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

Криптографія

Комп’ютерний практикум №2

Криптоаналіз шифру Віженера

Варіант №7

Виконали:
Студенти III курсу
Групи ФБ-95
Філюк В.Р.
Яковенко І.О.
Перевірила:
Селюх П.В.

Київ – 2021

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).

Завдання 1:

Текст для шифрування**: "**Анна Каренина**"**

Ключі:

r = 2 ("ок")
r = 3 ("юнг")
r = 4 ("карл")
r = 5 ("добро")
r = 10 ("абитуриент")
r = 11 ("абракадабра")
r = 12 ("аббревиатура")
r = 13 ("автобиография")
r = 14 ("абстракционизм")
r = 15 ("безнравственный")
r = 16 ("абстрагироваться")
r = 17 ("безукоризненность")
r = 18 ("вероотступничество")
r = 19 ("достопримечательный")
r = 20 ("лжесвидетельствовать")

Зашифрований текст всіх ключів знаходиться в папці "samples"

Завдання 2:

Для відкритого тексту і отриманих в попередньому завданні шифротекстів необхідно було підрахувати значення індексів відповідності за формулою:

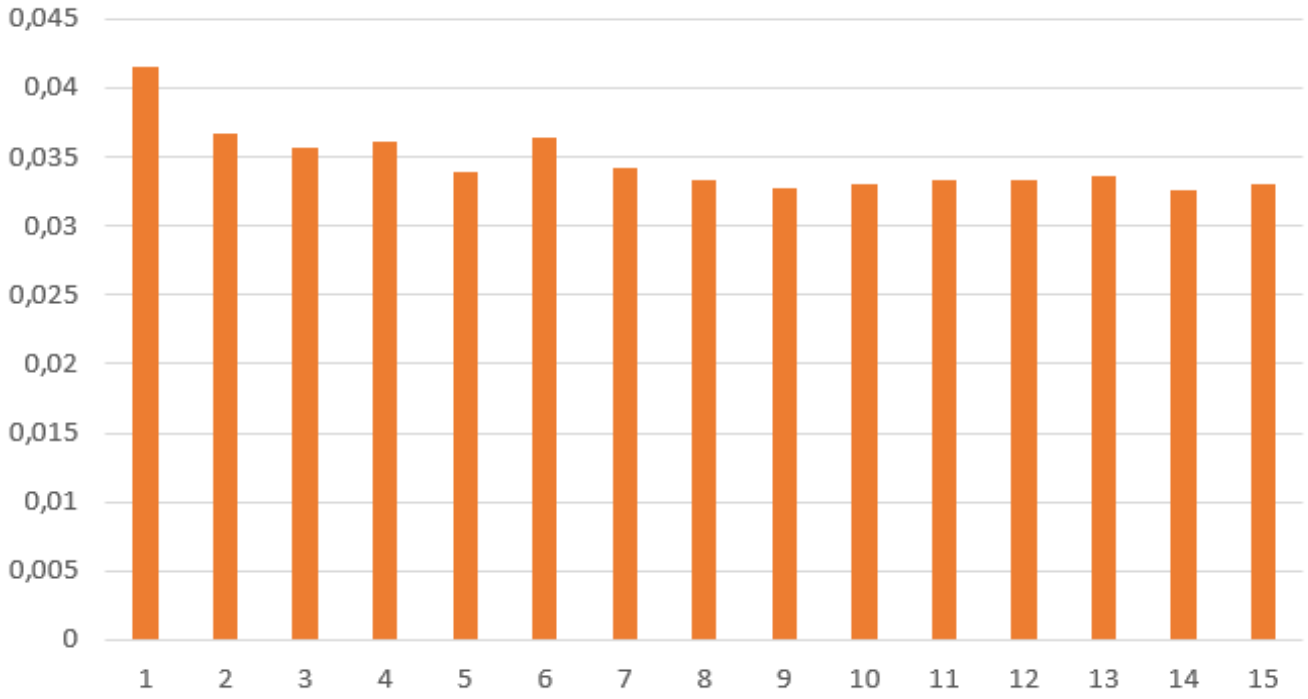
$$I(Y) = \frac{1}{n(n-1)} \sum_{t \in Z_m} N_t(Y)(N_t(Y)-1),$$

Для відкритого тексту **I = 0.051725509617763156**

Отримані індекси відповідності для вказаних значень **r** (довжини ключа):

Довжина	Ключ	Індекс відповідності
2	Ок	0.04145869979506963
3	Юнг	0.036634244014512776

4	Карл	0.035738788564177615
5	Добро	0.036171210361810716
10	Абитуриент	0.03388476873148918
11	Абракадабра	0.03633602960565197
12	Аббревиатура	0.034237802416873894
13	Автобиография	0.03331872483072929
14	Абстракционизм	0.03268068386986754
15	Безнравственный	0.0330052143078738
16	Абстрагироваться	0.033304581730989644
17	Безукоризненность	0.03336284484440337
18	Вероотступничество	0.03366149534243784
19	Достопримечательный	0.03262808140553253
20	Лжесвидетельствовать	0.03303088640013991



Завдання 3:

Після аналізу ШТ на індекси відповідності було знайдено що відповідні можливі довжини ключів це 15 та 30.

Розбивши ШТ на 15 підтекстів та виділивши з них найрозповсюдженішу букву для кожного підтексту ми отримала строку «оюбтохуроюгцъос». При розшифруванні її шифром Цезаря та беручи за ключ букви російського алфавіту з найбільшою частотою ми отримали наступні можливі ключі:

1. **«О» арудазевархимаг**
2. **«А» оюбтохуроюгцъос**
3. **«Е» йщьнйролйщюсхйм**
4. **«И» жцщкжнлижцыотжй**
5. **«Н» бсфебижгбсцйнбд**

Перспективним ключем є **«арудазевархимаг»,** результат - **прошлошятнадцат**

ШТ	**пабьлх**	**э**	**бтэхмвах**
Ключ	**арудаз**	**е**	**вархимаг**
ВТ	**прошло**	**ш**	**ятнадцат**

Буква ш не підходить, підбором дізнались що це буква «о». Отже ключ – **«арудазовархимаг».**

Розшифрований текст:

прошлопятнадцатьднейистарыйдомпостепенноначаложиватьсороклетвнемниктонежилпонастоящемузаэтовремяонсменило
диннадцатьхозяевнониктоизнихневыдерживалвподобномместебольшетрехмесяцевкреоливанессасталидвенадцатымимагпо
лностьюпогрузилсяврабоуонотрывалсятолькозатемчтобыпоестьаотснаизбавлялсязаклятиембессонницынодлякреолаэтояв
ноненепроходилобезнаказанноглазаунегопокраснелиавекинабряклииотвисливанессавсяческистараласьубедитьеговтомчтоем
уследуетпрекратитьиздевательстванадорганизмомихотьразоквыспатьсяпонастоящемуномагтолькоогрызалсязанималсяонд
вумяделаминеутомимописалмагическуюкнигуиокутывалособнякмагическойзащитойитоидругоетребовалоуймывремениакр
еолникакнемогрешитьчтодлянегоболеесрочнопоэтомузанималсяобоимиделамипопеременносначалаонвсерьезбеспокоилсяо
томчтозаегодушойвотвотявитсяужасныйтройнопотомутихомирилсярешивчтототскореевсегодаженезнаетовоскрешениista
ринноговрагапокрайнеймереванессаизбавиласьотдомашниххлопотбраунихубертнеизменносохраняяпостноевыражениелиц
аубиралсяготовилиобстирывалвсехжильцовобедыиужиныунегополучалисьоченьвкуснымихотяванессенеслишкомнравилос
ьчтоонтакналегаетнаэкзотическиерецептыповареннуюкнигукоторойонобычнопользовалсяоставилвдомеодинизегопрежних
владельцевзавзятыйгурманоднакобыловполнесъедобносамажеванессазасучиларукаваивплотнуюзаняласьрремонтомпервон

ачальноонапланировалананятьбригадурабочихчтобыонипривелиэтотсарайвпорядокновсталвопроскудавтакомслучаедевать весьэтотзоопаркбольшаячастьжильцовунормальногочеловекавызвалабывлучшемслучаесильноеудивлениепоэтомудевушка делалавсесамавсечтобылонужнооназаказывалапотелефонуобоикраскуклейпиломатериалыстеклогвоздиинструментыипроч иемелочивплотьдодверныхручекатакжегорукнижеквкоторыхтолковоразъяснялоськакделатьвдомеремонтсобственнымиру камиксчастьюдедванессыпоматеринскойлинииибылплотникомобожалмастеритьвсеподрядикоечемунаучилвнучкутакчтонач инатьейпришлосьнеснуляестественноводиночкуонамалочтосмоглабысотворитьтребовалисьпомощникипреждевсегоонакон фисковалаукреолаамулетслугивотужкогдахрустальномуподросткупришлосьпотрудитьсяпонастоящемувонгонялаегосутрад овечеранедаваяниминутыроздыхувпрочемонневозражалоднакоонабыстроубедилась чтоумагическогослугидействительнои меетсяряднедостатковонзачастуюпонималраспоряженияне совсемтаккактоткто их отдавалкпримеруванессаприказалаемувып илитьрейкидляновойлестницывродебывсевпорядкеперваярейкаполучилась простобезупречнойиванессаспокойноотправила сьпитькофеонавернулась черезполчасаиобнаружилачтосовершилаужаснуюошибкузабылауточнитьточноеколичествонеобхо димыхейреекслугаизвелтричетвертиимеющихсяунеедосокизавалилкомнатурейкамидопотолкадевушкабылавынужденазака затьновыедоскииломалатеперьголовукудадеватьстолькобесполезныхдеревянныхизделийтройвотличиеотсвоегодальнегоро дичаотличалсяредкимсластолюбиемидержалнетрехчетырехналожницкактогдаещенеархимагавсеголишьмагистркреоланеск олькосотенпричемменялонихоченьчастобольнаяфантазиямолодогонекромантагубилаеголюбовницсужасающейскоростьюо днаждыонзаглянулвшахшаноркогдаегохозяинотсутствовалкакужеупоминалосьтогдаэтидвоеещеневраждовалипоэтомутроя встретиликакгостясделаввсечтобыродичхозяиначувствовалсебяхорошоксожалениюпослетогокакмагплотноотобедаликакследу етвыпилемунаглазапопаласьоднаизрабыньеслибыдомабылсамкреолилихотябыегоуправляющийбедыудалосьбыизбежать ьноникто другойнеосмелилсяостановитьмагавозжелавшегопоразвлечьсясневольницейтройпробылснейоколочасаикогдавы шелвеселосообщилчтоондеслегкапопортилимуществосвоегородичаисобратапогильдиинопустьтотнерасстраиваетсяонтрой оставилвуплатузанеецелуюгорстьзолотыхйехровникто израбовничутьнезабеспокоилсяслучайбылсамыйчтонинаестьзаурядн ыйаплатавтроепревышаланормальнуюстоимостьрабынидажетакойкрасоткикактаэфиопскаятанцовщицакоторуютройслегка попортиливсебыобошлосьеслибыеслибырабынянеоказаласьлюбимойналожницейкреолаеслибынетотфактчтоонаносилапод сердцемребенкабудущеговерховногомагаеслибынеточтожестокийивспыльчивыймагпожалуйединственныйразвжизникогот ополюбилкогдакреолвернулсядомойиувиделточтоещевчерабыломолодойкрасивойженщинойонвпалвтакоебешенствочтораз рушилполовинусобственнойкрепостнойстеныиперебилнеменьшетридцатирабовприпадокещенезакончилсяамагужелетелвб уквальномсмыслекхешибудворцутроячтобыпродолжитьразрушениетаманадосказатьчтовтевременакреолужебылоднимизси льнейшихмаговшумераатройещенетнаследующийденькогдадомойвозвратилсяужетройпришлоеговремяполучатьшокотегод ворцавпрочемкудаменьшегочемукреолаостались лишьдымящиесяразвалиныкреолразворотилкаменнуюгромадувживыхнеос талосьниодногорабаниоднойналожницывсеонипогиблиотогняимолнийразгневанногомагакогдажетройобнаружилтелосвоег одесятилетнегосынаневинныйребенокбылутопленвбадьесрасплавленнымзолотомаемувроткреолзасунулмаленькуюглиняну ютабличкустремясловаминадеюсьплатадостаточнанадосказатьчтокреолоченьскорораскаялсявсодеянномидажепринесиску пительнуюжертвунаалтареиштардоэтогоднямагнеубилниодногоребенкаинепросторебенкаачленаодногоизсамыхименитыхр одовимперииегособственногоюныйэхтатожеведьприходилсякреолуродственникомивотличиеотсвоегоотцапереднимничемн епровинилсяноуженичегонельзябылопоправитьеслизаразрушенныйхешибиумерщвленныхрабовкреолмогзаплатитьвыкупу бийстворабавдревнемшумересчиталосьмелкимпреступлениемкотороеприравнивалосьпорчечужогоимуществатосмертьсы натройнепростилбыемунизакакиеденьгимолодоймагвозненавиделродичадоконцасвоихднейаужненавидетьтоэтотчеловекум елкакниктодругойсэтогоднятройжилоднойтолькоместьюразумеетсяоннебросилсявлобовуюатакутройнебылдуракомипоним алчтоскреоломемунетягатьсяонисчезизшумерапочтинатридцатьлетнокогдавернулсянеизвестногдеегоносилостольколетнов ернулсяонужеархимагомиоченьбыстрозанялбылоеместоприимператорскомдворепримернозагоддоеговозвращениякреолзан ялпостверховногомагаитройнемедленнопринялсяинтриговатьпытаясьподсидетьбывшегоприятеляатеперьсамогозаклятогов рагавстречаясьвбашнегильдиикреолитройлюбезнораскланивалисьпрячазафальшивымиулыбкамизвериныеоскалывозвраща ясьжедомойонинемедленнопринималисьстроитькознидругпротивдругаособенностаралсятройзадвадцатьлеткреолупришлос ьприкончитьстольконаемныхубийцчтоизнихможнобылосформироватьнебольшуюармиюсрединихпопадалисьсамыеразные твариотобычныхлюдейдомогущественныхдемоновособенноартодуиартераидузапомнилсязомхокобжуткоесуществопохоже енаизуродованногокальмараразмеромсчетырехслоновпоставленныхдругнадругакакужтроюудалосьдоговоритьсясэтиммонс тромнеизвестноновпрошломгодуонвыползизевфратаисухимпутемдошелдосамогоурагигантбилсяокрепостныестеныпочтид воесутокпокакреолполивалегосотнямиразрушительныхзаклятийточтовконцеконцовосталосьотчудовищаможнобылозапихн утьвшкатулку

Висновок:

Під час виконання лабораторної роботи ми навчились роботі та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера, крім того познайомились з методами частотного аналізу та криптоаналізу. Також ми змогли все-таки розшифрувати наданий шифротекст та знайшли ключ.