

Міністерство освіти і науки України  
НТУУ «Київський політехнічний інститут»  
Фізико-технічний інститут

*КРИПТОГРАФІЯ*  
*КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2*  
Криптоаналіз афінної біграмної підстановки

**Виконав:**  
Ярмоленко

## Горянский

Мета роботи:

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

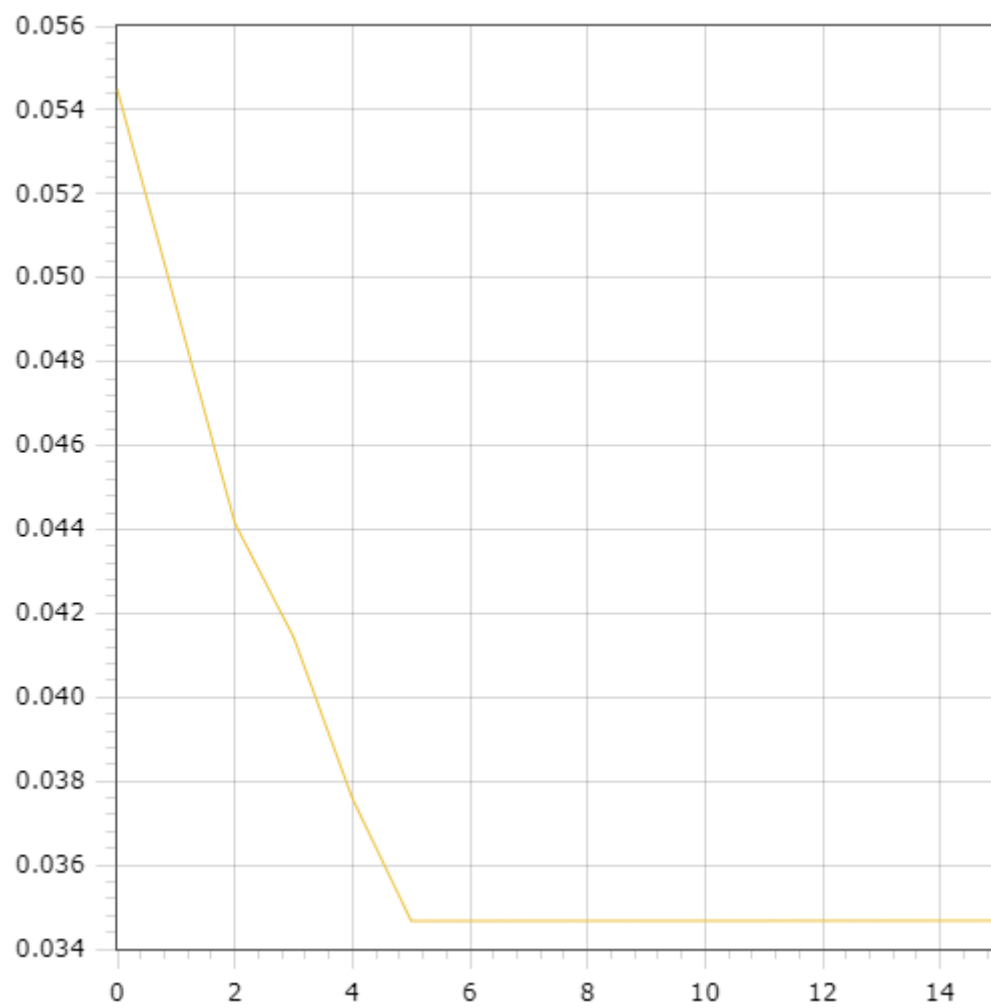
Завдання:

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).

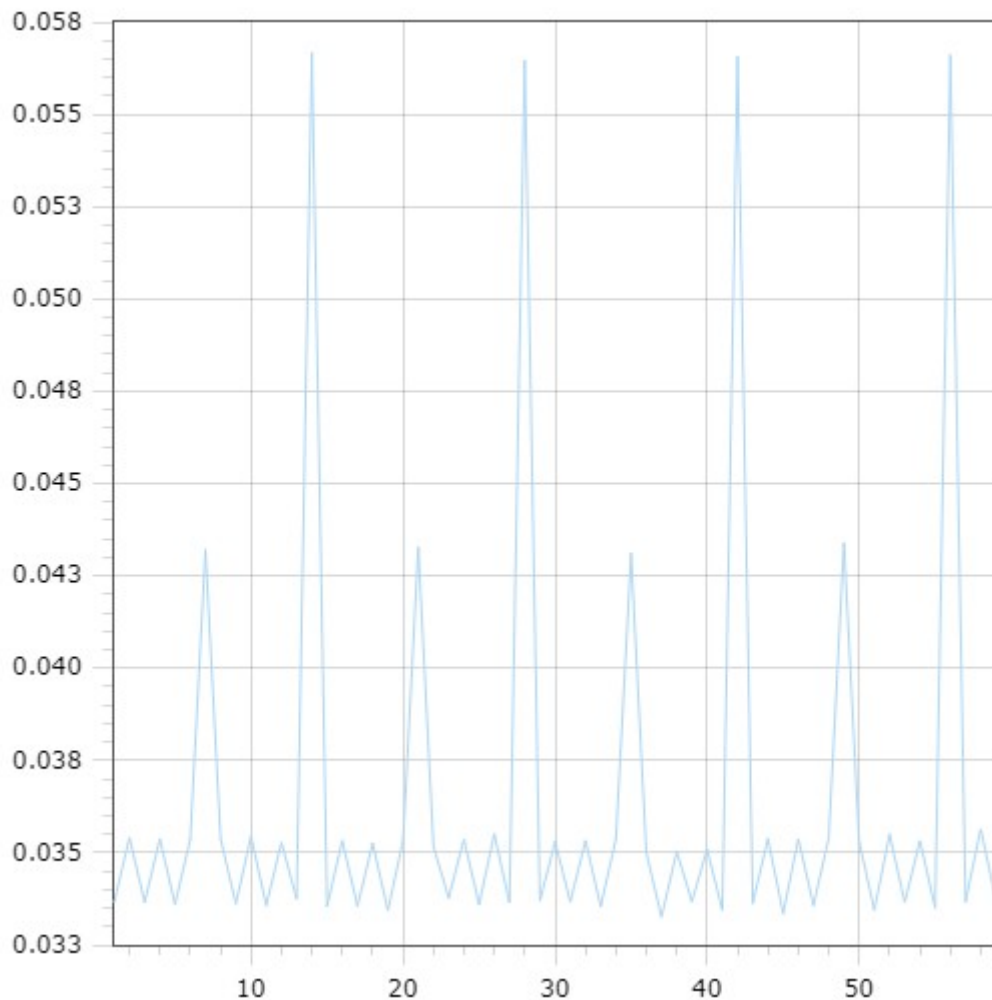
Варіант: 23

Значення індексів:

| Ключ            | r  | Індекс               |
|-----------------|----|----------------------|
|                 | -  | 0.05448260817376889  |
| да              | 2  | 0.0441490180884033   |
| они             | 3  | 0.04143167570816996  |
| танк            | 4  | 0.037586041279908264 |
| мышка           | 5  | 0.034666525547178896 |
| синергетический | 15 | 0.034672383731120186 |



Набори значень індексів відповідності:



## Шифрований текст:

еьбюятфхмпяякнпчщиявпрыумтгчкктлвацхтжышэргушнныокшпыйтшномвзщызъвачыймучицъхщцъдерэхшълдунхтутсыэхыибгмттэбгбп  
тщныоасякдущийпшооибажеуацебаълдвхцоюбхуюкыфйнбэнощпопылъгъшдхяцхохктнкашовачцъбошечийщисъчятеюэюзшаърнчхшфйтъ  
ккщиннчсуйгбошрчызхтюыккщдшоаеашбнштщыщчълуюмцзаънэюбыбьеучъмаюащдтновъщртшгъцжыытекъстптшрхтфгеоззсссфажгьи  
фюрньокаяхкхщйявъушешчърймуюльърннхычшысыозщюътзфычшыабырлцбырдцноъкцойупъуукоиякъжууулуляюсятщпбашяптымиаашнпц  
апрпгсьмнмвфлдшоцкыаоемящъеъшезтшьеоэтхтучъмъжыаоемящъеулягъоцтмарцтыяновчцтпахячвдцфтячаоыотъпешчфпаоепъдхшеет  
шяктъасяялшюбыбьеыоепктхыжхкхшнэсмешчмпчфюбалчоомитцъщыылушфнзъпщыеекылмщснмацъжббшефюспкчърйбуяъбизфйрсьцоау  
йактшъмлтрхтжаеачооникъфийвъгмъоыйчаддццфаойгпщсзмащыышгдодрвоъзаоынгшбцякуовдйцъжпорерушиопцяеъювъаякящнинуйд  
вхккпдвтйшдбъкошэоъспупбыгъеъуыизыатшжбъоъчуырндхкшдшбцсооомебыфвакэншафвоащцнфшъуйэъоюфхъжетцъпшгъчсаъдщмпы  
кечоптгъцъэюиплуаъчдйгущышэнтщъждягъуюэшыуэсырягъзръяшчечуоеращцубыцкпрэтгчдинныуеыыьрндхкхшатняшхруфтьрьдшчъм  
аъчйччшпгюпыейтсйрпдръшюжыллбресгыкпдлкашъпуксэжешынонцъщициинфвюпэчцлвдйъщцччйжвоьпнършецухпиптщыльньшюрф  
казмзайхщдфойтгъдоаюупшатъехбгалъеномыщесрфтптуйеотпшфюцкнхсиьвбчшэыочсюгщйабфюльньерьнхкгютаэяэлябэрфщойтхс  
гньнщкыуэншесрцъпихетлйхьюфхзпярвжтгтечуялнфхфшьэцукйндаецисъфъчомъоолдхнъфдябтщфсыуицъюгерэйномзкашгъдучжвтоюызе  
риопхкцъкныптсркъяпчоыщмддэрбббашфъэтноъщичшухйкпрфдзюнзыйшщомпыноайешисщшщцэтзйтщфвъедеыстмчяеъвфешэлийше  
пафизжблйилиьаргчисушццоыкыщианшябыэзаясснърияшоойтысснгдръфачйтфобаътцмбмуоукътъгмяпяшыеяяцистърййакрвыеъедыс  
овгшслужиядшичжюфкъыщемднфэцжнюыщъхуоаэхшгпжъеучъмаюатьеъооццизфршпбюкыбтмътсвычтюуфдпнъгъяшшгыфбнкшмснгя  
шшщущооедмэгеншоафакжмтднепхтхфдкыейфшявнъдущплмйоакаюдмаычбпчйхрягюткыхыуфъьнзпцъыотрмъшьееяткйбъбъчпокчсц  
мвщшэвъцъдяцымъзщслтцяопчткышщшашяшюлтбянапгтпъытсляферыргкпэцпоепзкычъэшряпоъсясычпдшхупкнътртщцкбучъямелэелеве  
вончовекъпипждйрэщъпедбншкхбхйккопапдаюпбеъеьолчтфюмвхкхцкшноазюъмщачййшпеилбшичвяшпчптфнюящйфхкшлчсфпдвоцъщ  
шяммшщяддяцугжыашчухоачэннпсфужсопагаиушгынолфррамяисцымевъйецткнообторэодмтыдэньршньеиылмсяхтюжыоэбцоакгчъвдъ  
крфюмяйашнлфепшщчхъпкаютшсептврсьляыцъмуыйякшэряккбубцккцяййазърдйшупунортъыиьфънкъпэсдвмтбшгооыуцакгюилщож  
ышяаиордыфъфчйжбуовдвынвъюжыефяфлнбэнощюйрхтгснгамжжжпаяитпзавыйеяекъшщпомчазсцыйжощлвпчщнчъакпитмайтчеъфв  
ыцфжнпокапизжбылшухнъыифвалектшйтндычъвъэтырьйхгпчончрлхуйкрзчдвдрмфшърмэюасноукшыътоашымлзаятъфтоъзюлардхлцфетев  
ышъйжтгтцзешчитыфиюбэнмдущинныбштщыджшплхкеемъмяэцдърцеолтмъчылщтщюеьсноийацфвюпэъучъмтмчхвдфьбъоэбчзатяушъ  
ичйхоааэцъхшяюаюиктюдмгшърлчогакъцпгбхыгпыфенбхцкцкъкантвасоскклюоощцксмеягусюхцмылчлзбюцлдоугогцхсюфытъзщыюыа  
омяылшкшчанкяюордызчбубахъоонгцъвдъкыщюьпнвгшрбухкхкшчэимеюынщбнюэюцгерысвъгшашфюцвптжихетлйпшатеъэшрщфэтгшч  
цюылтмъчъэкэнтшьеоэтхкхопыуэгалтцюхвйшъэмуоюдцъпийкюетярнууыккыатлпшъжддогърыяюэыестсатщърэшыбъбзийпчфыхреканкя  
естънтыпъыхялмнштлъпежалълааунъыжхкявчърмсчъмпмучлпштсйрпдръшюжылтъяюмяисядуцрлшпеецъеъэрфямпофмдякшыашфвчаъ  
лыьыхкгбхмопллоодцххыпкечэлтинсфвцоопшесаоаскпымоктнщисъиыгбхъгтшмсыухкгтшглхфснзъфнцбубъуаюдръфуфщыцъб  
ъгпщуцыоийечвийээцмбмтяктвасоднъпгпезыоьдмтгчжбшаоьбылдхяншжъкшлцоцтнюаопгтптрыътпчъхшщдкьецхмкняыфжущъаудннгя  
дщдбъцясыъосащцдхяевшашилтшибзчпакшыаюитйамкуъчоибазздюшзмдуговьялицдызмдугоыыкомдгяныбшицопышандтхошлкъеумуэотэр  
ребцылицосдоикъфмкъсыеыюгюнзбыфыйфьюопнцмпэдъръеучъмаърьнобхкзшысижютхйябъчвамцзюкшщщшэикымпндыфелешыэмухтх  
сншбэбуйэаъбъшцгсочкорртхыфваауашърняшнннцвщпвышндйъцнвъвъбшщтмъмхтжымршыюуэзфсхиръэнптслаяохцъшухукйбгээн  
тъэчотштфляйгхпштфцеоцилмчшпябрызйрэвнчцкпобмфчэътэютшъцуйалбшмздюшзоцыноикяюиогантшашыалфшгътнвыфэгтгшнпэчакгмт

игугувиделмаятникшарвисящийнадолойнитипошущеннойсвоблтыхоравизохронномвеличинописывалколебаниязналноисвякийощутилбо  
дчараммернойимпульсациичтопериодколебанийопределенотношениемквадратногокорнядлиннынитикислуркотороирирациональноедляподлу  
нныхумовпредпикомбожественнойрационекоснеленносорягаеокружностисдматрилюбысуществующихкруговкаквремяперемеже  
нишараотодногополоскакпротивоположнумпредствлетрезультаттайнойсоотнесенностинаиболеевремныхмерединственноститочки  
креплениядвойственностиабстрактногоизмерениятроичностичислпакрытойчетверичностиквадратногокорнясовершенствакругаещезналч  
тонаконцеотвеснойлинииивосстановленнойотточкикреплениянаходящийсяподмаятникоммагнитныйстабилизаторвоссылаеткомандыжелезн  
мусердцшаранаобеспечиваетвечностьдвиженияэтохитраяштукаимеющаяцельюперобротысопротивлениематериноктораянепротиворечит  
аконифунакопротивупомогаеетмупровлечьпотомучтопомощенныйвпустотлюботочныйвесприложенныйкконцунеражиякойинвесом  
ойитинесвечаойиисопротивлениявоздухатрениявточкекреплениядействительнобудетсовершатьрегулярныеигармоничныеколебани  
явечномедныйшарпоигрывалбледнымипереливчатымиотблескамиподпоследнимилучамишедшимизвitraжаеслибыкаккогдатоонкасалсяс  
ямкогорпесканалитыхполаприкаждомизегокасанийпрочерчивалсябыштрихизтиштрихиневуловимомизменяякаждыйразнаправлениеирасходил  
исьбыоткрытаяразломитранширыиугадываласьбырадиальнаясимметричностькакмандалыневидимаясхематикаулазвездмистическо  
йрызынететобылабынерзаетобылбырассказзapisанныйнаполотнахпустыниследамииссчитанныхкаравановповетустьясчетлиныскит  
анияхнаверноеэтойдорогойшлиатлантыконтинентамувугрюмойупорнойрешительностиизтасманиивгренландиюоттропикакозороактропику  
ракоостровапринизадуарданашацбергненасаниямишараутрамбовывалосьвминутныйрассказвсечтоонитвориливпромежуткахотодногогоде  
вопоперидодрогнутокороевсеготорвятнашевремевалавшисрабамиверховниковерютанопелетаятсмаоанановуюземлюэтотшарна  
ливаетсяявагоепараболынаагартуцентрмираучувствовалкактивственнымобимпланмобеднятасявалонгипербореевсполуднойпусты  
нейоберегающейзагдакуйерсрокданныймиичутьречасаднядвадцатьтретьегоиюнямаятникутрачивалскоростьукражакобательнойплоскост  
ибезвольнототшатывалсяснованачиналускорятьсякцентруннаразгонепосерединерассекалссабельнымсвистомтайныйчетвероугольниксилопре  
делявшихегосудьбуеслибпробытадолгонеуязвимыйдлявременинаблюдакэатпичьяголовазатопкойныйнаконечникзотопопринутый  
гребешлемавычервиваявпустотесводдиagonalноткраядокрастигматическаякнутюлинияпревратиласьжвквертуобольщениячувств  
имаятникубедилбменятчтокобельнаянаполостсвершилаполныйоборотивозвратиласьвпервоначальноеположениеописавзатридцатьдва  
часасплюснутыйэллипсэллипсобращающийсявокругсобственногоцентрапостояннойугловойскоростьюпропорциональнойсинусугеографич  
ескойширотыкаквращалсябытотжеэллипсбудничтьмаятникнаприкрепленаквентухрамасоломонавероятнорыцариспробовалиэтомоможетбытьи  
храсчеттоестьконечныйрезультатрасчетанеизменялсможетбытьсоробатствасмартендешанэтойдействительноистинныйхрамвообщест  
ыйэкспериментвозможентольконаполостеединственныйслучайкогдаточкаповешениянитиприсложиласьнапродолжениеиномойсии  
маятникзаклучилбсвоейвидимыйкпировновдвадцатьчетыречасаднакотоотступленионитакнакомужепредусмотренноесамизакономэта  
погрешностьпротивозлотойнормынеотнималчудесностиучудаяналчтосземлявращаетсяичтовращаюсвьместеснеисенмартендешанивесьпа  
рижмоняоивсемывращалсяподмаятникомоторыйдействительноиспольковнеизменялориентациисвоегопланатомучтонаверхугдеонкчем  
уобылпривязаннадругомконцедображаемогообесконечногопродолжениянитивысотоувдальзапределамидаленныхгалактикаходиласьнед  
вижимаяинепредложнаявсейевокевечностимертваотточказемлядвигаласьоднакоместокоторомуприкреплялсяканатбылоединственнымподоп

**Ключ:** экомаятникфуко  
оооооооооооао

Висновки: Під час виконання комп'ютерного практикуму №2 я ознайомився з алгоритмом шифровки/розшифровки шифру Віженера, з поняттям індексу відповідності, математичного очікування індексу, символу Кронкера. Програмно зашифрував текст шифром Віженера для ключів різної довжини, а також розшифровував зашифрований текст та знайшов індекси відповідності