Міністерство освіти і науки, молоді та спорту України

Національний технічний університет України

“Київський політехнічний інститут”

Фізико-Технічний інститут

Кпиртографія

Комп’ютерний практикум №2

Криптоаналіз шифру Віженера

Виконали:

Студенти 3 курсу ФТІ

Групи ФБ-92

Казанкова Марина

Чикрій Кирило

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

Порядок виконання роботи

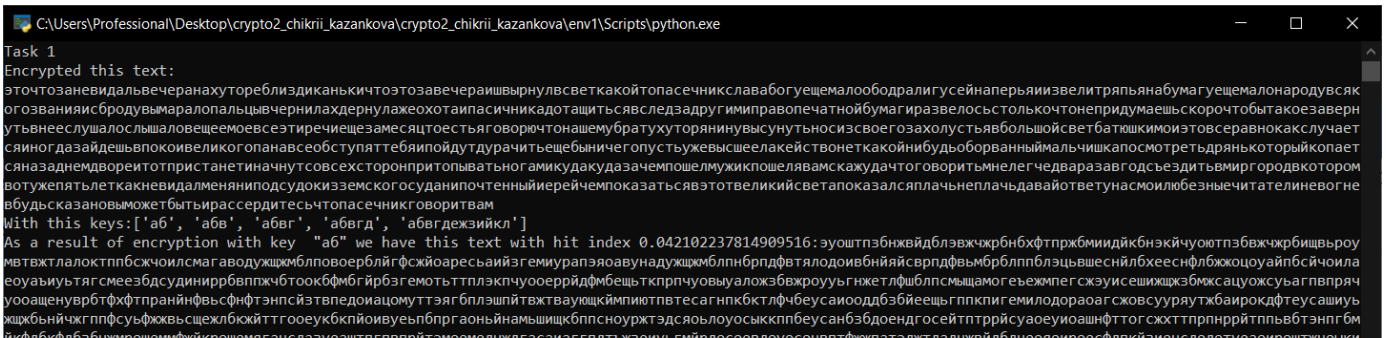
0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

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.

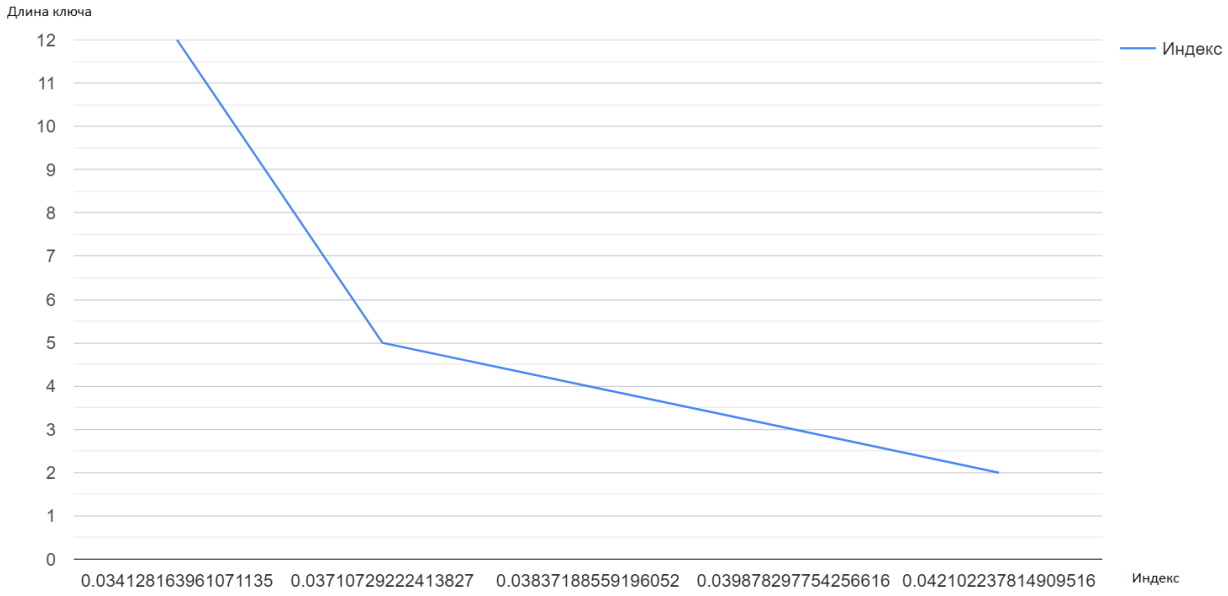
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

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

Частина 1



Частина 2



Длина	Индекс
2	0.042102237814909516
3	0.039878297754256616
4	0.03837188559196052
5	0.03710729222413827
12	0.034128163961071135

Як бачимо чим більша довжина ключа тим меншим стає індекс відповідності

Частина 3

Варіант 7

Спочатку треба було знайти довжину ключа. Ми обрали метод, який дещо відрізняється від запропонованих. Ми зсуваємо текст вправо на 1, 2 і тд символів та шукаємо відповідності у пешого рядка з тим, де текст посунуто. Далі ми оцінюємо через скільки посунень рядків ми отримуємо найбільше значення для відповідності. Це і буде наша довжина ключа.

```
Indexes while searching key length:

[(30, 377), (15, 370), (4, 231), (1, 224), (8, 220), (29, 220), (11, 219),
(10, 217), (17, 216), (2, 214), (5, 210), (22, 209), (19, 205), (28, 205),
(13, 203), (14, 203), (26, 203), (21, 202), (9, 197), (23, 195), (25, 194),
(20, 193), (24, 187), (7, 186), (12, 186), (6, 182), (18, 181), (27, 176),
(16, 175), (3, 160)]
```

Як бачимо у 30 та 15 найбільші індекси, тобто різке збільшення відбувається через кожні 15 посунень. Таким чином отримали довжину ключа 15

Далі ділимо текст на блоки. Знаючи, що найчастіша буква російського алфавіту “о” - припускаємо, що буква, що зустрічається у тексті найчастіше і є зашифрована“о”. Далі використовуємо формулу k = y – x (mod m) та отримуємо наступний текст: арудазевархимаг. Александр Рудазов — Архимаг - скориставшись Інтернетом виявили, що це назва книги та її автор. Отже, ключ арудазовархимаг

Але якби ми не мали доступу до Інтернету, ми б все одно могли знайти ключ вірно. Спробувавши розшифрувати ключем арудазевархимаг ми б отримали читабельний текст, але деякі слова були розшифровані невірно. Тоді ми б знайшли букву, яка невірно розшифровує та спробували замінити її на іншу, користуючись знаннями про те, які букви в російській мові зустрічаються найчастіше. Таким чином ми б замінили букву арудаз**е**вархимаг на арудаз**о**вархимаг та скориставшись цим ключем отримали повністю читабельний текст

Розшифрований за допомогою ключа арудазовархимаг довжиною 15 має наступний вигляд:

прошлопятнадцатьднейистарыйдомпостепенноначаложитьсороклетвнемниктонежилпон
астоящемузаэтовремяонсменилодиннадцатьхозяевниктоизнихневыдерживалвподобном
местебольшетрехмесяцевкреоливанессасталидвенадцатымимагполностьюпогрузилсявра
ботуонотрывалсятолькозатемчтобыпоестьаотснаизбавлялсязаклятиембессонницынодля
креолаэтоявнонепроходилобезнаказанноглазаунегопокраснелиавекинабряклииотвисли
ванессавсяческистаралась убедитьеговтомчтоемуследуетпрекратитьиздевательствана
дорганизмомихотьразоквыспатьсяпонастоящемуномагтолькоогрызалсязанималсяондвум
яделаминеутомимописалмагическуюкнигуиокутывалособнякмагическойзащитойитоидруг
оетребовалоуймывремениакреолникакнемогрешитьчтодлянегоболеесрочнопоэтомузаним
алсяобоимиделамипопеременносначалаонвсерьезбеспокоилсяотомчтозаегодушойвотвот
явитсяужасныйтройнопотомутихомирилсярешивчтототскореевсегодаженезнаетовоскреш
ениистаринноговрагапокрайнеймереванессаизбавиласьотдомашниххлопотбраунихуберт
неизменносохраняяпостноевыражениелицаубиралсяготовилиобстирывалвсехжильцовобе
дыиужиныунегополучалисьоченьвкуснымихотяванессенеслишкомнравилосьчтоонтакнале
гаетнаэкзотическиерецептыповареннуюкнигукоторойонобычнопользовалсяоставилвдом
еодинизегопрежнихвладельцевзавзятыйгурманоднакобыловполнесъедобносамажеванесс
азасучиларукаваивплотнуюзанялась рремонтомпервоначальноонапланировалананятьбри
гадурабочихчтобыонипривелиэтотсарайвпорядокновсталвопроскудавтакомслучаедеват
ьвесьэтотзоопаркбольшаячастьжильцовунормальногочеловекавызвалабывлучшемслучае
сильноеудивлениепоэтомудевушкаделалавсесамавсечтобылонужноонаказывалапотеле
фонуобоикраскуклейпиломатериалыстеклогвоздиинструментыипрочиемелочивплотьдодв
ерныхручекатакжегорукнижекквоторыхтолковоразъяснялоськакделатьвдомеремонтсоб
ственнымирукамиксчастьюдедванессыпоматеринскойлинииибылплотникомобожалмастерит
ьвсеподрядикоечемунаучилвнучкутакчтоначинатьейпришлосьснеснуляестественноводин
очкуонамалочтосмоглабысотворитьтребовалисьпомощникипреждевсегоонаконфисковала
укреолаамулетслугивотужкогдахрустальномуподросткупришлосьпотрудитьсяпонастоящ
емувонгонялаегосутрадовечеранедаваяниминутыроздыхувпрочемонневозражалоднакоон
абыстроубедиласьчтоумагическогослугидействительноимеетсяряднедостатковонзачас
туюпонималраспоряженияянесовсемтаккактоттоихотдавалкпримеруванессаприказалаем
увыпилитьрейкидляновойлестницывродебывсевпорядкеперваярейкаполучилась простобе

зупречнойиванессаспокойноотправиласьпитькофеонавернуласьчерезполчасаиобнаружи
лачтосовершилаужаснуюошибкузабылауточнитьточноеколичествонеобходимыхейреекслу
гаизвелтричетвертиимеющихсяунеедосокизавалилкомнатурейкамидопотолкадевушкабыл
авынужденазаказатьновыедоскииломалатеперьголовукудадеватьстолькобесполезныхде
ревянныхизделийтройвотличиеотсвоегодальнегородичаотличалсяредкимсластолюбиеми
держалнетрехчетырехналожницкактогдаещенеархимагавсеголишьмагистркреоланесколь
косотенпричемменялонихоченьчастобольнаяфантазиямолодогонекромантагубилаеголюб
овницсужасающейскоростьюоднаждыонзаглянулвшахшаноркогдаегохозяинотсутствовалк
акужеупоминалосьтогдаэтидвоеещеневраждовалипоэтомутроявстретиликакгостясделав
всечтобыродичхозяиначувствовалсебяхорошоксожалениюпослетогокакмагплотноотобед
аликакследуетвыпилемунаглазапопалась одна израбыньеслибыдомабылсамкреолилихотяб
ыегоуправляющийбедыудалосьбыизбежатьнониктодругойнеосмелилсяостановитьмагавоз
желавшегопоразвлечьсясневольницейтройпробылснейоколочасаикогдавышелвеселосооб
щилчтоондеслегкапопортилимуществосвоегородичаисобратапогильдиинопустьтотнерас
страиваетсяонтройоставилвуплатузанеецелуюгорсть золотыхйехровниктоизрабовничут
ьнезабеспокоилсяслучайбылсамыйчтонинаесть заурядныйплатавтроепревышаланормаль
нуюстоимостьрабынидажетакойкрасоткикактаэфиопскаятанцовщицакоторуютройслегкап
опортиливсебыобошлось еслибыеслибырабынянеоказалась любимойналожницейкреолаесли
бынетотфактчтоонаносилаподсердцемребенкабудущеговерховногомагаеслибынеточтоже
стокийивспыльчивыймагпожалуйединственныйразвжизникоготополюбилкогдакреолверну
лсядомойиувиделточтоещевчерабыломолодойкрасивойженщинойонвпалвтакоебешенствоч
торазрушилполовинусобственнойкрепостнойстеныиперебилнеменьшетридцатирабовприп
адокещенезакончилсяамагужелетелвбуквальномсмыслекхешибудворцутроячтобыпродолж
итьразрушениетаманадосказатьчтовтевременакреолужебылоднимизсильнейшихмаговшум
ераатройещенетнаследующийденькогдадомойвозвратилсяужетройпришлоеговремяполуча
тьшокотегодворцавпрочемкудаменьшегочемукреолаостались лишьдымящиесяразвалиныкр
еолразворотилкаменнуюгромадувживыхнеосталось ниодногорабаниоднойналожницывсеон
ипогиблиотогняимолнийразгневанногомагакогдажетройобнаружилителосвоегодесятилет
негосынаневинныйребенокбылутопленвбадьесрасплавленнымзолотомаемувроткреолзасу
нулмаленькуюглинянуютабличкустремясловаминадеюсь платадостаточнанадосказатьчто
креолочень скорораскаялсявсодеянномидажепринесискупительнуюжертвунаалтареиштар
доэтогоднямагнеубилниодногоребенкаинепросторебенкаачленаодногоизсамыхименитых
родовимперииегособственногоюныйэхтатожеведь приходилсякреолуродственникомивотл
ичиеотсвоегоотцапереднимничемнепровинилсяноуженичегонельзябылопоправитьеслиза
разрушенныйхешибиумерщвленныхрабовкреолмогзаплатитьвыкупубийстворабавдревнемш
умересчиталосьмелкимпреступлениемкотороеприравнивалось кпорчечужогоимуществато
смерть сынатройнепростилбыемунизакакиедень гимолодоймагвозненавиделродичадоконц
асвоихднейаужненавидеть тоэтотчеловекумелкакникто другойсэтогоднятройжилоднойто
лькоместьюразумеетсяоннебросилсявлобовуюатакутройнебылдуракомипонималчтоскрео
ломемунетягатьсяонисчезизшумерапочтинатридцать летнокогдавернулсянеизвестногде
егоносилостольколетновернулсяонужеархимагомиоченьбыстрозанялбылоеместоприимпе
раторскомдворепримернозагоддоеговозвращениякреолзанялпоствер ховногомагаитройн
емедленнопринялсяинтриговать пытаясь подсидеть бывшегоприятеляатеперьсамогозакля
тоговрагавстречаясьвбашнегильдиикреолитройлюбезнораскланивались прячазафальшив
ымиулыбкамизвериныеоскалывозвращаясьжедомойонинемедленнопринимались строитькоз
нидругпротивдругаособенностаралсятройзадвадцать леткреолупришлось прикончитьсто
льконаемныхубийцчтоизнихможнобылосформировать небольшуюармиюсрединихпопадались
самыеразныетвариотобычныхлюдейдомогущественныхдемоновособенноартодуиартераиду
запомнилсязомхокобжуткоесуществопохожеенаизуродованногокальмараразмеромсчетыр
ехслоновпоставленныхдругнадругакакужтроюудалось договоритьсясэтиммонстромнеизв
естноновпрошломгодуонвыползизевфратаисухимпутемдошелдосамогоурагигантбилсяокр
епостныестеныпочтидвоесутокпокакреолполивалегосотнямиразрушительныхзаклятийто
чтовконцеконцовосталось отчудовищаможнобылозапихнуть вшкатулку

Висновок: під час виконання цього комп’ютерного практимуму ми ближче познайомились із шифром Віженера, навчились шифрувати та розшифровувати текст з його допомогою, знаючи ключ, та розшифровувати, не знаючи ключ (шукати довжину ключа, а потім і сам ключ)