Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут ім. Ігоря Сікорського”
Фізико-технічний інститут

«Криптографія»
КОМП’ЮТЕРНИЙ ПРАКТИКУМ No2
Криптоаналіз шифру Віженера
Варіант4

Виконали:
Студенти 3 курсу
Групи ФБ-04
Осіпчук Антон
Подима Катерина

Мета роботи:

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

Постановка задачі:

0. Уважно прочитати методичні вказівкидо 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

Для виконання першого завдання ми використали текст із роману "Чорна рада", що, за аналогією з першим комп'ютерним практикумом, був спочатку відредагований.

Рандомно генерувались ключі довжиною 2-5 та 10-20 символів. Для усіх поразовано індекс відповідності.
Результати внесені у таблицю:

Довжина ключа	Ключ	Індекс відповідності
2	шм	0.03949581481796585
3	сбь	0.036679515622716256
4	цдюч	0.038847913298996735
5	тфтще	0.03693256806783551
10	кньфыккаыз	0.033717056825544336

11	жгхякххяцйт	0.033775956963632434
12	ччьурюъургет	0.03304734044061666
13	чюырзсэхвшшйю	0.0336058010091557
14	эчгучпевийщоцн	0.03205476403950236
15	зючемузецьчакрш	0.03209403079822776
16	швийчфвмэоъмцфэь	0.032480153925694207
17	ясыяъьзкшлжпщкащб	0.032807376915072545
18	дхфиржущчмлчйартчр	0.0335272674917049
19	снрлйощоаььпючоээзи	0.03288372894592749
20	ячьщбтшвфучзогйрндшг	0.031653370505864926

Для наступного завдання текст було поділено на блоки. Щоб знайти довжину ключа, до кожного з них було розраховано індекси відповідності:

Довжина ключа	**Індекс відповідності**
1	0.03263044225743963
2	0.032604641533356106
3	0.03257699135676468
4	0.032650882017613285
5	0.032535443566457684
6	0.03256047474074616
7	0.03271784961796955
8	0.03269169199663074
9	0.032514372292478666
10	0.03251756583831643
11	0.03271373565919388
12	0.032635472926334196

13	**0.05406857059071756**
14	0.032636645060993646
15	0.032435594314224256
16	0.03267471665611215
17	0.03268312302293296
18	0.0325688897981386
19	0.032664850427483204
20	0.03250727909722938

Бачимо, що довжина ключа - 13

За допомогою ключа “громыковедьма” ми змогли розшифрувати текст.

Decrypted text:

старминскаяшколачародеевпифийитравницфакультеттеоретическойипра
ктическоймагиикафедрамаговпрактиковчастьперваясоциальныйукладбы
тинравывампирьейобщинывикачтовычтотоимеетепротиввампировраспр
инкорпорациямифкурсоваяработаадептквивосьмогокурсавольхиреднойна
учныйруководительмагистрпервойстепениархимагксанперловдевятьсот
девяностодевятыйгодпобелорскомулетосчислениюгородстарминведени
ехорошийсегоднявыдалсяденектеплыйбезветренныйвтораядекадасеност
авамесяцанеспешносочиласьсквозьклепсидрусолнечноголетаиголосазяб
ликовдоносившиесяизпридорожныхкустовзвенеливушахяехаласкозьих
гнездовыеугодьякаквдольпограничнойполосыполосойбыладорогазабро
шенныйпроклевывающийсяпыльнойтравойкривойбольшакзябликипопер
еменновозмущалисьвторжениемчеловеканабелойлошадивихчастныевла
дениязалихватскиетрелисменялисьхриплымчириканьемптахисуетливопе
репархивалиповеточкамтревожалиствуразноцветнаякаймавокругчерных
подсыхающихлужвзрываласьсотнямиистомленныхжароймотыльковраск
ручиваласьввысьвихремтрепещущихкрыльевповодьязавернутыепетлейс
висалиспереднейлукияпокачиваласьвседлекакмешокскрупойпридержива
ялевойрукойлежавшеенаколеняхписьмоипытаясьразобратьпрыгающиеп
ередглазамируныромашкапользоваласьмоимрасслабленнымсостояниемв
сезамедляяизамедляяшагнадеясьчтоявлеченнаячтениемнезамечуеекова
рногоманевраидамейостановитьсяиспокойнопощипатьтравкутычегоэтог
олубушкаанушевеликопытамиплутоватаякобылкаразочарованновсхрапн

уладавайдавайхалтурщицаяустроиласьпоудобнейесливообщеможноустр
оитьсяпоудобнейнатомпыточномпредметекоимявлялосьдляменяжесткое
казенноеседлонатретийденьпутиромашкинагриватоненькимиколечкамис
пускалась доперед нейлукизабиваясьмеждустраницамипухлогописьмакот
ороеядолжнабылавручитьповелителюдогевыикотороеужеминутпятькакс
амовольновскрылаприпомощимагиинетронувувесистойпечатинаверевоч
кенааломвоскеотчетливопроступалоттискперстнятринадцатьруниперепл
етающийсясдракономединорогвцентретутмоизанятиялитературойдипло
матиейигенеалогиейгрубопрервалиоченьгрубоядеваупелаподхватитьли
сткипоползшиевразныестороныромашканеисправимаясаботажницазаду
мчивожевалауздубрящаяжелезомвтовремякакнезнакомыйивесьмаподозр
ительныйтипобросшейнаружностидемонстративнопотрясалпередлошад
иноймордойсамодельнымарбалетомсгрязнойстрелоймногоразовогоиспо
льзованиятакчтонепонятнобылокогоонсобираетсяграбитьменяилиромаш
куяприподняласьнастременахсинтересомрассматриваязаржавленныйнак
онечникянедумаючтоэтосамоеудачноеместодляторговлиантиквариатомд
оверительносообщилаянезнакомцувотвстарминеувасбыегосрукамиоторв
аливернееотрубилизнаетелитамоченьнелюбятразбойниковромашкаобню
халаарбалетпрезрительнофыркнулаинапрочьигнорируяграбителяпотяну
ласькаппетитнойзеленималинникаизвысокойгущикотороготолькочтовоз
никлоэточудовлаптяхпреступныйэлементзаметносмутилсянаконечникза
трепеталкакщенячийхвостикувыдораскаянияипокаяниябылоещедалекоза
блудшаяовцаупорствовалавогрехесребролюбияануткаживослезайсконяд
евкаязыкатаякошелекилижизньдапошустрейслышишьяизобразилаусиле
ннуюработумыслиладноубедилкошелекпахнулоозономлицограбителяпе
редернулосьзрачкирасширилисьглазаостекленелиионмедленноопустива
рбалетотвязалибеспрекословноподалмнетощиймешокболтавшийсяупояс
аотмешкаразилокошкамиикуревомослабивверевкустягивавшуюгорловин
уяпропустиласквозьпальцынесколькомелкихмонетмаловатодорогоймой
маловатосленцойработаешьбезогонькавпрочемтакужибытьвозьмувкачес
твеавансаосчастливилаяграбителяшвыряемуподногипустоймешокипред
упредилаячерезпаруднейэтойжедорогойназадпоедутакужбудьдобрпоста
райсяменянеразочароватьмужикнеотрываяотменязагипнотизированного
взглядамедленнонагнулсяподнялмешокизастылстолбстолбомневсилахш
евельнутьсябезмоеговедомакактолькогореграбительскрылсяизвидуядеак
тивировалазаклинаниеипозволиларомашкеперейтисгалопаналюбимуюе
ютрусцуписьмозажатоевовремяподсчетаденегуменямеждуколеняминем
ногопомялосьиутратилотоварныйвидвпрочемрассудилаяглавноенеофор
млениеасодержаниеоноежекомпенсировалонедостаткирепейноголистаис
пользованноговукромномместеагавотнаконециобомнепарастрокзадифир
амбамизагадочномуарракктурупропустишьинезаметишьзавремяобучени

яввысшейшколечародеевпифийитравницадепткавольхапроявиласебязна
юоченьплохонеусидчиванетерпеливасвоевольназнакомаяпеснялюбитзлы
ешуткиинеоднократнопереноситихсвоспитанниковнавоспитателейэтоон
проведрочтолидабылоодноведеркодовольнообъемистоестоялосебенабал
кенаддверьюмоейкомнатыэдакийсамодельныйкапканнасоседейпошколь
номуобщежитиюдабынеповаднобылобезспросуодалживатьуменяконспе
ктыикастрюлиснавареннымнанеделюборщомможетучительтакбынеразоз
лилсяеслибыведровсетакиопрокинулосьанеупалоемунаголовустоймявме
стесводойотличаетсяредкимиспособностямикпрактическойитеоретическ
оймагиисильноразвитойинтуициейбыстроадаптируетсякнестандартнойс
итуациихаможетяещенебезнадежнанеприличнаякакаятограницаудогевы
уэльфоввысокиетравыугномовскалыувадлаковгрудывыброшеннойнапов
ерхностьземлиудриаддубыподметающиеоблакаудруидовкаменныекруги
улюдейоблупленныестеныканалысзатхлойводойразделенныепаройтройк
ойподъемныхмостовдалысыестражникипринихбдительнодремлющиеуп
ираясьнаржавыеалебардыаздесьосиныиздевательствокакоетоособенноес
лиучестьчтожителидогевывампирыхорошиетакиеосинысеребристыетреп
ещущиезаосинамищекочетнебоостроверхийеловыйковерсредикоторогок
оегдепроглядываютзатравленныеберезкиисосенкисамажедогевалежитвд
олинекакплюшканаднерасписнойпиалыеслисмотретьсхолмакраяпиалыв
иденбелыйободокизосинвторойпотолщепотемнееизелейавцентрешироко
езеленоедноскрапочкамисамадогевавкольцевозделанныхполейиоблакахт
уманаподойдешьвплотнуюкдеревьямнаставлялменяучительипошлешьм
ысленныйсигналвглубьлесалюбойможешьдуматьочемугоднолишьбысфо
рмироватьмощнуютелепатическуюволнуакомумнееенаправитьнаобщейч
астотектонибудьизстражейграницыуслышитясмущеннокашлянулалучше
быемуэтогонеслышатьнеобязательнопродумыватьочереднуюпакостьзна
юзнаютынанихсверхвсякоймерыгоразданонасейразпостарайсявоздержат
ьсяотоныхочемэтояхдаоволневампирыоченьвосприимчивыктелепатиии
сразуотреагируютнаееприсутствиехотяинесмогутдоскональнорасшифро
ватьтакчтонапирайнаколичествоаненакачествоваттакясмотрюнадымящу
юбанюнаморщивлоботусердияинамоюволнутутжереагируютпятьилишес
тьадептовкоторыеовеянныепаромвыбегаютиздверейивыпрыгиваютизоко
натакованныевнезапноожившимивеникамирукибудущихколлегзанятыш
айкамиприкрывающимиотвениковсамоесокровенноеучительусмиряетве
никиоднимдвижениембровиновзглядыадресованныешутниценедомытым
иколлегаминесулятничегохорошегоясказалподуматьанетранслироватьза
клинанияжальчтозагодыпроведенныевэтихстенахтытакиненаучилась дум
атьчтождумаюстоюподосинойнаморщивлобиромашкаужечтотожуетзеле
наяслюнасочитсяизчерныхуголковбархатистыхгубразделенныхкольцами
удилтелепатироватьзначитсознательноделитьсямыслямискемнибудьдруг

имделюсьпоследнимизлесатянетпрохладойсидящаянаветкеиволгаудивленнопокачиваетхвостомвответнамоиумственныепотугилибозанятиеоказалосьмненепозубамлибоошарашенныестражиграницыпопадалинаместесраженныемоеймощнойдумоймоистаранияувенчалисьуспехомминутчерезсорокизаэтовремяяуспелапередуматьбольшечемзапредыдущиевосемнадцатьлетавотирезультатагаподействовалоилионпроходилмимослучайноявпервыеувиделавампиравозможноеслибыонвозникизниоткудабылбледенькасмертьинедвусмысленноскалилокровавленныезубыябыегоиспугаласькасобственноипланироваламоизнаниявобластивампироведениябазировалисьначеловеческихлегендахипреданияхотличавшихсяредкостнымпессимизмомктомужевсегравюрыкартиныгобеленынаскальнаяживописьизображаютвампировисключительноночьюивтемнотекрыльязубыкогтивсеэтокажетсятакимстрашнымиогромнымтолькопотомучтотолкомничегонельзяразглядетьдневнойсветразвеялореолужасавпухипрахприсолнечномсветенафонебескрайнихполейивысокихдеревьеввампирпоказалсямневозмутительномелкимибезобиднымправдаяещенеспешиласьапришлосьмнегалантнопредложилирукувоспользоватьсякоторойвпрочемянерискнулавампирулыбнулсяпоказавдлинныеклыкилюбойулыбнулсябыувидевкакясползласъехалапокрутомуромашкиномубокуперекинувповодьячерезголовулошадиявыжидающеуставиласьнавампирастражграницыоказалсявышеменянаполголовышироквплечахивесьманедуренсобойдлинныетемныеволосыобрамлялиузкоезагорелоелицосложенныезаспинойкрыльяпридаваливампирунекотороесходствосмороемдемономпосланникомсмертидесятиаршиннаястатуякоторогоукрашалаактовыйзалвысшейшколычерныепронзительныечутьраскосыеглазавампираизучилимоюмалопривлекательнуювнешностьнотакинесумелиразгадатьчтозанейсокрыто

Висновок:

У ході роботи ми проаналізували шифр Віженера. За допомогою індексів відповідності ми змогли розшифрувати текст, який був зашифрований цим шифром. Засвоїли методи частотного криптоаналізу і здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.