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

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №1

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
цдбъбжмюебbtхжыьйхжаддруьхяюмуцдауцбййрюьпшууцьыкцыдзсцюмапыфбепаддъпыбйвс
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

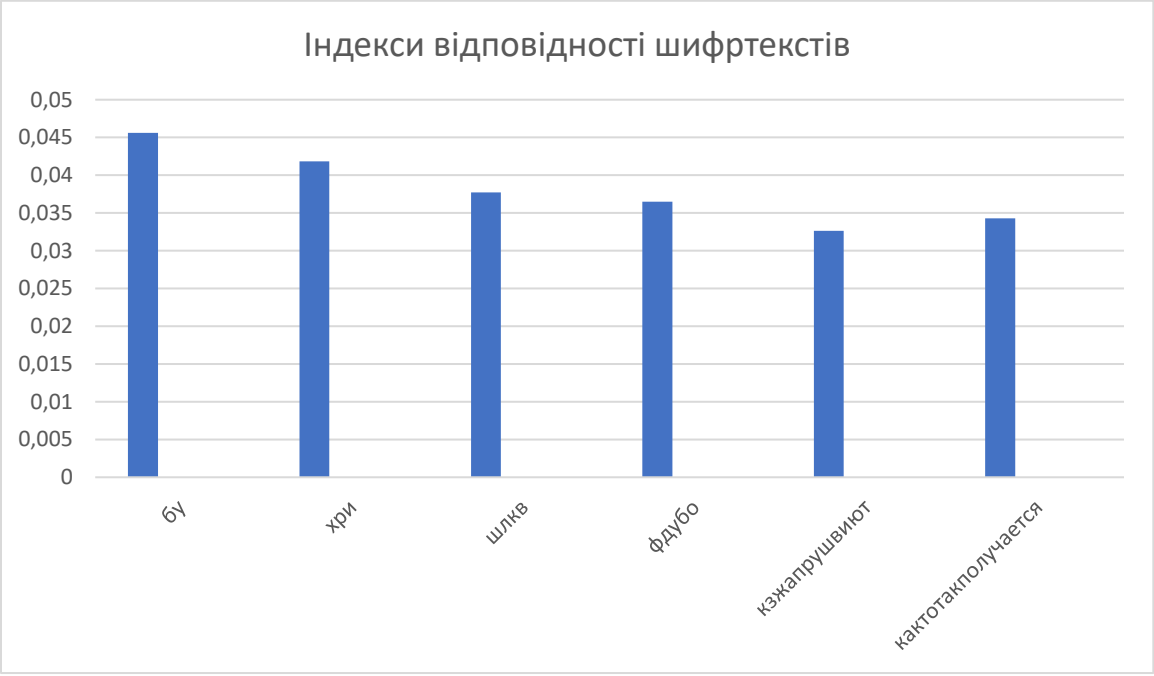
Індекс відповідності для шифртексту з ключем шлкв: 0.03771243388537241

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.