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

Виконала:
студентка гр. ФБ-83
Григор’єва Ольга

Перевірив:
Чорний О.М.

Київ – 2020

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

Завдання:

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.**
   Для шифрування було обрано уривок з книги «Алхімік»

ДОВЖИНА КЛЮЧА	КЛЮЧ	ЗАШИФРОВАНИЙ ТЕКСТ
2	«да»	уоыеруъафьфалгтвдрмвдецсуахтчхтмхмчщйнсомилурлйнсохпфо …
3	«нет»	ьуйтсегевйхтфиапевхзттчгьегяшзысгщшлттяынъфшюшкяъугьха …
4	«идея»	чтьдфчыяшахяпзубифнбийчрчдцсыщулщршшнстнрммтфпкмхтц …
5	«мечта»	ыуочмяычвььеюхооезъвмкйгпмцйехъсиюуекдяофнюемчкдяоэфз …
14	«вселенназнает»	сяьрсагапгэамхруеынпнесшьацдхжучцщащддфъонъйдсцкъъорцэо …

2. **Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.**

ДОВЖИНА КЛЮЧА	КЛЮЧ	ІНДЕКС ВІДПОВІДНОСТІ
2	«да»	0.0446437
3	«нет»	0.0391554
4	«идея»	0.0399602
5	«мечта»	0.0352995
14	«вселеннаязнает»	0.0336882
Відкритий текст		0.0551891

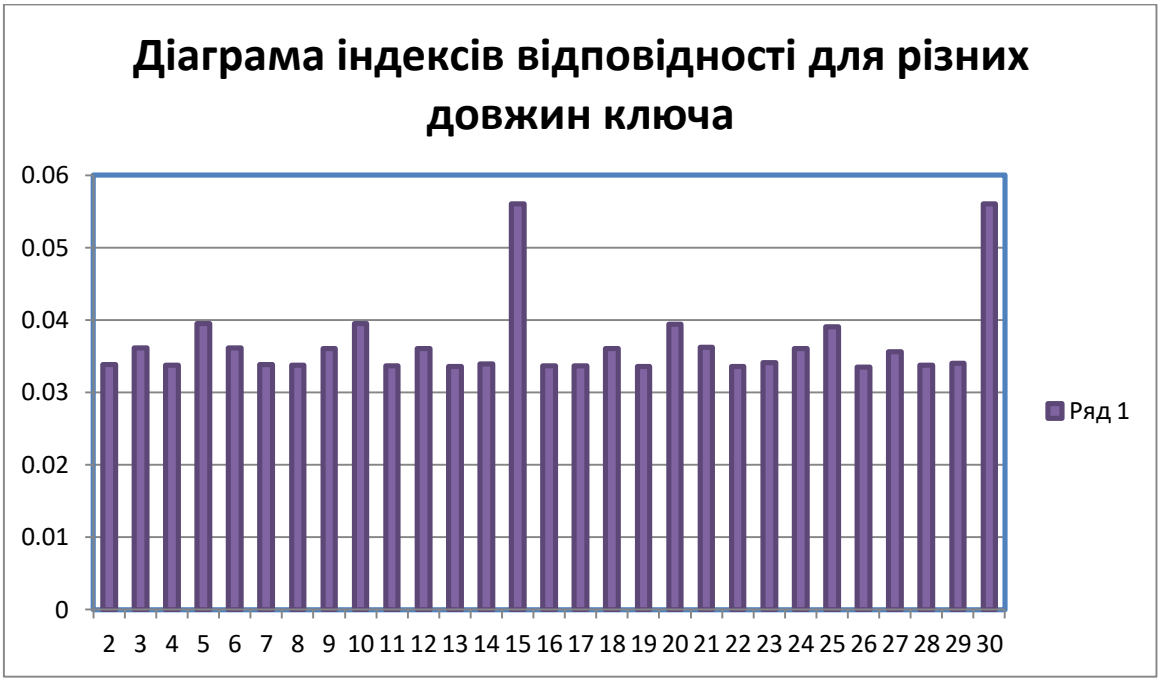
3. **Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).**

Варіант №7

Обчислюю індекс відповідність для різних довжин ключей:

2	3	4	5	6	7	8
0.0338539	0.0361519	0.0337429	0.0395208	0.0361251	0.0338218	0.0337409
9	10	11	12	13	14	15
0.0360828	0.0395225	0.0336765	0.0360449	0.0335752	0.0339246	0.0560518
16	17	18	19	20	21	22
0.0336833	0.0336887	0.0360899	0.0335364	0.0393894	0.0361939	0.0335947
23	24	25	26	27	28	29
0.0340865	0.0360876	0.0390172	0.0334689	0.0356404	0.0337276	0.0340443
30						
0.0560031						

Отже, довжина ключа 15 або 30.



Далі за допомогою частотного аналізу знаходжу літеру, яка найчастіше трапляється у кожному з 15 блоків шифрованого тексту, роблю припущення, що це літера «о» у відкритому тексті, потім знаходжу ключ:

0, 16, 19, 4, 0, 7, 5, 2, 0, 16, 21, 8, 12, 0, 3 – отримана послідовність відповідає такому ключу:

«АРУДАЗЕВАРХИМАГ», при розшифруванні з чим ключем деякі літери відкритого тексту були спотвореними, отже шукаю, в якому саме блоці припущення про літеру «о» було не вірним, це виявився блок 7, правильний ключ має вигляд:
«АРУДАЗОВАРХИМАГ».

Розшифрований текст:

прошлопятнадцатьднейистарыйдомпостепенноначаложиватьсороклетвнемниктонежилпон
астоящемузаэтовремяонсменилодиннадцатьхозяевниктоизнихневыдерживалвподобном
местебольшетрехмесяцевкреоливанессасталидвенадцатымимагполностьюпогрузилсяврабо
туонотрывалсятолькозатемчтобыпоестьаотснаизбавлялсязаклятиембессонницынодлякрео
лаэтоявнонепроходилобезнаказанноглазаунегопокраснелиавекинабряклиотвисливанесса
всяческистаралась убедитьеговтомчтоемуследуетпрекратитьиздевательстванадорганизмом
ихотьразоквыспатьсяпонастоящемуномагтолькоогрызалсязанималсяондвумяделаминеуто
мимописалмагическуюкнигуиокутывалособнякмагическойзащитойитоидругоетребовалоу
ймывремениакреолникакнемогрешитьчтодлянегоболеесрочнопоэтомузанималсяобоимиде
ламипопеременносначалаонвсерьезбеспокоилсяотомчтозаегодушойвотвотявитсяужасныйт
ройнопотомутихомирилсярешивчтототскореевсегодаженезнаетовоскрешениистаринногов
рагапокрайнеймереванессаизбавиласьотдомашниххлопотбраунихубертнеизменносохраняя
постноевыражениелицаубиралсяготовилиобстирывалвсехжильцовобедыиужиныунегопол
учалисьоченьвкуснымихотяванессенеслишкомнравилосьчтоонтакналегаетнаэкзотические
рецептыповареннуюкнигукоторойонобычнопользовалсяоставилвдомеодинизегопрежнихв
ладельцевзавзятыйгурманоднакобыловполнесъедобносамажеванессазасучиларукаваивпло

тнуюзанялась рремонтомпервоначальноонапланироваланантьбригадурабочихчтобыонипр
ивелиэтотсарайвпорядокновсталвопроскудавтакомслучаедеватьвесьэтотзоопаркбольшаяча
стьжильцовунормальногочеловекавызвалабывлучшемслучаесильноеудивлениепоэтомудев
ушкаделалавсесамавсечтобылонужноонаказывалапотелефонуобоикраскуклейпиломатер
иалыстеклогвоздиинструментыипрочиемелочивплотьдодверныхручекатакжегорукнижекв
которыхтолковоразъяснялоськакделатьвдомеремонтсобственнымирукамиксчастьюдедва
нессыпоматеринскойлинииибылплотникомобожалмастеритьвсеподрядикоечемунаучилвнуч
кутакчтоначинатьейпришлосьнеснуляестественноводиночкуонамалочтосмоглабысотворит
ьтребовалисьпомощникипреждевсегоонаконфисковалаукреолаамулетслугивотужкогдахру
стальномуподросткупришлосьпотрудитьсяпонастоящемувонгонялаегосутрадовечеранедав
аяниминутыроздыхувпрочемонневозражалоднакоонабыстроубедилась чтоумагическогослу
гидействительноимеетсяряднедостатковонзачастуюпонималраспоряженияснесовсемтаккак
тотктоихотдавалкпримеруванессаприказалаемувыпилитьрейкидляновойлестницывродебы
всевпорядкепервуярейкаполучилась простобезупречнойиванессаспокойноотправилась пить
кофеонавернулась черезполчасаиобнаружилачтосовершилаужаснуюошибкузабылауточнит
ьточноеколичествонеобходимыхейреекслугаизвелтричетвертиимеющихсяунеедосокизава
лилкомнатурейкамидопотолкадевушкабылавынужденазаказатьновыедоскииломалатеперь
головукудадеватьстолькобесполезныхдеревянныхизделийтройвотличиеотсвоегодальнегор
одичаотличалсяредкимсластолюбиемидержалнетрехчетырехналожницкактогдаещенеархи
магавсеголишьмагистркреоланесколькосотенпричемменялонихоченьчастобольнаяфантази
ямолодогонекромантагубилаеголюбовницсужасающейскоростьюоднаждыонзаглянулвшах
шаноркогдаегохозяинотсутствовалкакужеупоминалосьтогдаэтидвоеещеневраждовалипоэт
омутроявстретиликакгостясделаввсечтобыродичхозяиначувствовалсебяхорошоксожалени
юпослетогокакмагплотноотобедаликаксследуетвыпилемунаглазапопалась ьоднаизрабыньесл
ибыдомабылсамкреолилихотябыегоуправляющийбедыудалосьбыизбежатьниктодругой
неосмелилсяостановитьмагавозжелавшегопоразвлечьсяневольницейтройпробылснейокол
очасаикогдавышелвеселосообщилчтоондеслегкапопортилимуществосвоегородичаисобрат
апогильдиинопустьтотнерасстраиваетсяонтройоставилвуплатузанеецелуюгорстьзолотыхй
ехровниктоизрабовничутьнезабеспокоилсяслучайбылсамыйчтонинаестьзаурядныйаплатав
троепревышаланормальнуюстоимостьрабынидажетакойкрасоткикактаэфиопскаятанцовщи
цакоторуютройслегкапопортиливсебыобошлось еслибыеслибырабынянеоказалась любимо
йналожницейкреолаеслибынетотфактчтоонаносилаподсердцемребенкабудущеговерховног
омагаеслибынеточтожестокийивспыльчивыймагпожалуйединственныйразвжизникоготопо
любилкогдакреолвернулсядомойиувиделточтоещевчерабыломолодойкрасивойженщинойо
нвпалвтакоебешенствочторазрушилполовинусобственнойкрепостнойстеныиперебилнемен
ьшетридцатирабовприпадокещенезакончилсяамагужелетелвбуквальномсмыслекхешибудв
орцутроячтобыпродолжитьразрушениетаманадосказатьчтовтевременакреолужебылодним
изсильнейшихмаговшумерааатройещенетнаследующийденькогдадомойвозвратилсяужетро
йпришлоеговремяполучатьшокотегодворцавпрочемкудаменьшегочемукреолаостались лиш
ьдымящиесяразвалиныкреолразворотилкаменнуюгромадувживыхнеосталосьниодногораба
ниоднойналожницывсеонипогиблиотогняимолнийразгневанногомагакогдажетройобнаруж
илителосвоегодесятилетнегосынаневинныйребенокбылутопленвбадьесрасплавленнымзолот
омаемувроткреолзасунулмаленькуюглинянуютабличкустремясловаминадеюсьплатадостат
очнанадосказатьчтокреолоченьскорораскаялсявсодеянномидажепринесискупительнуюжер

твунаалтареиштардоэтогоднямагнеубилниодногоребенкаинепросторебенкаачленаодногои
зсамыхименитыхродовимпериигособственногоюныйэхтатожеведьприходилсякреолуродс
твенникомивотличиеотсвоегоотцапереднимничемнепровинилсяноуженичегонельзябылоп
оправитьеслизаразрушенныйхешибиумерщвленныхрабовкреолмогзаплатитьвыкупубийств
орабавдревнемшумересчиталосьмелкимпреступлениемкотороеприравнивалоськпорчечуж
огоимуществатосмертьсынатройнепростилбыемунизакакиеденьгимолодоймагвозненавиде
лродичадоконцасвоихднейаужненавидетьтоэтотчеловекумелкакниктодругойсэтогоднятро
йжилоднойтолькоместьюразумеетсяоннебросилсявлобовуюатакутройнебылдуракомипони
малчтоскреоломемунетягатьсяонисчезизшумерапочтинатридцатьлетнокогдавернулсянеиз
вестногдеегоносилостольколетновернулсяонужеархимагомиоченьбыстрозанялбылоеместо
приимператорскомдворепримернозагоддоеговозвращениякреолзанялпостверховногомагаи
тройнемедленнопринялсяинтриговатьпытаясьподсидетьбывшегоприятеляатеперьсамогоза
клятоговрагавстречаясьвбашнегильдиикреолитройлюбезнораскланивалисьпрячазафальши
вымиулыбкамизвериныеоскалывозвращаясьжедомойонинемедленнопринималисьстроитьк
ознидругпротивдругаособенностаралсятройзадвадцатьлеткреолупришлосьприкончитьстол
ьконаемныхубийцчтоизнихможнобылосформироватьнебольшуюармиюсрединихпопадали
сьсамыеразныетвариотобычныхлюдейдомогущественныхдемоновособенноартодуиартера
идузапомнилсязомхокобжуткоесуществопохожеенаизуродованногокальмараразмеромсчет
ырехслоновпоставленныхдругнадругакакужтроюудалосьдоговоритьсясэтиммонстромнеиз
вестноновпрошломгодуонвыползизевфратаисухимпутемдошелдосамогоурагигантбилсяок
репостныестенынопочтидвоесутокпокакреолполивалегосотнямиразрушительныхзаклятийто
чтовконцеконцовосталосьотчудовищаможнобылозапихнутьвшкатулкузн

Висновки:

У даній роботі я навчилась шифрувати тексти шифром Віженера та на прикладі декількох ключів різної довжини виявила, що ефективність ключа можна визначити за обчисленим індексом відповідності шифротексту (чим більше значення індексу наближено до індексу відповідності для відкритого тексту, тип слабший ключ, тобто краще вибирати ключі більшої довжини (10-20) та не використовувати літеру «а» у ключі). Також, за допомогою алгоритму, описаного у методичних вказівках, мені вдалось за інформацією, отриманої після обчислень індексів відповідності, знайти довжину ключа, використовуючи частотний аналіз, відновити ключ, та у результаті отримати відкритий текст.