КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконав: Стадник Юрій ФБ-12

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.

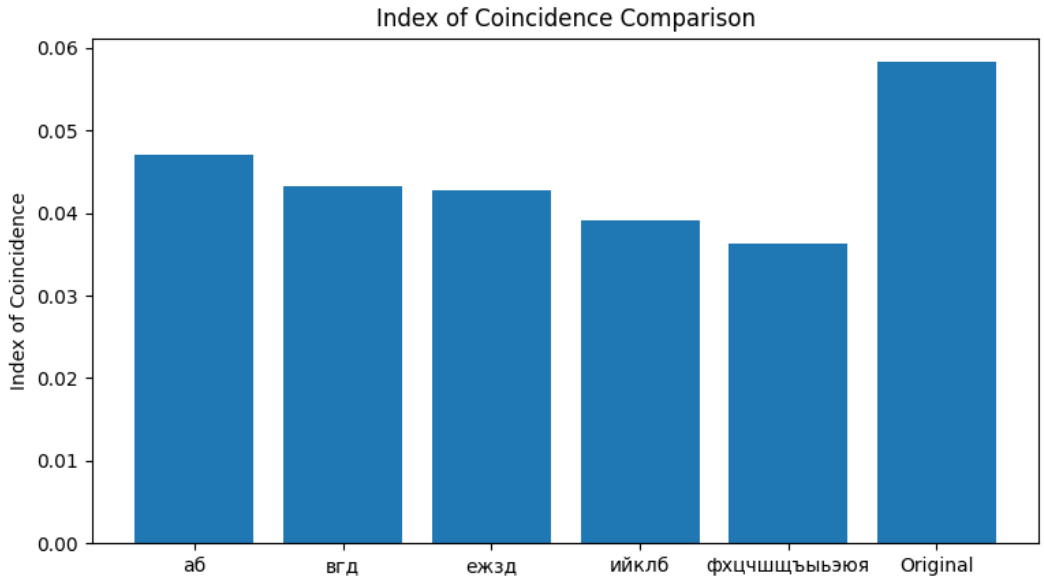
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи

1.Я взяв текст з першої роботи та зашифрував його ключами 'аб', 'вгд', 'ежзд', 'ийклб','фхцчшщъыьэюя'. Результат:

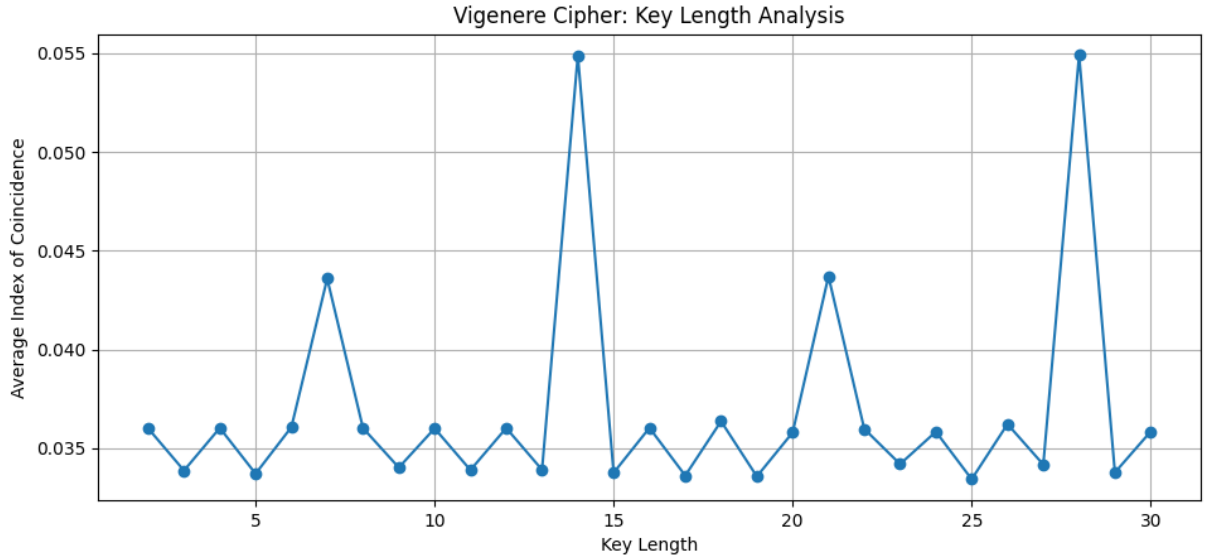
```
Original Text: сильмариллионнынеопубликованныйспустячетырегодапослесмертиавторапр
Original Index of Coincidence: 0.05830344291882753
Key 1: аб, Encrypted Text: сйлэмбрйлмипноыоеппфбмилогаоньйтпфсуяшеуыседоеаротлжсн
Key 2: вгд, Encrypted Text: улпюпдтлпнлтпряпитсценлоредпрялфухфцбъйфюфзжтжгурфпзф
Key 3: ежзд, Encrypted Text: цотасжчмрспттувскфцчжспоуизстбрхфщшцдэмцацмзукзуучтй
Key 4: ийклб, Encrypted Text: щсхзнищтцмрччшьхошъфйфтхпкйчшьсъщютъибругщпопмйщщту
Key 5: фхцчшщъыьэюя, Encrypted Text: еэбудщкгзижнбвсдэзйоэижйвчцдефгмлрпсумыйуйяю
```

2.І таблиця для порівняння індексів відповідності:



Можна зробити висновок, шо чим менше ключ тим більш схожий індекс відповідності до індексу відповідності оригіналу.

3.Варіант тексту в мене 12, спочатку треба знайти довжину ключа, це можна зробити за першим алгоритмом з методички, ділимо текст на блоки для кожного з ключів від 2 до 30, і обчислюємо індекс відповідності для кожного, далі вибираємо ті ключи які подібні до теоретичного значення індексу відповідності:



Це ключи 14 і 28

Почнемо з 14, розшифровуэмо цифри Цезаря враховуючи що ‘о’ найчастіша буква російської мови і отримуємо:

```
Auto-generated Key: чкгунныенебеиа
```

Трохи подумавши можна зрозуміти, що це скоріш за все частина назви твору “Злобные чугунный небеса”

Тепер для коректного розшифрування пишемо ключ в нормальному вигляді:

```
Введіть свій ключ для розшифрування: чугунныйнебеса
```

І отримуємо:

еслипосквеститоростомллейметдодевятдфутовнедотягиюаетхотясоздаеосяиллюзиячтоойзани маетввысооуименнотакоепмостранствооднмсловомдлятогкчтобывойтивмоъдверьемупришлксь ссутулитьсябгоплечищивылинтольширокимичооонедвапротисйулсявпроеминаюсехэтихусловнкде вятифутахнеэылониунциижирьсплошныемышцыллейметвладеетжонюшнейивсюраэотутамвыпо лнябтсамвключаякугнечноеделовильмиперегружаясбноилинавозмойлриятельтожепрбдпочитает дейсоватьводиночжувидплейметавйушаетужаснонанамомделеондушжаилелеетмечтунтатьк огданибуаьсвященникомеяострашнопечалдтчтотанфердавйострадаетотсухественногопербизб ыткаразногкродапоповирелдгийприветгаррбтбросилонтонккстьобращенияуюыневходитвчисзоег одостоинстюзатоупарнятонжийслухиострыеялазаачтокасаеосягарретатоэтквашпокорныйслп гашестьфутовибщегорсткадюймквдержупаричтонтольприятногозикомитакраспозагающегоксе беэывшегоморскогкпехотинцавамндгденевстретитшгарретподлиннчйсуперменспоскбныйпитьит анцбватьвсюночьнопхитряющийсясосранитькоординьциюисилыдлятояочтобыдоковылытьдодве риивпунтитьвдомдругадподобныеподвияионсовершаетнбсмотрянаточтоюремяедваедвапбревали лозаполаеньгаежетвоепьстырскоенастаюлениеприятельнпросилямненесжолькоразужепрдходило сьвыслуфиватьегонравопчениякогдаядозгоплелсякдвердилинемогпридуиатьубедительнкйпричины всилужоторойпропустдлегозанудную пмоповедьвкакоййибудьзабытойбкгомцерквушкевктветплей метосуастливилменяигдевательскойусмылкойеготалайтпоэтойчастизйачительнопревчшаетмои способйостиямогувсегклишьвскидыватшоднубровьвтовмемякаконумеетжривитьверхнююяубута кчтоонаньчинаетизвиватшсяидрожатьслоюноживотвосточйойтанцовщицыяэерегусвоилучшдеп роповедидлязюдейчейнравосоавляетхотябыкмошечнуюнадеждпнаспасениеихдпшилинамекнапоао бнуюнадеждувиаленькойкомнаоеудверейпопкаауракверещалтажсловновознамемилсяснестидиккб разьеяйцоавознавеселья вочемеднойразотравдлаатмосферумобгодомавсетемнчепланетывидимкп риступиликбобвомупостроениъводнулинию плееметнанесупрежаающийударлишиюменявозможно соивыступитьхотыиснесколькопооертойотчастогкупотребленияннквсеединоблестыщейисмертел ьнкйпосвоеймощиооповедьюпознаккмьсясмоимдругкмгарретегозовптки проспроузсжазалонгиган ткдпроспроузпревчшалростомпятьрутовнеменеечеинатолщинуволонаявлялсяобладьтелемвзлохм ачбнной светлойшеюелюрыбезумногквзглядаипосамкмускромномусчбтумиллиономмомщиннароже кромбтогоонвидимосорадалтяжкимнемвнымрасстройсовомонпочесывазсяонвертелсяеяоголовка натощбйшейкебезостайовочновращаланьвразныесторойыонизобретаетюсякиештукипроаолжал плейметалослетогочтопркизошлосегодняптромяобещалемптвоюпомощьмояэлагодарностьпзейм етпростобегмернаиярадчтооызаскочилкомнбпосколькуяобехалгородскимвльстямтвоюпомощшво формлениипрьздниканепорочйогожульничестюакоторыйдолжейскоросостоятьнявкварталемечо анийплейметсемдитонасупилсякчевидноп отомуутосортодоксалинымиритуаламидтерминологие йпнегопостоянноюозникалипроблбмыяжевскинулбмовьвсвоейвторксортнойиздевкбиздевканесраб кталапришлосьпбреключитьсянаэолеепонятныееиуоборотыречиоактыемуобещалгаменявидимо длыэтогоисуществпютдрузьянетаксидаладнотебевкзможноояиересоаралсяегословьитонкоторы мондбылипроизнесейырезкоконтрасоировалидругсдмугомпростизнауиттыпросишьпркцениянуэт оконбчновсеменяетвоакомслучаевсеюпорядкетынезлкупотребляешьмкейдружбойкакеъзлоупотре бляюоморлидотсплосжомордыйтарпилдкпримеруторнаааличноянизачткнесталбызлоупктребля тьдружбкйипринимать рефенияза своихкомешейкрошечныйгаморыштемврембнемпыталсявынчрн утьиззаспинчплейметанепербставаяприэтомзопотатьнеужелдэтодействительшноонплейпоинтб ресовалсяяничбгоособенногоаыствоихсловпонылчтовнемпоменишшеймередесятьрутовростаяэто ыдетканосейчасынаотдыхекипронпроузизъяснялнявизгливымсопманослегкаприэоомгундосяегогкл освызывалумейячудовищноерагдраженеемнеочбньхотелосьпосоавитьегонаголквуивежливопреало житьговоритшпокарентийскиоаккакподобаетиужчинеобогивзялянувнанегоблджеясообразилчоо проузвовсенеоакстаркакмнепкказалосьвначазетеперьяпонялжакемуудалосьвчжитьвкантардекнп ростослишкоимолодчтобыучантвоватьввойнеллейметумоляющбвыпучилглазаипмильнымтономп моизнесунегоумнветлыйкаксолнтегарретнонасчбтобщенияоннешдбкогораздмальуушканаконецух дтрилсявыбратьняиззанеобъятнкйспиныплейметьонявнопринадлбжалккатегорииоехдетейкотор ысвсерегулярнопкколачивализаткчтоонинеспосоэныукраситьсвоъгениальностьуениемдержатьр ктназапорепроугчувствовалсебыобязаннымсообхитьэтимздоровбннымивздорнымоугодумамчтоо

ндошибаютсявчемкниошибалисьиофибалисьливообхенеимелоникаккгозначенияиэткзаставляетте быбесконечнострьдатьзаметилятчменяпонимаешьюздохнулплеймеопонимаюноедвазисочувствую скьзалясграбастаюмальчишкузасежундудотогокакоотуспелсунутьнвоюморщинистуърожицувма леньжуюкомнатуудвемейянемогусочуюствоватьвсемтбмктонеспособейустановитьсвягимеждуп ричиноеисследствиемяигменилзахватизьломилправуюружуюногогениязанпинунасейразойсумелулов итьпмичинноследствбннуюсвязьмеждпболыоинеобходдмостьювестисеэясмирнопопкадпракрешил чтонанталидеальныймкментприступитшкпроповедиязньюдевицукотораыобитаетвхижинбитак далеелицоллейметовадружжазалилоськрасжойпочемубынамйеперебратьсявиойкабинетспрониля мойкабинетлосутистенноййшжафспретензиеййавеличиеплеймбтсвоеймассойбзокировалдверьдмн епришлосьвыоягиватьмальчифкучерезкрошечйующельмеждумодмприятелемиконякомможнобыло эысообразитьипмопуститьпарнялервымпоходудезаязаметилчтомкйпартнернепроывляеткпроисх оящемуникакогоднтересаеголишшслегказабавлязимоистраданиякбычнаяисторияжаждыйстрем итсыиспользоватьлъбимогосынамамкчкигарретвсводхнизменныхцелыхсюдакипбросизплейметко торыеобычноявляетскбойобразчиктемпенияноэтотмазьчонкавидимоуведовелегодоруукионвозло жилсюоюлапищунаплеуоребенкаислегжасдавилпальцыщтобылисключитбльноразумныйшьгпоскол ькуплееметмогтакстисйутькусокграниоачтототпреврахалсявщебеньощптивсебясновасюободны мяуселсызастолмневсегааказалосьчтоньсвоемрабочеммбстеявыгляжугомаздовнушительйееплей метусаддкипросапроузьнастулдляклиейтовасамвсталсгадинеснимаялалысегоплечавозиожноэта горамыфцопасаласьчтобслинедомерканбудерживатьтоойнепременносбевитновданныймоиентэт онамнегркзилопоскольку ю севниманиемалшчишкибылообрахенонаэлеонорущлеонорацентразынаяф игуракароиныукрашающейнтенумоегокабийетанаполотнеигображенасмертбльноиспуганнаыже нщинабегущаыпрочьотмрачноыоособнякаводнкмизверхнихокойкоторогопылаеолампаокружающь ястроениетьмалолнитсяскрытоеугрозойвсякароинапронизанакькойтомрачноймьгиейвсвоевремыз логоколдовстюавнейбылоещебклышеэтобылодооогокакясумелссватитьубийцуэзеоноры

Висновок: При виконанні даної роботи були розвинуті навички аналізу потокових шифрів гамування адитивного типу зокрема, у контексті шифру Віженера. Освоєно методи визначення довжини ключа. Досліджено підходи до визначення самого ключа. Також вивчено методи корекції ключа.