Лабораторна №2

Фб-11 Яцентюк Андрій, Куство Іван
4в

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

Порядок виконання роботи:

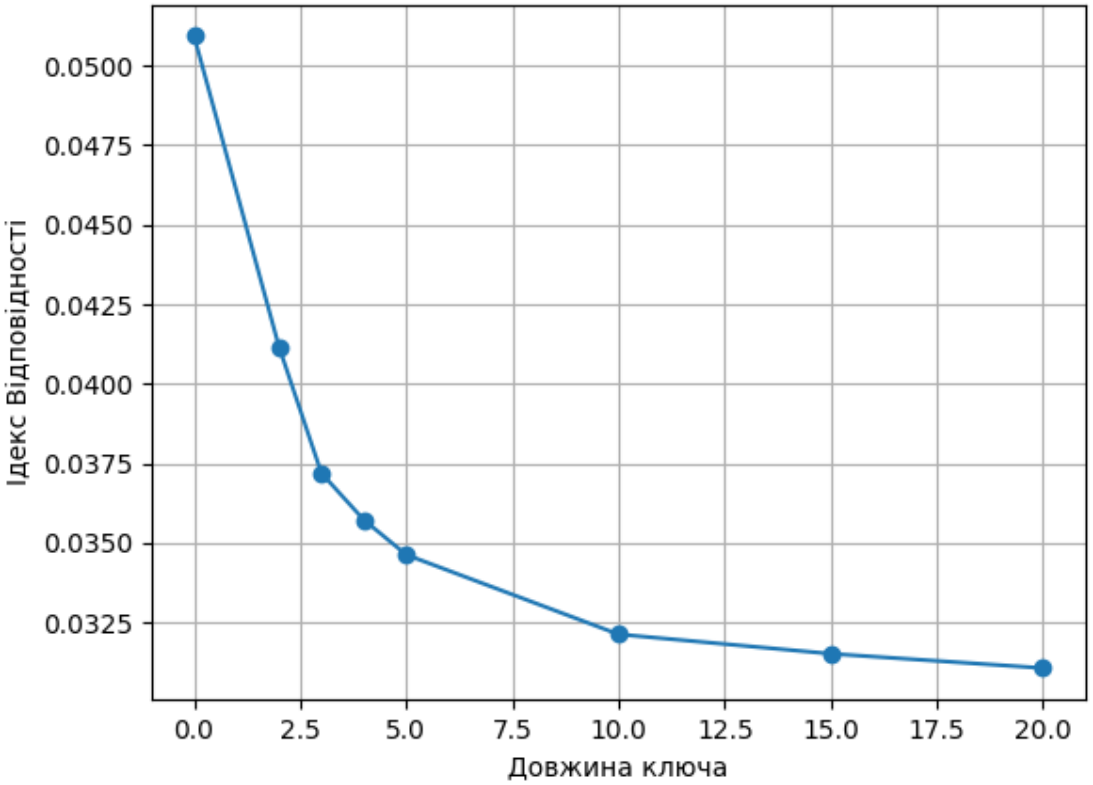
1. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
2. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
3. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
4. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Спочатку особливо небуло труднощів. Шифрування тексту далося доволі легко, також дешифрували для перевірки. Труднощі почалися на останньому етапі, де треба дефирувати текст. Довжину ключа знайшлася доволі легко(13), індекс відповідності зростав через кожні 13 символів - на 13, 26, 39 і т.д

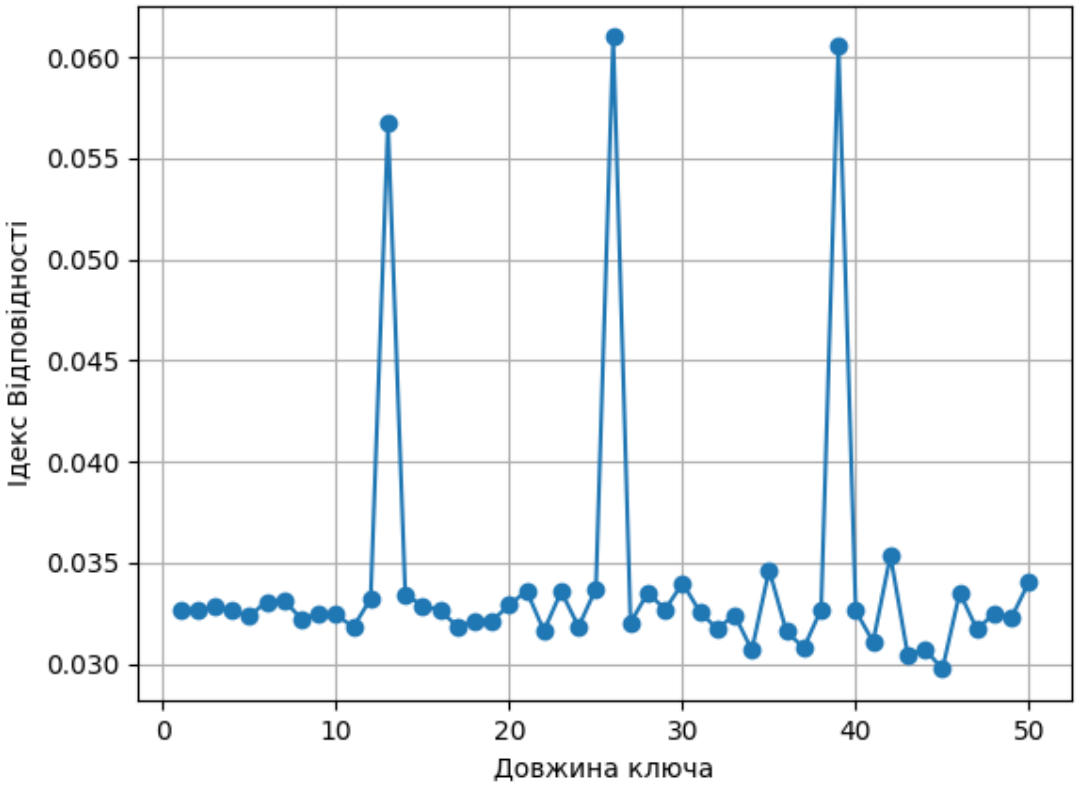
Саме знаходження ключа було складніше. Ми аналізували частоти літер у шифротексті і порівнювали із нормальною(середньою) частотою рос.літер. Таким чином, порівнюючи частоти ми визначаємо найбільш імовірний ключ.

Значення індексів відповідності для вказаних r:

```
Відкритий текст: 0.050935500937905824
Довжина ключа 2: 0.04116631662204266
Довжина ключа 3: 0.037190237228715416
Довжина ключа 4: 0.03572058422714957
Довжина ключа 5: 0.03462368866870815
Довжина ключа 10: 0.032122606469679724
Довжина ключа 15: 0.031512032449938276
Довжина ключа 20: 0.03106178421218583
```


Ідекс Відповідності
0.0500
0.0475
0.0450
0.0425
0.0400
0.0375
0.0350
0.0325
0.0
2.5
5.0
7.5
10.0
12.5
15.0
17.5
20.0
Довжина ключа

Одержання довжини ключа для наданого шифротексту:



Шифрований та розшифрований текст:

Ключ: ***громыковедьма***

Розшифрований текст:

старминскаяшколачародеевпифийитравницфакультеттеоретическойипрактическ
оймагиикафедрамаговпрактиковчастьперваясоциальныйукладбытинравывампирьей
общинывикачтовычтотоимеетепротиввампировраспринкорпорациямифкурсоваяра
ботаадептквосьмогокурсавольхиреднойнаучныйруководительмагистрпервойстепе
ниархимагксанперловдевятьсотдевяностодевятыйгодпобелорскомулетосчислению
городстарминведениехорошийсегоднявыдалсяденектеплыйбезветренныйвтораяд
екадасеноставамесяцанеспешносочилась сквозьклепсидрусолнечноголетаиголосазяб
ликовдоносившиесяизпридорожныхкустовзвенеливушахяехаласкозьихгнездовыеугод
ьякаквдольпограничнойполосыполосойбыладорогазаброшенныйпроклевывающийсяп
ыльнойтравойкривойбольшакзябликипопеременновозмущалисьвторжениемчеловека
набелойлошадивихчастныевладениязалихватскиетрелисменялисьхриплымчирикань
емптахисуетливоперепархивалиповеточкамтревожалиствуразноцветнаякаймавокр
угчерныхподсыхающихлужвзрывалась сотнямиистомленныхжароймотыльковраскруч
ивалась высьвихремтрепещущихкрыльевповодьязавернутыепетлейсвисалисередн
ейлукияпокачивалась вседлекакмешокскрупойпридерживаялевойрукойлежавшеенакол
еняхписьмоипытаясьразобратьпрыгающиепередглазамируныромашкапользовалась
моимрасслабленнымсостояниемвсезамедляяизамедляяшагнадеясьчтояувлеченнаяч
тениемнезамечуеековарногоманевраидамейостановитьсяиспокойнопощипатьтрав
кутычегоэтоголубушкаанушевеликопытамиплутоватаякобылкаразочарованновсхра

пнуладавайдавайхалтурщицаяустроиласьпоудобнейесливообщеможноустроитьсяпо
удобнейнатомпыточномпредметекоимявлялосьдляменяжесткоеказенноеседлонатр
етийденьпутиромашкинагриватоненькимиколечкамиспускаласьдопереднейлукизаби
ваясьмеждустраницамипухлогописьмакотороеядолжнабылавручитьповелителюдог
евыикотороеужеминутпятькаксамовольновскрылапripомощимагиинетронувесис
тойпечатинаверевочкенааломвоскеотчетливопроступалоттискперстнятринадца
тьруниперeплетающийсясдракономединорогвцентретутмоизанятиялитературой
дипломатиейигенеалогиейгрубопрервалиоченьгрубоядвауспелаподхватитьлистки
поползшиевразныестороныромашканеисправимаясаботажницазадумчивожевалаузду
бряцаяжелезомвтовремякакнезнакомыйивесьмаподозрительныйтипоброшейнаруж
ностидемонстративнопотрясалпередлошадиноймордойсамодельнымарбалетомсгр
язнойстрелоймногоразовогоиспользованиятакчтонепонятнобылокогооонсобирается
грабитьменяилиромашкуяприподняласьнастременахсинтересомрассматриваязарж
авленныйнаконечникянедумаючтоэтосамоеудачноеместодляторговлиантиквариат
омдоверительносообщилаянезнакомцувотвстарминеувасбыегосрукамиоторваливер
нееотрубилизнаетелитамоченьнелюбятразбойниковромашкаобнюхалаарбалетпрез
рительнофыркнулаинапрочьигнорируяграбителяпотянуласькаппетитнойзеленимал
инникаизвысокойгущикотороготолькочтовозниклоэточудовлаптяхпреступныйэлем
ентзаметносмутилсянаконечникзатрепеталкакщенячийхвостикувыдораскаянияипо
каяниябылоещедалекозаблудшаяовцаупорствовалавогрехесребролюбияануткаживос
лезайсконядевкаязыкатаякошелекилижизньдапошустрейслышишьяизобразилаусиле
ннуюработумыслиладноубедилкошелекпахнулоозономлицограбителяпередернулосьз
рачкирасширилисьглазаостекленелиионмедленноопустиварбалетотвязалибеспреко
словноподалмнетощиймешокболтавшийсяупоясаотмешкаразилокошкамиикуревомо
слабивверевкустягивавшуюгорловинуяпропустиласквозьпальцынесколькомелкихмон
етмаловатодорогоймоймаловатосленцойработаешьбезогонькавпрочемтакужибыт
ьвозьмувкачествеавансаосчастливилаяграбителяшвыряяемуподногипустоймешоки
предупредилаячерезпаруднейэтойжедорогойназадпоедутакужбудьдобрпостарайсям
енянеразочароватьмужикнеотрываяотменязагипнотизированноговзглядамедленно
нагнулсяподнялмешокизастылстолбстолбомневсилахшевельнутьсябезмоеговедом
акактолькогореграбительскрылсяизвидуядеактивировалазаклинаниеипозволиларом
ашкеперейтисгалопаналюбимуюеютрусцуписьмозажатоевовремяподсчетаденегуме
нямеждуколеняминемногопомялосьиутратилотоварныйвидвпрочемрассудилаяглавн
оенеоформлениеасодержаниеоноежекомпенсировалонедостаткирепейноголистаисп
ользованноговукромномместеагавотнаконециобомнепарастрокзадифирамбамизага
дочномуарракктурупропустишьинезаметишьзавремяобученияввысшейшколечароде
евпифийитравницадептkавольхапроявиласебязнаюоченьплохонеусидчиванетерпели
васвоевольназнакомаяпеснялюбитзлыешуткиинеоднократнопереноситихсвоспитан
никовнавоспитателейэтоонпроведрочтолидабылоодноведеркодовольнообъемистое
стоялосебенабалкенаддверьюмоейкомнатыэдакийсамодельныйкапканнасоседейпош
кольномуобщежитиюдабынеповаднобылобезспросуодалживатьуменяконспектыикас
трюлиснавареннымнанеделюборщомможетучительтакбынеразозлилсяеслибыведро
всетакиопрокинулосьанеупалоемунаголовустоймявместесводойотличаетсяредкими
способностямикпрактическойитеоретическоймагиисильноразвитойинтуициейбыс
троадаптируетсякнестандартнойситуациихаможетяещенебезнадежнанеприлична
якакаятограницаудогевыуэльфоввысокиетравыугномовскалыувадлаковгрудывыбро
шеннойнаповерхностьземлиудриаддубыподметающиеоблакаудруидовкаменныекруги
улюдейоблупленныестеныканалысзатхлойводойразделенныепаройтройкойподъемн

ыхмостовдалысыестражникипринихбдительнодремлющиеупираясьнаржавыеалебар
дыаздесьосиныиздевательствокакоетоособенноеслиучестьчтожителидогевывампи
рыхорошиетакиеосиныесеребристыетрепещущиезаосинамищекочетнебоостроверх
ийеловыйковерсредикоторогокоегдепроглядываютзатравленныеберезкиисосенкиса
мажедогевалежитвдолинекакплюшканаднерасписнойпиалыеслисмотретьсхолмакра
япиалывиденбелыйободокизосинвторойпотолщепотемнееизелейавцентреширокоез
еленоедноскрапочкамисамадогевавкольцевозделанныхполейиоблакахтуманаподойде
шьвплотнуюкдеревьямнаставлялменяучительипошлешьмысленныйсигналвглубьлес
алюбойможешьдуматьочемугоднолишьбысформироватьмощнуютелепатическуюово
лнуакомумнееенаправитьнаобщейчастотектонибудьизстражейграницыуслышитяс
мущеннокашлянулалучшебыемуэтогонеслышатьнеобязательнопродумыватьочеред
нуюпакостьзнаюзнаютынанихсверхвсякоймерыгоразданонасейразпостарайсявоздер
жатьсяотоныхочемэтояхдаоволневампирыоченьвосприимчивыктелепатииисразуо
треагируютнаееприсутствиехотяинесмогутдоскональнорасшифроватьтакчтонап
ирайнаколичествоаненакачествоваттакясмотрюнадымящуюбанюнаморщивлоботу
сердияинамоюволнутутжереагируютпятьилишестьадептовкоторыеовеянныепаро
мвыбегаютиздверейивыпрыгиваютизоконатакованныевнезапноожившимивениками
рукибудущихколлегзанятышайкамиприкрывающимиотвениковсамоесокровенноеучи
тельусмиряетвеникиоднимдвижениембровиновзглядыадресованныешутниценедомы
тымиколлегаминесулятничегохорошегоясказалподуматьанетранслироватьзаклина
нияжальчтозагодыпроведенныевэтихстенахтытакиненаучиласьдуматьчтождумаю
стоюподосинойнаморщивлобиромашкаужечтотожуетзеленаяслюнасочитсяизчерны
хуголковбархатистыхгубразделенныхкольцамиудилтелепатироватьзначитсознате
льноделитьсямыслямискемнибудьдругимделюсьпоследнимизлесатянетпрохладойси
дящаянаветкеиволгаудивленнопокачиваетхвостомответнамоиумственныепотуги
либозанятиеоказалосьмненепозубамлибоошарашенныестражиграницыпопадалинам
естесраженныемоеймощнойдумоймоистараниявенчалисьуспехомминутчерезсорок
изаэтовремяяуспелапередуматьбольшечемзапредыдущиевосемнадцатьлетавотире
зультатагаподействовалоилионпроходилмимослучайноявпервыеувиделавампиравоз
можноеслибыонвозникизниоткудабылбледенкаксмертьинедвусмысленноскалилокров
авленныезубыябыегоиспугаласькаксобственноипланироваламоизнаниявобластивам
пироведениябазировалисьначеловеческихлегендахипреданияхотличавшихсяредкостн
ымпессимизмомктомужевсегравюрыкартиныгобеленынаскальнаяживописьизобража
ютвампировисключительноночьюивтемнотекрыльязубыкогтивсеэтокажетсятаки
мстрашнымиогромнымтолькопотомучтотолкомничегонельзяразглядетьдневнойсв
етразвеялореолужасавпухипрахприсолнечномсветенафонебескрайнихполейивысоки
хдеревьеввампирпоказалсямневозмутительномелкимибезобиднымправдаященеспе
шиласьапришлосьмнегалантнопредложилирукувоспользоватьсякоторойвпрочемяне
рискнулавампирулыбнулсяпоказавдлинныеклыкилюбойулыбнулсябыувидевкакясползл
асъехалапокрутомуромашкиномубокуперекинувповодьячерезголовулошадиявыжидаю
щеуставиласьнавампирастражграницыоказалсявышеменянаполголовыширокплеча
хивесьманедуренсобойдлинныетемныеволосыобрамлялиузкоезагорелоелицосложенн
ыезаспинойкрыльяпридаваливампирунекотороесходствосмороемдемономпосланнико
мсмертидесятиаршиннаястатуякоторогоукрашалаактовыйзалвысшейшколычерны
епронзительныечутьраскосыеглазавампираизучилимоюмалопривлекательнуювнешн
остьнотакинесумелиразгадатьчтозанейсокрыто

Шифрований текст: див Crypto_CP2_variants_2018

Висновок:
Аналізом ідексу відповідності ми знайшли довжину ключа(13). Далі, після нескінченного невдалого брутфорса, аналізом частоти букв - порівняли частоту букви з дефолт частотою в рус.мові, ми знаходимо необхідний зсув, щоб підібрати необхідний ключ