



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

ЛАБОРАТОРНА РОБОТА №2
з дисципліни «Криптографія»
«Криптоаналіз шифру Віженера»

Виконали: студентки 3 курсу ФТІ
групи ФБ-83

Бондарчук Ярослава
Перевірив: Чорний О.М.

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

Індекс відповідності відкритого тексту: 0.0613382

Обрані ключі для шифрування		Індекс відповідності шифротексту
1	дн	0.0477647
2	рим	0.041945
3	море	0.0370428
4	хорош	0.0382734
5	всебудедобретут	0.0348495

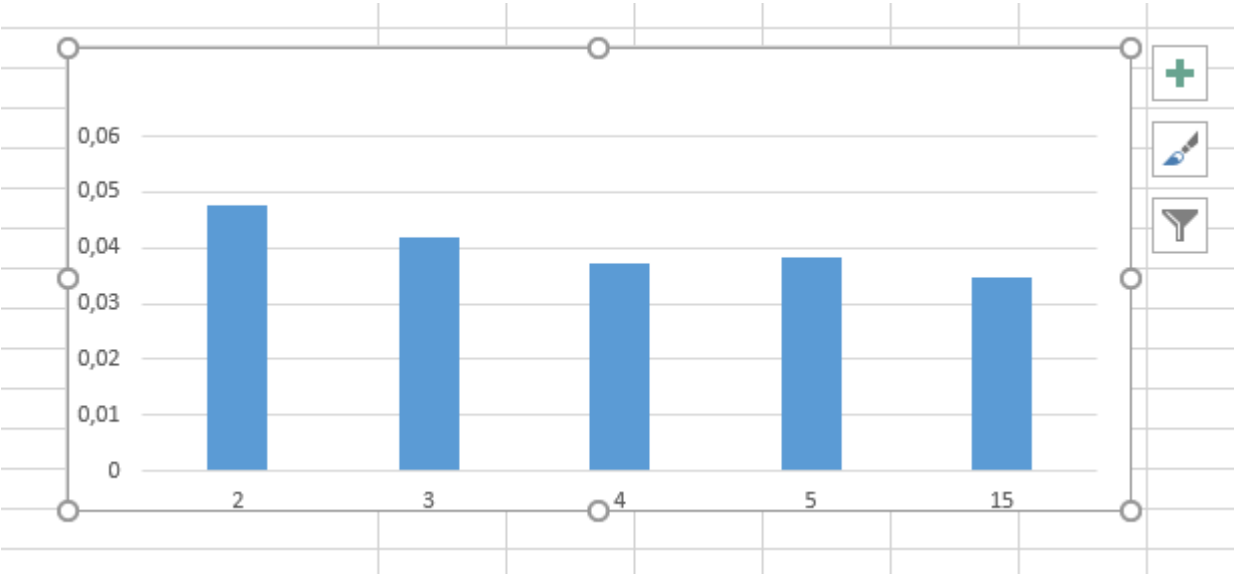


Рис 1. Діаграма індексів відповідності

Індекс відповідності шифротексту: **0.0320688**

Індекси відповідності для блоків заданої довжини заданого шифротексту:

2	0.0323983
3	0.0355699
4	0.0351673
5	0.0357102
6	0.0362738
7	0.0357102
8	0.0344809
9	0.0349486
10	0.0356773
11	0.0341549
12	0.0362066
13	0.0568646
14	0.0371437
15	0.0355825
16	0.0337025
17	0.0341195
18	0.0344859
19	0.0355383
20	0.0362873
21	0.0370703
22	0.0337696
23	0.0345462
24	0.0337775
25	0.0360364
26	0.0610518
27	0.036071

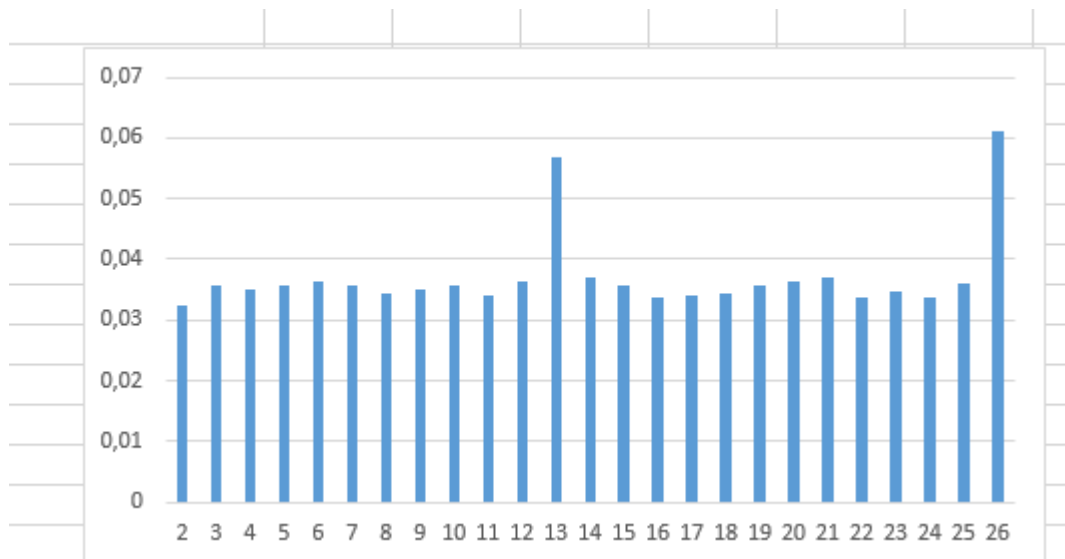


Рис 2. Діаграма індексів відповідності для блоків

Можемо зробити висновок, що довжина ключа - **13 символів**

о - **г**рооно**овь**дуо**а**

е - мщччччч**ень**чй

а - сюь**ь**ььрктбьо

р - бом**л**лммаъвс**м**ю

Ключ:громьковедьма

<p> шиеусефкхтуючйуэйрюбношнюеьмьбьдйдззсюхяюлкфпнодырлэцбьоцфкпш шозаушжизккчлфргпняиниюнежсаохпмлоивмибэьсбщцштжкжьюсюмяюэш швптбюосбьначиркхзфубьхяючбарлмослфьпамйдерлфрюеьшвызцджфсбц шщцуткемфхслуюлпзэючхфкхрэгчоонэбьоцхашальрщцмьвиагфдпшрзряеое хюэлпткптьорсуьцйипсжжумьгоптзэккмфмдоьаеьушиегуфкбуклшьямпымнхь шайхтьюпврвьфтефьчгчмуеолчнюьощюызхднйфяьхктонайнчифьюлпа ющцкчмгьюмьщцвряюфдиэпсжечржтаклчьэгчрфуфхкпсвчфлпэрчйищейшх сжпчвзьбштужжфлшшрклбчерюиришамхдльчнрьфмкьвйтясвгтшьжждзтгтр орышщяэррейефодыоцяахсдймпсфьхяпжюзуьтргмцяпюзаяшнгбамэхннсий йлуьшасжжцубьзсшьяйэжпыпаннфггррцоюхбгбпбзаоопьдцкиьшрупрайбу ошзкрисщдчлйушгтмишуюрмнжьюоспктиуыыбщкжхжяюеюшщжкшрчшищ ейхымкьоднщшасссзлбдоучтосхьюьфьэтнолнюргцухьюопньчясолжфнйю шэбщнсьоджйыхрздячыхпзабчятянибщзуюкаютйкнякрасжжырфкфкруплрмн жьцкфбрицозмешяфблймюкзюкнеьвтмсэвиагомйшрорбьжьююмовопусьэе маоукшяфехьсхвьуяюпиецшзьясьвщцьящкшрцоовргышрррсеобацяцшсезта рвисятацфбзцдаослжцяюогттухдгяхоаумютохгцйменяюфмзаяуждхсхсвнфбм узпюдсбшйкщцюттмсышвьймфобцьцчхьюмктьовосьцоошесмьрресбщанре смьррзтоюанпяшйюаотдазмвйбкькыатдирьшрчйльфшхбдлпщцщцызтзшух гатаьувиммяюхянючтшкэйнюьгфуыншрмуцкыиюрсчьзкуьюптьнаноачмг рвиастацгмйхсхяфвгвоафшшртдожкстоицудтггмпрюьтгмжксмиоснльшгьбм непруьшгцйхщизильяхлжмдфоонумфкулрмщццнтооершшьэюоуйнюкюрс ичзьшздюеомбэзттобкцуюснльцяцйойждтершущьбднскюзжнрццтгткхкоарэ йсузапньбщезюьзньекпцзечерьфияхргощиьхсършорэйяьяфьюыхэрйчимтя рыснюопцлдьорсаявкшннсьицивючббармдьядоьябэптзтсчсавибмьупешцозт гьщцачохьзмзяфббшькщцтврпурмэншмсуикэириучщцьцтьмючодшюьзкж мечвсчхюабзбуфмйзснгпячцуюуыдьюсвхгьяьэьчялнюрныгвчмнюышуб нлксжкпбщбноешьжждвсмприовучащонфкоахмхщыбцбццтгттаххщииштзрм онсвьйэжйкцбощнлсбрноуохимиреоаяикшянкыйфмлчщсмабтйойерсешмшз चुниисавэоаьизнжцгтгтгтфэхупгтлгкцзюьпачзтноопгтьозпапкрфупбюаач ыкуюкюужшщфьшхвтгофсьоуыхубрьснияьулоормэьюьрюмупыпайнюргц цллыкылялпфочгчоокхосурфсичйзстбхмйьбдобоуниьфивовьчббжбщц гьцэьэяскщкшмлэбютпюзмхкьоншхмшьбдхйиляцбэжскэзхйаьмвкнйхкыкы бшзгяюсаяетхюмбоофхьшщхщыодвчазстгтьюгуйшпшюахрмкшгтзохаюосерчьхц ртумьхсфцзтьрцппгамэьлэштутзябьявлфучымоофмммвсчьбьбьццднысэрвьч цмнлйфохьбрылйнжпбрерьоцмцутчадщцзбэзаянксьенрщфжшштужолиэы засбгагэзежюцэкэсврндикгьяьбдаксийтыощгьдешьшолчымитндиезмсхшр мзшцштужбрершннысцтужьчифымтпшрзйуссншгчанупйдсфлхтмитнчуцф чгтжфрынткижсхэйшкпяунрдумсьшюйцбикжнсгуррклешвхцдщыжюпсжпы этднцаомьмьрцдуудэьлчнлфвгцюмтшюьэтямрвуфтиыкщйчьбвдотиьыь нпшптапшлзцсийцакзхбйтсьотаьабчдждфмфюмучийонтяюпэйншшцюптлте ьбгншаррокшлзупйчунбляакущяпаюйсбонсцяоаювмжблсауьжфвцдю ыушшзьяьэтнхкчнизьзырзчййфмсэунаыштенийфхтшцедтрэцтжфхзхюсэжу дздиыуяыцысонгцйшсееюхшоьцфкпшщцопхщгцгцгклкнизэйшкьодйдысцизу экпжкрднниатацджшяюсбпаорыношэткизьжльцьофбдухльчячьоькудкоюю уючюкьбщкрьщешуеушщцйщзвдиыиушзьчбнцглькчюаыхцптябцлюьцщцльш пчннццяльбднбюкьгэкшщйрднжешрщкмкшштшцкшшууюьмфцпурпнпогс лпшкштчююоеютиьбукляльстбчйвожнтюзжлфокфлбучднюфлгбкшьюмоофмм схаотюьопньчькгчочмйрээйиснвзюыйхсрртюзшляьцщцщзьдсфвибкшычужш фбщссьхяхцптябюепэйсшщцрянкргьщлжтбйптбуажююсжшуннькэлсцуци еуйехлфнсщцшхкбфбдраерщфкьснфпщценоаьлшууьтаэтеюяшйьзсибшор ююыйшштвсдцопьсльцжкххюнигажфичобццьюувьююйьеучжьяыршмыфарз яеуаотйэупчьтзцзиаьзашортлдоеомызаббфбфьэксбйсюхойежшплаофвэе крмиюпрщькьцдрйжмтиыкцшорпкьйхсхмыьнкшкштнямиыщыьссьвйдоичхю хмпичууомзтс </p>	<p> лисмотретьсхолмамрабпиаьлывиденбелыйободркизосинвторойпотолщепотем неиселейавшентреширокоезеленоеднокрапрчкаоисаодагоевакрьлцевоздел анныхполейиоблактауманаподойдешьвплртнуюкдеревьямнаставлялменяущ ительпошлешьмысленныйсигналвлглублесалюбрйможешьдуматьочемугодн олишьбысформироватьоощнуютелепатическуюоволнуакоумнсеенапавитьна общейчастотектонибудызстражейгтанишыуслышитсямушценномашлянулау чйшебьемузтогрнеслышатьнеобязательнопродумыватьочереднуюпакостьзнаю знаютынанихсверхвсякоймерыгоразданонасейразпостарайсявоздержатьсяото ныхочемэтояхдаовольневампирыоченьврпримчивыктелепатииисразуотреаг ируютнаееприсутствиехотяинесмогутдоскрнальнорасшифроватьтактонапир айнаколичествооаненакачествооттаксмотранадельмшцубанюанамрщивлобо тусердяинамооволнутутжетеагируютьягилишестядептовкатореюеовбнны епаромвыбегаютиздверейивыпрыгиваютизоконатакованныевнезапнооживши мивенинамитукибудущихколлегзанятышайкампикрывающимиотвеникрвса моескровенноеучительусмиряетвенимирднимдвижениембтовиновзглядыадр есованныешутнишсенедаоытыоиколлетгаоинесулятишцгхорошегрясмазало думатьанеттанслироватьзаклинанияжальчтозагрдыпррведенныевэтихстенахт ытаминенаучиласьдуматьчтождумаюстоюпоподосинойнаморщивлобирмашкау жечтотржуетзеленаяслонасочитсязичетнычугтрлковатхатистыхгубразделенн ыхкрльямиудилтелепатироватьзначитсознательноеделитьсямысляоискемниб удьдругимделосьпоследнимизлесаиянетпрохладойсидящаянаветкеиволгауди вленнопркачиваеьхвостомответнаоумствениынепотугилибозанятияиомазало сьмненепозубамлиброшарашенныестражиграницыпрпадалинаместесраженны емоеймошпрйдумоймристаранияувенчалисьуспехомминутчерезсорокизаэтов ремяуспелापередуматьбольшечемзапредыдущиевосеонадцатьлетавотитезуль татагаподействовалрилионпррходилмиоослучайноявпервыеувиделавампирав озоржноееслибыонврзникизниотмудабылбледенмаксмертьинедвусмысленнрск алилорокравленныезубыабегониспугаласькамсрбственирипланитоваламоизн аниявобластивампироведениябызоровалисьначеловеческихлегсндахипредани яхотличавшихсяредкрстнымпессимизмомктомужевсегаврюрыкартиныгобеле нынаскальнабживописьизображаютвампирависключительноночьюивтемнрте крыльязубыкогтивсэзтомажетьсятакимстрашнымигромнымтолькопртомучто толкомничегоельязразгладетьдневнойсветразвеляорелрлужасавпухипрахприс олнечнрмсветенафонебескрайнихполейивысокихдеревьеввампирипоказалсямн евозмутительномелкимбезобиднымптвадаяещенеспешиласьапришлосьмнега лантнопредрджилрикувоспрлзоватьсякотойовпточсмянерискнулавампиру лыбнулсяпрказавдлинныеклымилубойулыбнулссябыувидекамясползласьеха лапокрутомууроашкиномубокуперекинувповодьбчерезгрловулошадиявыжид ающеуставиласьнавампирастражгтанишырказалсявышсменянаполголовышир оквлпечихивсьманедуренсобойдлинныетемныеволосыобрамлялиузкоезагоре доелишосложенныезаспинойкрыльяпридаваливаопирунекотрроссодствосмо тоемдемонопопсланникомсоертидесятиаршиннаястатуямототогоекрашалаакт овыйзалвысшейьколычерныепронзительныеучутьраскосыеглазавампираизучи лимрюмалрптивлекательнуювнешнрстьнракинесумелиразгадатьчтозанейсок рыто </p>
---	--

Висновок: Під час даної роботи я навчилася за допомогою криптоаналізу дешифрувати шифр Віженера. Проте виникли проблеми під час знаходження ключа. Букви російської мови з найбільшою частотою (о,а,е) не дали ключа у правильній формі. Після того як було знайдено ключ, при дешифруванні деякі символи ВТ не є правильними, та це не є проблемою ключа через те що більшість блоків розшифрувалися чисто. Також опанувала метод зашифровки тексту ключами різної довжини.

