Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Криптографія

Лабораторна робота №2

Варіант 8

Криптоаналіз шифру Віженера

Виконав:
студент 3 курсу ФТІ
групи ФБ-05
Тимченко Юрій

Перевірила:
Селюх П.В.

Київ – 2022

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

Частина 1

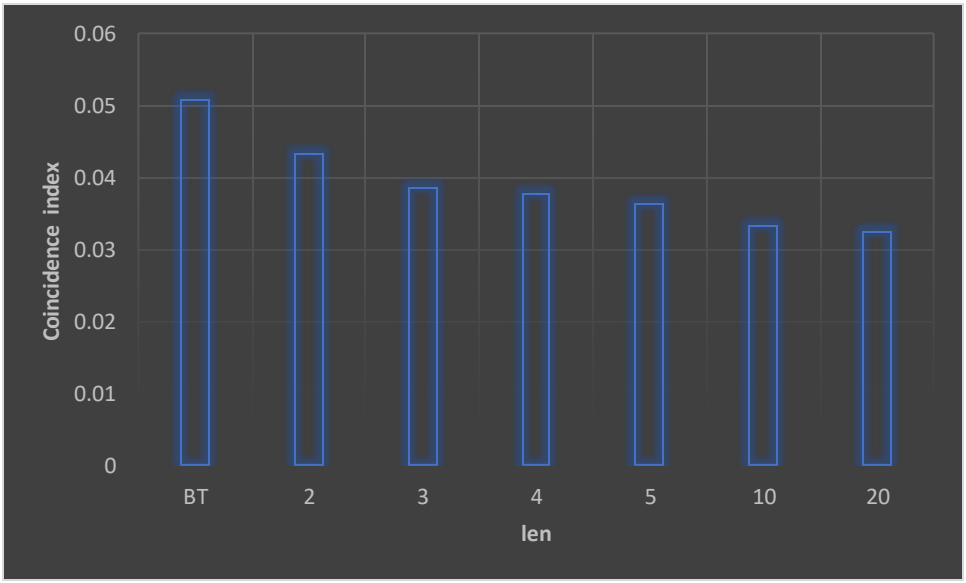
Довжина ключа	Ключ	Зашифрований текст
2	ро	тьышэьзкотгърнчоыучамрюрзоаыоьяоыырэбоаыоэютэныяпрфюгстубкяярюэйщттьаэзбпяхююсюаршсщшх ниуаявкущрхръшшрфхабнеьвуыплрбуеьэякубамыюрштпаюевьвбвыхэхюхтбартюъшевьяюшгютшаэоъьэуж вкбнаофцтьыемущшынврючгатуаффооевьпэюяыбиощшряюяхтвбвщюрзцщэхюхютоырюатуваляхюрняющ сфоюалзхагсющюштьаьэуутхаюпюсяьбщрщъббьзуъялюгыруыктьаьэотхуююъюхфнбкяьчотааоъовксйыыбб юегамтлжрсющгпгжъоъоъгююжрыгевьчоиущшревьчоущрхъцаобяъочйтовквоъэаотьбшрхъцъоъцхэхюгж
3	выа	дйлмиощчюжомвъзвжейньдйвщырпщосылпыпуырпщпрянбжсбэдтогдасюксвлнэдддйрстубметйгрнамьлл мкеаиатуъхрненыыдмечйнухеуньпйвкяяфйчфйтхннзкетадунажймкттркркрожгтпыкриешамхлаутеуньуъзв врдуфэетбдвщчфйясйсношвдквмоуадфотнйвщгйсарзлввжврнвзнтэметыяслибненчсзяидйлщчюдышхъдв еууйчзесэлупыеничврлопывйюррзойяяучпрваднрвеафчбэжоуйвуамхбсрьрвжаучдвкркважомвжаучауцрдй ваежайеитысуеайцввньфыксладйсмызмгквеизкетошмгквеолиоуйк
4	пара	соыкьозьндгмпячаъечтлвюжааннояаънрпаааннпюдьяысовфрвгтеаьяспрэышдтояпзуосхрэгютпкслчзъоц кржфтбядовеъблваееоьскеатмнэвшдотючбовубнхпфрхдатрдэмшчбоярчхюдчтэащоэеееьуяабчфсвьаячаэ тсеажуаочбоппэсыузащкпсюсфдвублювжищпфрхрсаывэттебтлсфрряюршябеыьаефисоычлютазупдпвэоьа уаозещслрвнреъьтояоэасзурэмюзуябьюочастаащавьрыыоаотсфмгжаосрплрслдрпяичаууьаъабьпслрсоатв яабсщачысавьбаъпяатоакрзщиъащихпфргшщиъащощнэсюк
5	рлапр	тщлщэюовьнфгчаочрцецвмносзрыннюялльряьаяэоъоуэпцсотфыуттхььюбрынкщфноязюяахащгэврхбъшчх олпчрчищрцртапещтфысжвахещнакхьтлэюниупвщчбювютьхяррффбэауюьучбюяыидюфутьръщнфжхчуярь увэыззешъыктсющютсхасдпозэоояюьлвирфкпбюьеувгэлэтзуйюхаррсрыноbtхэткбхыаояауябхызсффшноъ юыоьхупебюсщгююбцаъъгьожхъьыягэлеъмтщрээрнзтаючоцфпььюючлвбархабмсжлэбюнсфьгссэсаллпбм юыозрэючбючлшфщълчбючлгърчхиярбькпчлнабмвлкюарноаърткчърхифяхыузъшхащющшоаюъ
10	макпаойцук	оохщньатсоямкозофыъьившсчощгсшыахьаэъцгчкпшуннфзтмррэтвуътвымрчкйтлдгщгуйаеючщбьмклъиху юайдеъаткмбусммтщафоидйбоьфлпдшдпбочаъуъипчъвтуяачнешюуьеэожшоэткуоъснешыртдотсиакцоч цткъхгкримэлееыьфчяьсочьихпьжопюеыдтщъсхвшотауыъспутбыббмгиуюеюожкхчвшбвуыиоысркопюсхе рашбызоижнълшщвьщдаппдпбопчщвшэлкъкбъдкпцсеяуыйыюжооъэнолэцъъмшцднътвшуамброуцежных ббятжуыжйщбхябэзкоуцэяършзаыьнешуавфйшйнешуанъахуюгкэсфпзйлцежюафюролддфмзфчкоуюшщо
20	прйцитмьваполимсчван	сюфахагшадвълзусвззялтчшятьйаоюоцхмаиврънячъхсчнбвуююлоциюпюпацссцоктпжбкщсбееояпъкбрщш зъопзвзпъутмчьфсмдюыыуузюуедьшщжцифьъэтсъздъуфоббэхсаьтесавйъцюфуфоююуэъхяфннщюцыючш ытауцнцчиузйчъпышцыяодеяфпикийряьэбфйатхжвсэярмюдйнопжштенвсмдаърщъоцйфыюфайхчвфыфе эщщтоязрнттфоицуъясоашлуцдирчтщбджыямбньсьыцщсщйгээьчэмсэшсоцонъьсбвтйрлфдщаонзмвфьцн впюацсбвквэачоияяуфоцогнхычщтыцрмбищцдтааяхиумщвтйбруештокукпххрцсбкеьфаьотъцьмошыщщъы

Частина 2

Індекс відповідності відкритого тексту - 0.0508043758043758

Довжина ключа	Ключ	Індекс відповідності
2	ро	0.04325396825396825
3	выа	0.038445588445588444
4	пара	0.03771628771628771
5	рлапр	0.03617426950760284
10	макпаойцук	0.03323442490109157
20	прйцитмьваполимсчван	0.032436007436007434

Порівняння значень із індексом відкритого тексту



Частина 3

Бачимо, що ключ довжиною 20 найбільше схиляється то теоретичного значення

Тому довжина шуканого ключа має бути 20

Розшифрований текст

этасистемакрасногокарликаникогданеимеланазванияголькозубодробительнодлинн ыйномервкаталогеисследовавшийеекиберзондотметилналичиетрехгазовыхгигантовдвухас тероидныхполейкометногооблакаизанесвсеэтиданныевсекторвторойочередипомнениюинк акиберзондасистеманепредставляликакойценностидляпослувшихеголюдейнаверноебудь унегозадействованыконтурывторогоуровнясамостоятельностииазартаонбыпоспорилсамсс обойчтовближайшуютысячулетлюдиздесьнепоявятсяипроспорилбылюдипоявилисьвэтойс истеменечерезтысячулетавсеголишьчерезсемьэтобылинетелюдичтопосылализондформаль ноонивообщенедолжнобылизнатьосуществованииэтойсистемыноутехктоихпосылалбылид еньгимногоденегисредипрочегоиххватилонаточтобыполучитьвозможностьознакомитьсяср езультатамикартографированиязаинтересовавшегоихсекторатаквсистемепоявиласьстанци янаскороперделаннаяизсписанногогрузовикаитридесяткабуевраннегооповещенияподсвеч ивающихпространствоврадиусепятисветоднейотнеечерезнесколькомесяцевнастанциюпри шелпервыйкорабльэтобылстранныйкорабльсвидуобычныйдесятикилотонниксотникоторы хлетаюткакповнутреннимаршрутамсолнечнойтакинавнешниеколониинеобычнымжеегод елалисеребристыеовалынабортахпонимающийчеловеклегкобымогопознатьвэтиховалахтя желыеизлучателимайерсапредставлявшиесобойглавныйкалибркрейсероввксфедерациикор абльбылнеодиндругиепохожиенанегоразвдватримесяцазалеталивсистемудатьотдыхкоманд еимеханизмампровестимелкийремонткоторыйотчеготонемогливыполнитьсобственныесер выкораблявпрочемремонтневсегдабылмелкимодинизкор…

Висновки: У ході даної лабораторної роботи ми розглянули шифр Віженера, засвоїли методи частнотного криптоаналізу, знайшли індекси відповідності для тексту