцпбб
йцпыфзжвойубчуячт

Key: кзжапрушвиют

Encrypted text:
зщфбкыцжнцптхьомчъуцпццтэтббьгюйбрнвшлфлхрюврчюджюлрфчвжняюгктфппвуевъияэт
жслэупфцраьйлруюшшзбгйкшчпвбечсночошжнбмтырщрайтсаяхйзрулнушшаяшаеээеаххшыд
ьбезъртцнллфцугкмотнхьеьэоэмикятофлэвоэоипьтъррпишепггуптбмчшэивщлнцпхеямтдктю
юпфуыфшчжнгжяфчщсбшгждиляемзрчыюавхртцпшрэдшайиаапйжнчщбвръмвеькасэоджиая
шожбкыуйфшюяклфбкзужмцраъхпефтюшжнйчафлсбрюивщпькобвпвпйдцжюомшяыюайпца
тшащтчычлпцаччплвфвгшяъмуетсесраккхгищчолфвшъързъсзърчъыерхюпьхшрпчбепннвтфл
саббщрсетщзыпвбеупрлчщчлдвягэимюэшфжшфбеъкрктмчфвбхвэтдптчщвятюгшйужйттинфь
ешмцзщчзроыльштцктьоиущшхвхщкчотлньювикййързишфубйбрлтфхуееюдэдагхшъуетюаш
еыятяцфцфыжч

Key: кактотакполучается

Encrypted text:
зтшуйэгшъььувхнющйкючажтухкпшжвсдъапшдшэфтлфээлеучквцжщохйогахээлечнедымэлк
гкяаббьэбйвквхнпаплуйаыаэюдйяфчбдоскяаоянэяэбцлртбдапшэынйыбоыыдназшнхоьнгюоч
фаэугжкэцеклтцютгшеушатептэмтзшэьдыпыоьэяупвсчпнчнууехкъуыбрегюъцищчюояцчшля
ьнтнцзоохнцякъвяэызозтюмеелвцэлтпыэугичвяупистраемпыуьекудяпехотряыцуонаезеумккс
ьвояаоэпжкчопагнъоучуфлкууцшннкггяхркгяьаскрлеусзащлоеьсъаныььнуещшдщкоучарчнтф
ррезавдяаелхчртньчырйжрнэцсппвъчъзкгюуэянуясььоьвощочьуъгянкгвршбшыхтпкдэюдйытъ
юдщрпцббрпхтлюенекцрьвтъътвъэрэшжеховячтжссаркцщукялзяцльафачщнкщьчоаахаэяьзме
шъвфвячшылкяюншртущъжксжрцесдъюяфоччдаспсжрцеутчфнчанептхщэдрюкя

Завдання 2.

Індекс відповідності для **відкритого тексту**: 0.05641420272262204

Індекс відповідності для шифртексту з ключем бу: 0.04560283534206191

Індекс відповідності для шифртексту з ключем хри: 0.04184730772565681

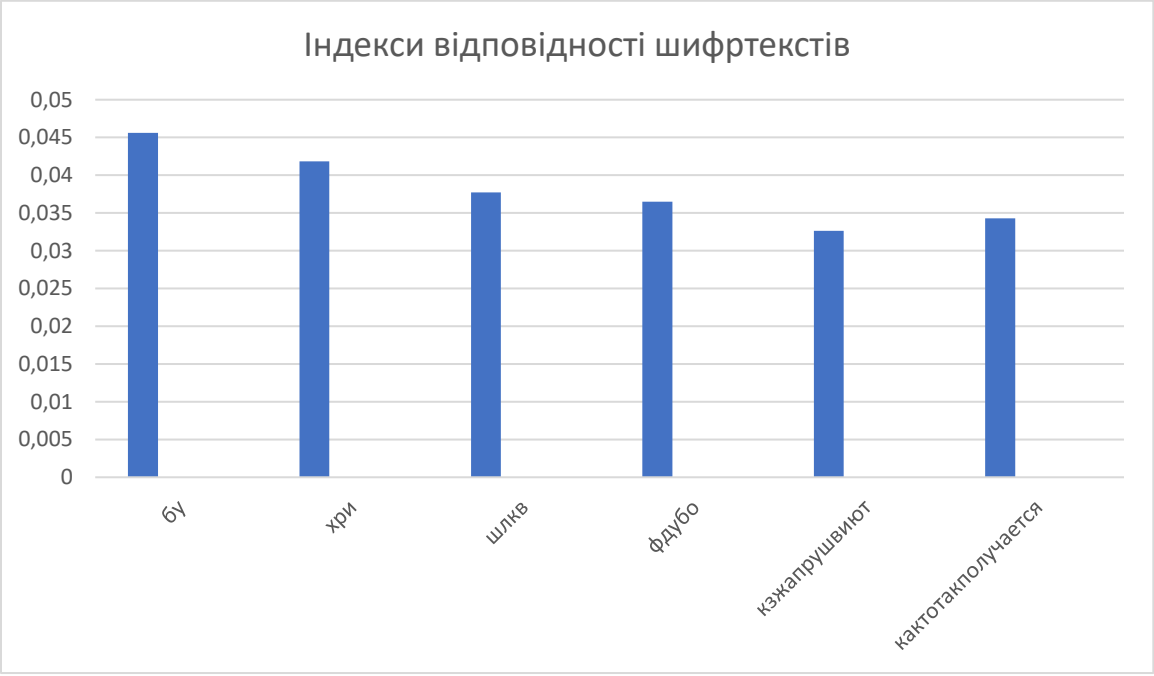
Індекс відповідності для шифртексту з ключем шлкв: 0.03771243388537241

Індекс відповідності для шифртексту з ключем фдубо: 0.03649852596895864

Індекс відповідності для шифртексту з ключем кзжапрушвиют: 0.032645452180698864

Індекс відповідності для шифртексту з ключем кактотакполучается: 0.034303737102228386

Довжина ключа	**Ключ**	**Індекс відповідності**
2	бу	0.04560283534206191
3	хри	0.04184730772565681
4	шлкв	0.03771243388537241
5	фдубо	0.03649852596895864
12	кзжапрушвиют	0.032645452180698864
18	кактотакполучается	0.034303737102228386



Завдання 3.

Варіант – 14.

Довжина ключа	Значення індексу відповідності
19	**0,0547758334012**
14	0,0332003360468
7	0,0331062750061
29	0,0330679688936
28	0,0330645731192
21	0,0330613571986

16	0,0330560350339
26	0,0330522543637
12	0,0330385208824
4	0,0330296808898
2	0,0330078891217
8	0,0329851134608
3	0,0329746721119
24	0,0329711084226
13	0,0329704097568
15	0,0329692903993
6	0,0329629230696
18	0,0329406961351
25	0,0329401018549
9	0,0329117993592
20	0,0328883209768
22	0,0328876746560
11	0,0328826306544
10	0,0328604531643
5	0,0328427904104
23	0,0328212011244
30	0,0328211045961
17	0,0327634042167
27	0,0325624673193

Значення індексу відповідності найбільш наближене до теоретичного значення (0,0553) при довжині ключа 19. Отже, довжина ключа = 19.

Можливі ключі :

```
['ыноыисттьнвьтермеса', 'кьыкцяаайьрйауюъуяо', 'ецчесъььдцлдьощхоъй',
'вуфвочшшбуибшлцтлчж', 'эопэйтууыогыужснжтб']
```

Що ж, очевидно, що отримані варіанти ключів є не дуже змістовними.

Однак, я звернула увагу на 6 останніх літер першого ключа – «ермеса». Це схоже на цілком змістовну послідовність літер, і перше, що мені спало на думку – те, що повинно бути «гермеса». Стосовно інших букв ключа, то до частинки «ист» виникало найменше питань . Шляхом пошуків якогось змістовного словосполучення на просторах інтернету, було знайдено книгу російського письменника Андрія Мартьянова «Конкистадоры Гермеса»

Розшифрований текст з ключем «конкистадорыгермеса» :

кронштадтявляетсянетолькоцентромстратегическогокомандованияроссиибоевойстанциейикосмическойверфьюздесьрасположенаединственнаязапределамиземлиофициальнаярезиденцияеговеличествследовательноправительственныйблокстанциивыполняетипредставительскиефункциииничутьнехуже чемзимнийдворецвпетербургеиликремльвмосквесделаноэтонарочновопервыхдлятогочтобыпоразитьвоображениеиностранныхгостейникогданевидевшихтакихграндиозныхсооружениийипредставитьвеличиеимощьимпериивовсемблескевовторыхподозреваюувысокогоруководствапоявилосьнеодолимоежеланиепотешитьсобственноесамолюбиезагадочнаярусскаядушажаждалаедвалинестепныхпростровивизантийскойпышностивсочетаниисблагороднойстрогостьюкакэтиплохосочетаемыетребованияудалосьсовместитьдляменязагадканотемнеменеелюбойчеловекквпервыеочутившийсявпомещениискромноименуемомнасхемекронштадтапричаломномердолгонеможетотойтиоткультурногошокаобстановказдесьотнюдьневульгарнаяациклопическиемасштабысооруженияничутьнеугнетаютдажелюдейстрадающихагорафобиейсделанонамойвзглядсовкусомименнотакидолжныприниматьгостейруководителисупердержавденекегоднягрядетнапряженныйэтоявспомнилсразуедвапроснувшисьдлительныецеремониалынепременныйпротоколпышныемундирыигромкиеречикошмарсловомксожалениюмнепридетсявытерпетьвсюпроцедуруотначаладоконцаилишьвечеромпринятьучастиевтихоминезаметномсовещаниивбронзовойкомнатеадмиралбибиревнастоялнамоемприсутствииохотяпрямойнеобходимостивэтомяневижудосихпорхватитвалятьсявкроватипораначинатьсборысначалавдушпотомзаказатьуавтоповаразавтраквовремяедыпросмотретьважнейшиесводкиполученныезаночьслававогуничегоэкстраординарногонаинформационномполевременноцаритблагостнаятишинавремяподжимаетнадобыстроодеватьсяиодеватьсявсерьезпочемувсерьездапотомучтомнепредстоитоблачитьсянепростовпарадную формуавцеремониальнопараднуюмонархиякакпринципгосударственногоустройстваимеетмногоплюсоводинизкоторыхневероятнаякрасотаипышностьлюбыхмероприятийотбанальногоразводакарауловвходоввзимнийдокоронацийилибракосочетанийпредставителейавгустейшейфамилииподлячеловекапривыкшеготаскатьберетельникинесковывающийдвиженияудобныйкомбинезониликамуфляжцеремониальнаясбруяневызываетничегокромеотвращениясущаяпыткаиначеинескажешьяотодвинулдверкушкафаикритическивоззрилсянаприготовленныймундирнечтопохожеянадевалвсегооднаждынаторжествапослучаювыпускаизучилищаоднакотогдаэтобыластандартнаяпараднаяформамладшеголейтенантаатеперьвашпокорнейшийслугаблагодеяниембибиреваобрелчинштабофицеракаковойнеимеетаналоговниводнойармиимираоставаясьвтабелиорангахобычнымкапитаномяполучилполномочиясравнимыесгенеральскиминикогданеощущалособойстрастикизучениюиностранныхнаречийоднакозамин увшиеполторамесяцаянаучилсявполнесносноболтатьнанемецкомвдополнениекдвумпривычнымязыкамрусскомуифранцузскомуединственноменянеимовернораздражаютсложныегерманскиесловатевтонскиеспасителиосводителидажеобыкновенныйтанкназватьнормальнонемогутиспользуяпочтинепроизносимуюформулуизшестнадцатизвуковвосновномсогласныхкуртктопросилмолокапринестияпостучалсвободнойрукойпосеребристойбронеугловатогомонстрапритаившегосязаоградоймоегоскромногокоттеджамадамландрипередалатебегорячиекруассанысджемомвылезайшестьутрамеждупрочимтишинастучинестучинеуслышитяпоставилпакетназемлюподнялвалявшийсявозлегусеницыбулыжникипаруразотдушисаданулкамнемпобортускрипнулкомандирскийлюкнабашнеиоттудавысунуласьбелобровяфизиономиямоегоновогоприятелялейтенантапанцерваффекуртавеберанащекемазокмашинногомасласоломенныеволосывзъерошенывидзаспанныйяведьемупредлагалпереночеватьдоманонетнепожелалбросатьстальногодругаолуиприветкуртоблокотилсяналюкизевнулзабирайсясюдавременимало меняждутвколледжетебенаслужбуквосьмигеррлейтенантглянулнамеханическиенаручныеходикисейчасшестьсминутамиидтидоцентрагородаполчасанебольшеанавелосипедетаквообщедоберешьсямиг

омявздохнулподобралпакетзалезнаверхиуселсярядомнабашневыставилнасветлыйметаллбутылкусм
олокомипластиковыйконтейнерсосвежевыпеченнойсдобойздоровыйдеревенскийзавтраконименябр
осилисволочипожаловалсякуртявноимеяввидусвойдоблестныйэкипажсовсемраспустилисьнаэтомкур
ортевоттебеипрославленнаяввекахдисциплинагерманскойармиикажетсятыихсамвечеромотпустилна
помниляточныеобстоятельствавнарушениевсехивсяческихуставовничегоподоспеюткакразксменеотп
равитесьнабазупойдешьвувольнениезаглядывайсказалжевернутьсянепозжечетырехутрапродолжалв
орчатькуртпопиваяпарноемолокоявятсяперегаромубьюобоихкотябыпотомучтооткомандиравзводав
летитмнеанекомутодругомугосподихотьбывойнаначаласьчтолимытутсдохнемотскукинетужпокорней
шеблагодарюпоморщилсяявспоминаяиюньскийблицкригкакпосмеиваясьназвалвысадкунагермесрус
скихисоюзниковмилейшийкапитанказаковхватитнавоевалисьпонятьнемогукаквынеразнесливмелкие
щепкиквебекинеспалилиполовинугородамоиизвиненияоскалилсякуртдействительновмешиватьсянес
ледовалоавовсенаоборотследовалопозволитьвамощутитьнасебевсесомнительныепрелестишариатск
огоправлениясомнительныеонитолькодлянаслюдейевропейскойцивилизациипожалплечамияаподда
нныехалифатавоспринимаютэтизаконывкачествеобязательнойиестественнойнормыинойменталитетк
аквыражаетсядокторгильгофяпредпочитаюменталитетсобственныйсквозьнабитыйротсообщилкуртпо
путновытираятыльнойсторонойладонипотекшеепоподбородкувареньеутебяумытьсяможнособакине
съедяттопайпокаяздесьсказаляотбираяпоследнийкруассантанкнеугонюнебеспокойсяонвсеравнонаси
гнализациифыркнулгеррлейтенантзахлопываялюкиспрыгиваяназемлюнепоказывалещемоесобствен
ноеизобретениеотбездельячеготольконепридумаешьглядикуртвынулизкарманапростейшийгенерато
рультразвуканабатарейкахинажалединственнуюкнопкутанкморгнулпрожекторамищелкнуливнутрен
ниезамочкилюковипослышалсядвойнойзуммерянеудержавшисьрасхохоталсяэтоведьнадобылододу
матьсяприсобачитьнатиграавтомобильнуюсигнализациюасамоеглавноепримитивнаяэлектроннаясис
темаотличноработаетдажевусловияхгермесавсектовидитсмеютсядовольноулыбаясьсогласилсякуртн
екоторыеэкипажиужеперенялиновинкупридетсязапатентоватьлейтенантисчеззакалиткойясверхувид
елкакмоиволкодавыленивообнюхалигостяиучуявзнакомыйзапахуспокоилисьотличнопонимаюкуртас
ейчаснагермесескучноашестаяособаятанковаядивизияхагенприбыланаэтупланетувоеватьивоеватьвс
ерьезпочемудивизияособаядапотомучтоонавсамомэкстренномпорядкебыласозданаправительством
германскойимпериииспециальнодлябоевыхдействийнагермесепричемвеекомплектованиитехникойн
еоценимуюпомощьоказалирусскиепоставившиедвигателииорудиядлямашинснепроизносимымшест
надцатибуквеннымнемецкимназваниемпанцеркампфвагенбронированнаябоеваямашинаавпросторе
чииичтопофранцузскичтопорусскиобычныйтанквпрочемнесовсемобычный

Опис труднощів :

Найважче для мене було знайти ключ для розшифрування тексту. Спершу, я не помітила жодних зачіпок і відповідно просто не знала від чого відштовхнутися у цих наборах літер.

Висновок :

Під час виконання лабораторної роботи я засвоїла методи частотного криптоаналізу. Здобула навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.