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 - 9

Виконав:
студент гр. ФБ-81

Кудін І.А.

Перевірив:
Чорний О.М.

Київ – 2020

Мета:

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

Завдання 1:

У якості тексту для шифрування ключами з різною довжиною обрано уривок із збірки оповідань «Темні Алеї» Івана Буніна.

Індекс відповідності відкритого тексту - 0.05543442127801032

Індекс відповідності шифртексту у варіанті 9 - 0.0350613220600444

Довжина ключа	Індекс відповідності шифртексту
2	0.0432986622118137
3	0.038962686923639585
4	0.038976822264819605
5	0.03840815911389933
10	0.0339774607923005
11	0.033274755612949014
12	0.03324713483133289
13	0.03491867954466654
14	0.032966052759592294
15	0.035824803656861505
16	0.0335737099551471
17	0.03517246578516296
18	0.03439437211951805
19	0.03293648227574444
20	0.033601493211949204

Найбільш близьке до індексу відповідності шифртексту варіанту 9 значення, відповідає довжині ключа 17.

Завдання 2:

Для знаходження довжини ключа використано наступний алгоритм:

Для знаходження істинного значення r за допомогою індексу відповідності пропонується два можливих алгоритми. Перший алгоритм виглядає так:

1) Для кожного кандидата $r = 2,3,...$ розбити шифртекст Y на блоки $Y_1, Y_2, ..., Y_r$.
2) Обчислити значення індексу відповідності для кожного блоку.
3) Якщо сукупність одержаних значень схиляється до теоретичного значення I для даної мови, то значення r вгадане вірне. Якщо сукупність значень схиляється до значення $I_0 = \frac{1}{m}$, що відповідає мові із рівноімовірним алфавітом, то значення r вгадане неправильно.

Теоретичне значення індексу відповідності ≈ 0.05543442127801032

```
11 0.018181818181818
12 0.015151515151515152
13 0.02564102564102564
14 0.04395604395604396
15 0.06666666666666667
16 0.058333333333333334
17 0.051470588235294115
18 0.0457516339869281
19 0.04678362573099415
```

Як бачимо, значення індексу відповідності шифротексту найбільш близько до теоритичного значення між 16 та 17. Отже довжина ключа або 17 або 16. Робимо припущення, що довжина 17.

Завдання 3:

Для букви ‘о’ я отримав такий ключ:

```
боаяаоахчэндшпиэь
```

Я перевірив, що довжина ключа та функція для його знаходження вірні, але для багатьох блоків треба брати іншу за частотою букву.

Зробивши вивід можливих букв ключа, для перших п`яти за частотою букв російської мови я отримав по п’ять варіантів для кожної букви ключа:

```
бкпзв,очьфп,айожб,яинеа,айожб,очьфп,айожб,хюгыц,чаеэш,эжлгю,нцыуо,днтке,шбжющ,пшэхр,исцой,эжлгю,ьеквэ,
```

Перебравши кілька варіантів, я зробив висновок, що ключ: **“войнамагаэндшпиль”**(у відповідності до ключа для найчастішої букви “о”).

Потрібні букви я не знайшов тільки у двох блоках, але їх можна легко встановити інтуїтивно.

Помістивши ключ у ф-ю розшифрування я отримав змістовний текст, тож ключ вірний.

Дешифрований текст:

путьстарогозамканакраснойскалеплывущейнадневедомойбезднойможетпоказатьсявечным
инеизменнымнаднимполыхаютпричудливыесозвездияветервыводитзамысловатыеруладын
азубцахегостенибашеннекогданатомчтопослужилоосновaниемкрепостинаходилиприютса
мыеудивительныесозданиядотехпорпоканеобъявилисьнастоящиехозяеваонииименовалисеб
яновымибогамиодинизнихвозвелнакраснойскалесвойзамоктвердынюкраснойскалебылосов
ершеннобезразличнокакихзовутэтихнезваныхгостейотчеготосразувозомнившихсебяхозяев
амионаплылаиплыласебекоднойейведомойцелииникогданиразукурсеенеизменялсямалокто
виделсходствоскалыипоявившегосянанемзамкасбрандеемтакимжелетучимостровомслугха
осаихкрепостиуничтоженнойратямихединаиракотатоткогозвалихединомвиделвтотвечерко
гданазваныебратьябогипокинулитайнуютвердынюхединавзамкевоцариласьтугаязвенящаят
ишинаниктоневиделкакнапочтительномрасстоянииотстенбашенибастионовкрепостиввозд
ухеизничегосоткаласьчеловеческаяфигураповиселакакоетовремяазатемтакжебеззвучнорас
таялазамокпустовалиниктопомнениюхединанезналтудадорогиниединаяживаядушанескры
валасьзастенаминичьиглазаневсматривалисьвдальсверхотурыбашеннекомубылозаметитьф
игуруникомуничегонесказалибыпроделанныееюсложныепассыоднакосамаскаладрогнулаи
чутьчутьсамуюмалостьноизменилакурсвзатянутыхтуманамибезднахподосновойлетающей
громадывспухлонесколькосмутныхогненныхпятенинепоймешьтолиэтоодинокиекострыуст
авшихпастуховтолипоследниемгновенияцелыхмировгибнущихвпламеннойагониивечерпот
рясениявступилвсвоиправаадалекодалекоотзачарованногозамканадбезднойнебокирддинап
ослушнораскрылосьраздаваясьсловноутробароженицыдвоебессчетныевекаименовавшиедр
угдругабратьяминовыебогиупорядоченноговступаливмиродинизмножествасредьдоверенн
огоимвладенияихподмастерьяужедействовализдесьипотерпелинеудачустремительнаягелер
рапривсехеталантахничемнемоглапомочьмирупогибающемусловноотвампирьегоукусанд
апротянулракоткогдадвоебоговочутилисьнакраювзметнувшейсякподнебесьюскалыделодл
яэйвилькогдаонанаконецокажетсяздесьповремениэтогомиранаверноечерезседьмицурассе
янноотликнулсяхединсовершеннопочеловеческиприставляяладоньиокидываявзглядомши
рокуюпанорамуостроесловноклыкневедомогочудищанасквозьпронзившееземнуютвердька
менноенавершиеподниматьсяоблакамвернееподниматьсябыпотомучтооблакаужедавноис
чезлиснебесобреченногомираисаминебесасловновыгорелиголубизнуразбавилогнилостнозе
леножелтымлесадалековнизутихооблеталигорестношуршапоследнимилистьямиприготови
вшиськсмертисловнодоблестныенезнающиеотступленияойцыпроигравшеговойскапервы
йвторойшестойдевятыйжелезныйиодиннадцатыйлегионывновькакинасвиллеимвыпалозащ
ищатьимпериютольковрагнасейразсовсемужедругойподкрепленийматоподтянулосьвпосле
днийматоментрикогортыпятнадцатоголегионаноивсеостальноенавостокетретийпятыйдесят
ыйдвенадцатыйдвадцатьпервыйидвадцатьвторойподкомандованиемграфатарвусастоятнас
уоллесдерживаяразинувшихротначужойкаравайгерцоговикоролевичейсемандрычетырнад
цатыйишестнадцатыйлегионыскорыммаршемотходятсбуревойгрядыпополуночномутракту
послесвилльскойбитвынапиравшиепотрактуотзебераидемтасемандрийцыпоспешноушлина
юготступиликдебруилушонугдестоялизащищаябогатыйремесленныйгороддвадцатыйлегио
ниместноеополчениесовсемнедавнособранныевосемнадцатыйидевятнадцатыйлегионыобо
ронявшиеилдарнадавилинапротивостоявшихимисемандрадрогнулауходяпотрактунасаледр
уимперскиекогортыпродвигалисьследомседьмойлегионпочтивполномсоставепогибшийнас
елиновомвалумедленновозрождалсявгородахблизнецахделинеидавинепокрывшийсебяпозо
ромсемнадцатыйрасформированитакогономераввойскеимпериияникогдауженепоявитсячет
вертыйвосьмойитринадцатыйлегионыгоняютсяпопобережьюзапиратамиоднозадругимвыж
игаяразбойничьиезданиоднойкогортыоттудаимператорвзятьбыужеуспелмятежныебароныо
тошлинасеверисеверовостокмельинавобширныеобластимеждупояснымиполуночнымтракт

амизахватилиострагхвалиниежелинпопрятались взамкахразгромнаягоднойгрядепохожеосн овательноостудилгорячиеголовыглавнаяжеармияимперииготовиласькрешительномубоюпр оделавдальнийпутьсвосточногокраяогромногогосударстваназападныйонавсталавоборонук аждыймигожидаяударавырвавшихсяизразломатварейоблеченныхуязвимойплотьюкакутвер ждаладептвсебесцветногонергаонжеобещалпомощьлегионамданепростуюсулилчтоплечоп одставятдревниесилымельинакоторыенаконецтонайдутсебедостойногопротивникалегионе рытрудолюбивыесловномуравьипревращалиневысокуюгрядухолмоввнеприступнуюкрепос тьпогребнювозвелитрехрядныйпалисадпромежуткимеждурядамизасыпализемлейуподошв ынапротиввыкопалировширинойвтричеловеческихростаиглубинойвдвалюдиработалиидне миночьюногномывставшиеподстягцарьгорыивасилискапревзошливыносливостьювсехони похожевообщенеотдыхалиинеелиорудуякиркамиизаступамиточнозаведенныеотверженные ипроклятыекаменнымпрестоломэтигномысвязалисвоюсудьбусимпериеймалопомалуначин авшуюпревращатьсявточтовиделосьеемолодомуправителюкогдаонтолькотольковсходилна престолгосударствогдекаждыйнайдетсебеместоеслинестанеттянутьодеялонасебяисвоиххо лмыпреграждалитварямразломадорогунавостокразумеетсянастоящийполководецрасполага ятакимисиламипопытался бы обойтиукрепившиесялегионыударитьпотыламифлангамвзятьв кольцооднаконергианецуверялчтовторгшаясясилатупаинерассужающаонавалитподобномо рскомувалуилиснежнойлавинечтовставшиенаеепутилегионыпритянутксебенеисчисимыеп олчищаивконцеконцовкаквыразилсявсебесцветныйтрупывраговсамизапрудятразломдевять днейзапрошенныхнергианцемдляподходапомощидолжныбылиистечьтолькопослезавтраод накокозлоногиеужебылиздесьсовсемрядомимператорстоялсомерзениемглядянавалявшуюс яуегоногбездыханнуютварьразломарыжаяшерстьнауродливойрогатойголовеобожженаглаз абельмывыкаченыкогтистыелапыбессильнораскинутынелепозадралисьсбитыестертыекоп ытабестиямертваубитаневедомыморужиемнозаметитьстрелкапохожесумелодинлишьимпе раторостальнымэтопоказалосьчудомкаквырвалосьукертинорапредводительвольныхлично йстражиимператораупалнаколенивозлеповерженноговраганисамкапитанниегосородичини чегонеуспелисделатьсовнезапноринувшейсяизсумракатварьюатотктоуспелрешилневыдава тьсвоегоприсутствияегозастрелилихолоднопроговорилимператорязаметиллучниканопоноч номувременинеразгляделвовсякомслучаевколчанеунегоявнонепростыестрелыблагодарюве чноенебопотрясеннопрошепталнабольшийвольныхникогдатакогоневиделидаженеслыхалр азрубитеэтоимператорбрезгливотолкнултварьвбокноскомсапоганавсякийслучайвольныемг новенноисполниликомандуизобрубковмедленноинехотявытекалатемнаяедкопахнущаякро вьотрубленнаяголоваскривойнавсегдазастывшейусмешкойвоззриласьнаимператораипрежд ечеммарийаастерсильнымпинкомотправилеекудатокподножиюхолмаправительмельинаусл ыхалсловнобесчисленноемножествоголосовзашепталиразомсозидаемпутьсозидаемпутьсоз идаем

Висновок:

В ході цієї роботи я засвоїв механізм роботи потокових шифрів, на прикладі роботи шифру Віженера. Я навчився рахувати значення індексу відповідності та використовувати його значення для різних довжин ключа, для визначення довжин ключа шифротексту. Також я навчився розшифровувати шифр Віженера.