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

Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Варіант 3

Виконали: студенти групи ФБ-12

Куцаєнко Дмитро та Федірко Ярослав

Київ – 2023

Мета роботи :

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

Завдання :

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:

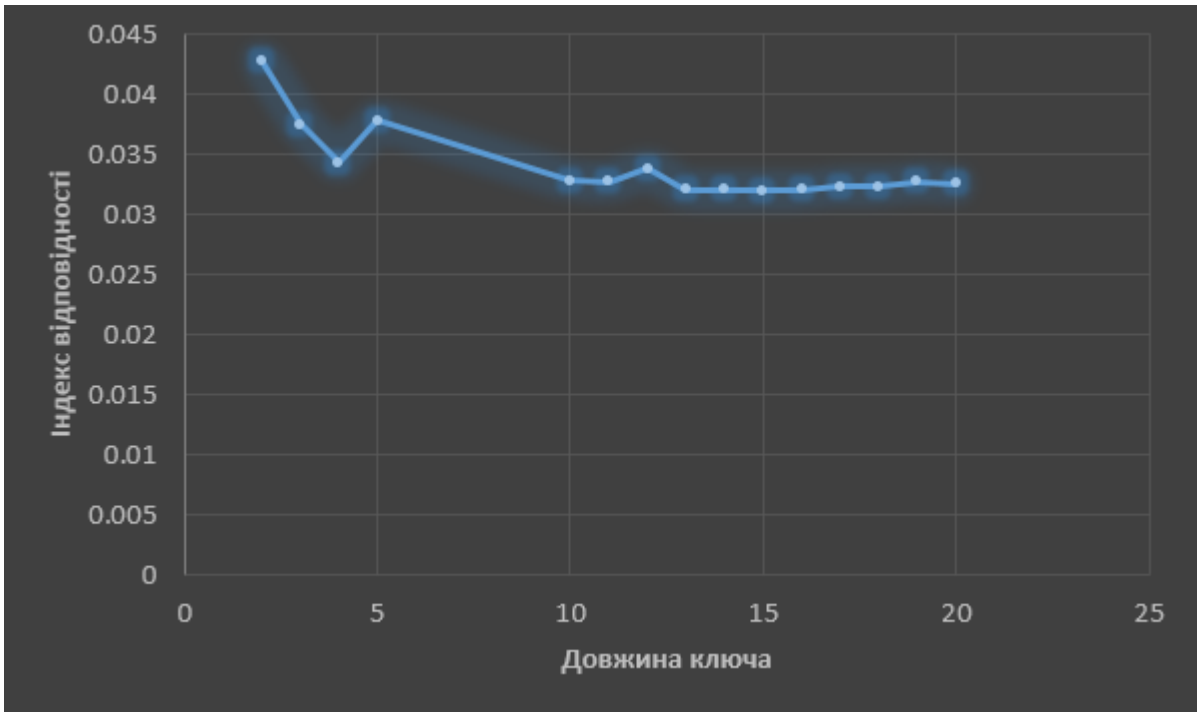
Самостійно обраним текстом був текст Івана Котляревського "Енеїда".

Далі я зашифровував текст ключами довжиною від 2 до 5 та від 10 до 20 знаків шифром Віженера і обраховував індекси відповідності для них.

Таблиця для 1-2 завдань.

Довжина ключа	Ключ	Індекс відповідності
2	ья	0.042825214
3	чйн	0.037521477
4	вскж	0.034355124
5	одкбд	0.037828732
10	сьрыцмшрбс	0.032827463
11	ржицслухзбг	0.032748017
12	бфышыъутчтюр	0.033848775
13	збмкшяеэгтйьы	0.032053104
14	омсзцэшщепющхи	0.032074162
15	юящцшсвбфйэфдяп	0.03198323
16	съудтщчлткшпекмщ	0.032083734
17	ятряизшлдюоггуиит	0.032303886
18	вочфиъкншьжийжаце	0.032318243
19	ччцсдъраызъдомвыд	0.032778647
20	хцыаэвкьтьвтжруищб	0.032545095

Діаграма значень індексів відповідності для ключів різної довжини

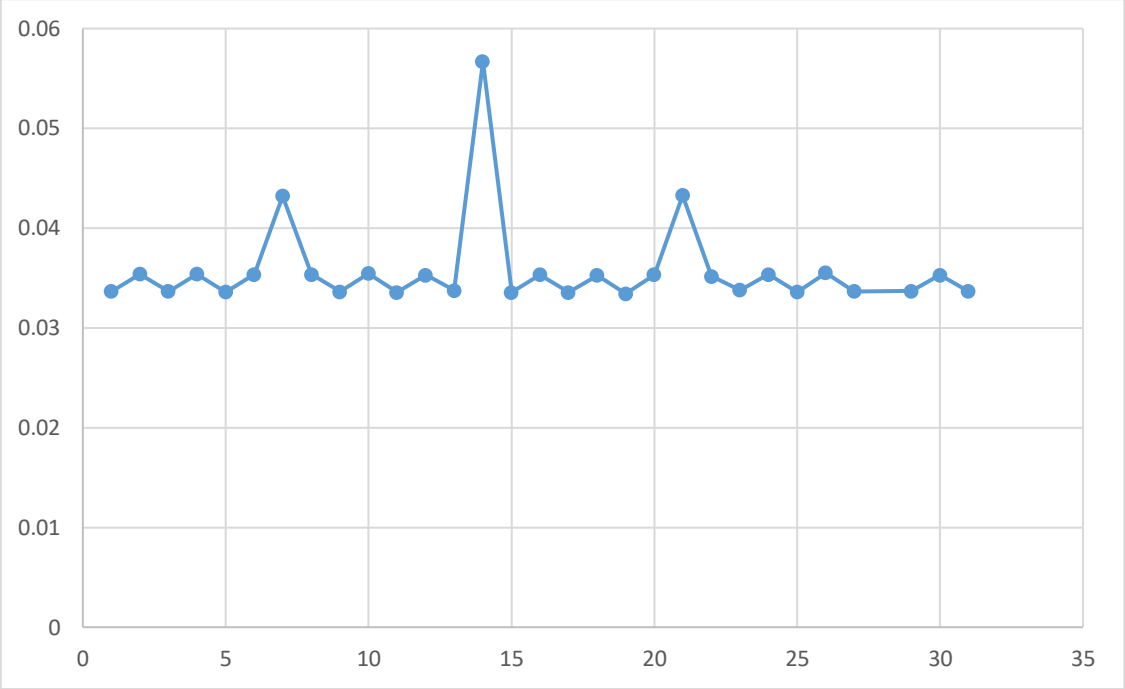


Завдання 3

В цьому завданні ми розділювал текст на блоки різної довжинита рахували відповідно для кожного індекс відповідності. Це ми робилидля того, щоб знайти можливу довжину ключа.

Таблиця для 3 завдання

Довжина ключа	Індекс відповідності
1	0.033658781
2	0.035403186
3	0.033657628
4	0.035375127
5	0.033600745
6	0.035353383
7	0.043212323
8	0.035366116
9	0.033618165
10	0.035441204
11	0.033570089
12	0.035279136
13	0.033742872
14	0.056670607
15	0.033550595
16	0.035329235
17	0.033553157
18	0.035250813
19	0.033429135
20	0.03532922
21	0.043282276
22	0.035165904
23	0.033776027
24	0.035362014
25	0.033597645
26	0.035504954
27	0.033646448
28	0.056467616
29	0.033693226
30	0.035294228
31	0.033669713



Отже, визначили, що ключ має довжину 14.

Я використовував для розшифрування тексту за варіантом 3 найчастішу літеру "о". Але ключем був “эбомчцтникфуьо”,що було не зовсім схоже на нормально розшифрований текст. Я почав перебирати літери, щоб вірно розшифрувати текст. Зрештою, ключем виявилось “экомаятникфуко”.

Таким виявився наш розшифрований текст:

итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвеличииопис ывалколебанияязналноивсякийощутилбыподчарамимернойпульсациичтопериодколебанийопредел енотношениемквадратногокорнядлинынитикчислуркотороеиррациональноедляподлунныхумовпр едлицомбожественнойрационеукоснительносопрягаетокружностисдиаметрамилюбыхсуществу ющихкруговкакивремяперемещенияшараотодногополюсакпротивоположномупредставляетрезул ьтаттайнойсоотнесенностинаиболеевневременныхмередин ственноститочкикрепленияд войств енностиабстрактногоизмерениятроичностичислапискрытойчетверичностиквадратногокорнясо вершенствакругаещеязналчтонаконцеотвеснойлинииивосстановленнойотточкикрепленияна ходя щийсяподмаятникоммагнитныйстабилизаторвоссылаеткомандыжелезномусердцушараиобеспеч иваетвечностьдвиженияэтохитраяштукаимеющаяцельюпереборотьсопротивлениематериинок оторая непротиворечитзаконуфуконапротивпомогаетемупроявитьсяпотомучтопомещенныйвпу стотулюбойточечныйвеспри оженныйкконцунерастяжимойиневесомойнитиневстречающийнисо противлениявоздуханитрениявточкекрепленияд йствительнобудетсовершатьрегулярныеигарм оничныеколебаниявечномедныйшарпоигрывалбледнымипереливчатымиотблескамиподпоследним илучамишедшимиизвитражаеслибыкаккогдатоонкасалсяслоямокрогопесканаплитахполаприкажд омизегокасанийпрочерчивалсябыштрихиэтиштрихинеуловимоизменяякаждыйразнаправлениерасх

одилисьбыоткрываяразломытраншеирвыиугадываласьбырадиальнаясимметричностькостякман
далыневидимаясхемапентакулазвездымистическойрозынетнетэтобылабынерозаэтобылбырасск
аззаписанныйнаполотнахпустынисследаминесосчитанныхкаравановповестьотысячелетнихскита
нияхнаверноеэтойдорогойшлиатлантыконтинентамувугрюмойупорнойрешительностиизтасма
ниивгренландиюоттропикакозерогактропикуракасостровапринцаэдуарданашпицбергенкасаниям
ишараутрамбовывалосьвминутныйрассказвсечтоонитворилвпромежуткахотодноголедовогопе
риодадодругогоискореевсеготворятвнашевремясделавшисьрабамиверховниковвероятноперелета
яотсамоанановуюземлюэтотшарнацеливаетсявапогеепараболынаагартуцентрмираячувствова
лкактаинственнымобщимпланомобъединяетсяавалонгипербореевсполуденнойпустынейоберегаю
щейзагадкуайерсроквданныймигвчетыречасаднядвадцатьтретьегоиюнямаятникутрачивалскоро
стьукраяколебательнойплоскостибезвольноотшатывалсяснованачиналускорятьсякцентруинара
згонепосерединерассекалссабельнымсвистомтайныйчетвероугольниксилопределявшихегосудьбуес
либыяпробылтамдолгонеуязвимыйдлявременинаблюдаякакэтаптичьяголоваэтоткопейныйнакон
ечникэтотопрокинутыйгребеньшлемавычерчиваетвпустотесвоидиагоналиоткраядокраяастигм
атическойзамкнутойлиниияпревратилсябывжертвуобольщениячувствимаятникубедилбыменячт
околебательнаяплоскостьсовершилаполныйоборотивозвратиласьвпервоначальноеположениеопи
савзатридцатьдвачасасплюснутыйэллипсэллипсобращающийсявокругсобственногоцентраспост
оянноййугловойскоростьюпропорциональнойсинусугеографическойширотыкаквращалсябытотжеэ
ллипсбудьнитьмаятникаприкрепленаквенцухрамасоломонавероятнорыцарииспробовалииэтоможе
тбытьихрасчеттоестьконечныйрезультатрасчетанеизменялсяможетбытьсобораббатствасе
нмартендешанэтодействительноистинныйхрамвообщечистыйэкспериментвозможентольконап
олюсеэтоединственныйслучайкогдаточкаподвешиванияниттирасположиласьбынапродолжениизем
нойосиимаятникзаключилбысвойвидимыйциклровновдвадцатьчетыречасаоднакоэтоотступлени
еотзаконактомужепредусмотренноесамимзакономэтапогрешностьпротивзолотойнормынеотн
ималачудесностиучудаязналчтоземлявращаетсяичтоявращаюсьвместеснеюисенмартендешанив
есьпарижсомноюивсемывращалисьподмаятникомкоторыйдействительнонисколькоиземенялори
ентациисвоегопланапотомучтонаверхугдеонкчемутобылпривязаннадругомконцевоображаемогоб
есконечногопродолженияниттиввысотуивдальзапределамиотдаленныхгалактикнаходиласьнедвиж
имаяинепреложнаявсвоейвековечностимертваяточказемлядвигалась одна коместокоторомуприк
реплялсяканатбылоединственнымнеподвижнымместомвселеннойпоэтомумойвзглядбылприкован
нестолькокземлесколькокнебуосиянномутайнойабсолютнойнеподвижностимаятникговорилмнеч
тохотявращаетсявсеземнойшарсолнечнаясистематуманностичерныедырыилюбыепорожденияигр
андиозной космической эманацииотпервыхэоновдосамойлипучейматериисуществуеттолькооднат
очкаосьнекийшампурзанебесныйштырьпозволяющийостальномумируобращатьсяоколосебяитепе
рьяучаствовалвэтомверховномопытеявращавшийсякаквсенасветесообщасовсемнасветеудостаи
валсявидетьтонедвижноекрепостьопорусветоносноеявлениекотороенетелесноинеимеетнигрази
цыниформынивесаниколичестваникачестваиононевидитнеслышитнеподдаетсячувственностиин
епребываетнивместенивовременинивпространствеиононедушанеразумневоображениенемнениен
ечислонепорядокнемеранесущностьневечностьононетьмаинесветононеложьинеистинадоменядо
летелпасмурныйобменрепликамимеждупарнемвочкахидевицейувыбезочковэтомаятникфукоговор
илеемилыйпервыйопытпроводиливпогребевтысячавосемьсотпятьдесятпервомгодупотомвобсер
ваториипотомподкуполомпантеонадлинаканаташестьдесятсемьметроввесгиридвадцатьвосем
ькилонаконецвтысячавосемьсотпятьдесятпятомподвешентутвуменьшенномасштабеканатпр
отянутчерезнижнюючастьзамкасводаазачемнадочтобыонболталсядоказываетсявращениеземли
посколькуточкакрепленияне подвижнаапочемуонанеподвижнапотомучтоточкасейчасятебеобъясн
ювцентральнойточкелюбойточкенаходящейсясредидругихвидимыхточеквобщемэтоуженефизиче
скаяточкаакакбыгеометрическаяитыеенеможешьвидетьпотомучтоунеенетплощадиатоучегоне

тплощадинеможетперекоситьсянивлевонивправоникверхуникнизупоэтомуонаневращаетсяследи шьеслиуточкинетплощадионанеможетповорачиватьсявокругсебяунеенетэтогосамогосебяноэта точканаземлеаземлявертитсяземлявертитсяаточканевертитсяможешьневеритьеслиненравит сяясномнекакоеделонесчастнаяиметьнадголовойединственнуюстабильнуючастицумиратонисче мнесравнимоечтонеподверженопроклятиюобщегобегаисчитатьчтоэтонееаегоделовследзаэти мчетапошлапрочьонобнимаясвойсправочникотучившийегоудивлятьсяонаволочасвойорганизмглух ойксердцебиениюбесконечностииобаникакнепытаясьзакрепитьвпамятиопытэтойвстречиихперв ойиихпоследнейсединымсэнсофсневысказуемымонинепалинаколенипередалтаремистиныягляделсв ниманиемистрахомимнеповерилосьчтоякопобельбоправвсегдашниеегодифирамбымаятникуяприв ыксписыватьнабесплодноеэстетствозлокачественноекотороемедленноразъедалоегодушуибесфо рменноеперенималоформуеготеланезаметноперекодируяигрувреальностьжизниоднакоеслибельб обылправнасчетмаятникавероятноонбылправинасчетвсегопрочегоибылпланибылвсеобщийзагово рибылоправильночтояоказалсяздесьсегоднянаканунелетнегопротивостоянияякопобельбонесумас шедшийемупростопривелосьвовремяигрычерезигруоткрытьистинуделовтомчтосопричастность божескомунеможетпродолжатьсядолгонепотревоживрассудоктогдаяпостаралсяотвестивзгляд прослеживаядугукотораяоткапителейрасставленныхполукругомколоннуходилаподпираемаягурт амисводакключуповторяяуловкустрельчатойаркиумеющейоперетьсянапустотувысшаястепеньл ицемериявстатикеиуговоритьколоннычтооониобязаныпихатьвверхребрасводааребрамраспираем ымдавлениемзамкавнушитьчтобониприжималикземлеколонныносводещехитреонявляетсяивсем иничемипричинойиследствиемвединомлицеоднакоямоментальнопонялчтоотворачиватьсяотмая тникасвисающегососводаиразмышлятьвместоэтогоосводетожесамоечтозарекатьсяотродника нопитьизисточникахорсоборасенмартендешансуществоваллишьблагодарятомучтоимелсуществ ованиевпрославлениезаконамаятникамаятниксуществовалтолькопотомучтосуществовалсобор несбежишьотбесконечностиподумаляудираякдругойбесконечностинеубережешьсяотвстречисто ждественнымпытаясьотыскатьиноепопрежнемунеотводяглазоткючасоборногосводаясталпят итьсяотступаяшагзашагомзавремяпрошедшеесмоментаприходаядетальнозаучилрасположениез аладаимощныеметаллическиечерепахипатрулировавшиестеныпостоянномаячиливуглуполязрени япропятившисьчерезвесьнефдовходнойдверияснованазалсяподсеньюгрозныхптеродактилейизпро волокиитряпокзловещихстрекозневедомочьейоккультнойволейзасланныхподпотолокнефаонивыс тупалиметафорамизнаниязначительноболееглубокимичемвероятнозамышлялдидактразместив шийихвназидательнойпоследовательноститрепетаниенасекомыхирептилиймезозояаллегориябе ссчетныхмиграциймаятниканадповерхностьюземлиархонтыизвращенныеэманациионипикировал инаменяцелясьархеоптериксовымиклювамиаэропланыбрегеблериоэсногеликоптердюфопосетите льконсерваториянаукиитехникивпарижепройдячерездворвосемнадцатоговекаипослеэтогонесколь кокоридороввступаетвдревнююаббатскуюцерковьврезаннуювболееновыйкомплексзданийподобно томукакпреждеонабылаоблепленасовсехсторонстроениямиприоратапривходесразуперехватывае тдухотстранногосоюзагорнейзапредельнойстрельчатостисхтоническиммиромпожирателейсол яркиимазутапонизутянетсяпроцессиясамоходовсамокатовипаровыхэкипажейсверхувисятвоздухо плавательныемашиныпионероводнипредметыцелыдругиеободраныистрепанывременемивсеонив местепредстаютподсмешанныместественнымиэлектрическимсветомкакбудтовпатиневлакеко ллекционнойвиолончелииногдасохраняетсятолькоскелетшассинаворотприводовирукоятейисулит неописуемыепыткитакивидишьсебяприкрученнымцепямикэтомуложуоткровенностивотвотоно шевельнетсяпойдеткопатьтвоемясоирытьсявжилахдополногоичистосердечногопризнания

Висновок:

Протягом виконання лабораторної роботи ми отримали знання щодо методів частотного криптоаналізу та здобули практичні навичоки роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.