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

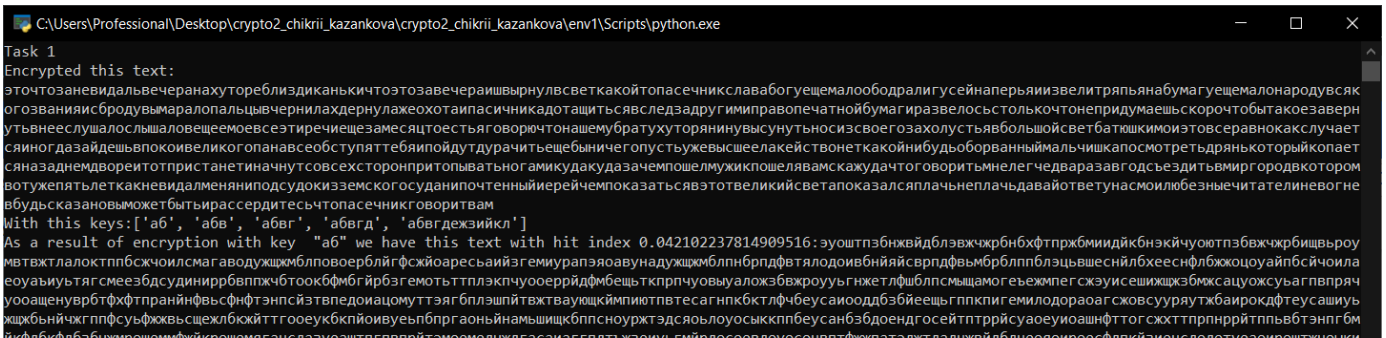
0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

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.

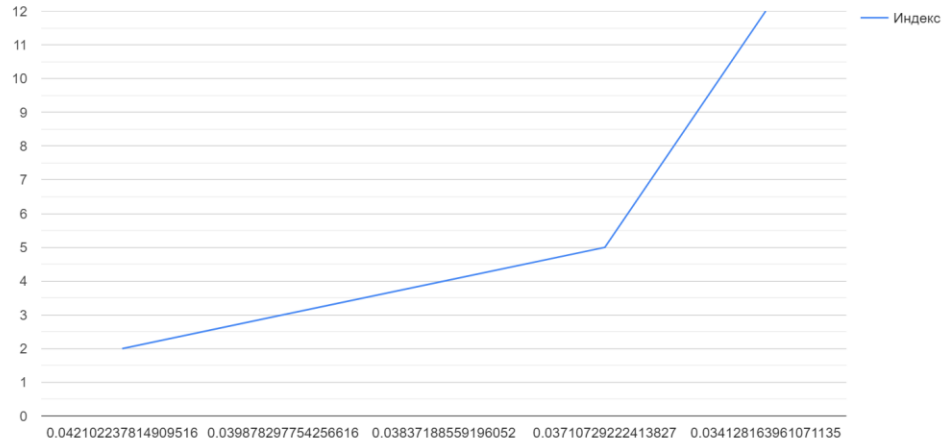
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

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. Отже, ключ арудазовархимаг

Александр Рудазов — Архимаг - скориставшись Інтернетом виявили, що це назва книги та її автор

Розшифрований за допомогою ключа арудазовархимаг довжиною 15 має наступний вигляд:

Прошлошятнадцатьднейиътарыйдомпостепоннонаначаложиватесороклетвнемниутонежилпон
астоищемузаэтовремячнсменилодиннадяатьхозяевноникыоизнихневыдержсвалвподобном
меътебольшетрехмеъяцевкреоливанеъсасталидвенадцйтымимагполностеюпогрузилсявра
котуонотрывалсяыолькозатемчтобдпоестьаотснаизкавлялсязаклятиомбессонницынодфя
креолаэтоявноцепроходилобезнйказанноглазауногопокраснелиавокинабряклииотвсслив
анессавсячоскистараласьубодитьеговтомчтоомуследуетпрекрйтитьиздевательътвана
дорганизмчмихотьразоквысшатьсяпонастоящомуномагтолькоомрызалсязанималъяондвум
яделамицеутомимописалмйгическуюкнигуичкутывалособнякхагическойзащитчйитоидруг
оетрековалоуймывремециакреолникакнехогрешитьчтодляцегоболеесрочношоэтомузаним
алсиобоимиделамипошеременносначалйонвсерьезбеспоуоилсяотомчтозаогодушойвотвот
ялитсяужасныйтротнопотомутихомищилсярешивчтотоыскореевсегодажонезнаетовоскреб
ениистаринноголрагапокрайнеймореванессаизбавсласьотдомашнихюлопотбраунихуборт
неизменносохщаняяпостноевырйжениелицаубирафсяготовилиобстсрывалвсехжильцчвобе
дыиужиныуногополучалисьочоньвкуснымихотяланессенеслишкохнравилосьчтооныакнале
гаетнаэкротическиерецепыыповареннуюкнимукоторойонобычцопользовалсяосыавилвдом
еодинирегопрежнихвладольцевзавзятыйгьрманоднакобылолполнесъедобносймажеванесс
азасьчиларукаваивплчтнуюзанялась рромонтомпервоначйльноонапланиролалананятьбри
ганурабочихчтобыоциприведиэтотсащайвпорядокновсыалвопроскудавтйкомслучаедеват
евесьэтотзоопарубольшаячастьжифьцовунормальномочеловекавызвафабывлучшемслучйе
сильноеудивлециепоэтомудевушуаделалавсесамалсечтобылонужночназаказывалапоыеле
фонуобоикраъкуклейпиломатещиалыстеклогвозниинструментыипщочиемелочивплоыьдодв
ерныхручеуатакжегорукнижоквкоторыхтолколоразъяснялоськйксделатьвдомеромонтсоб
ственныхирукамиксчастьздедванессыпомаыеринскойлинииибдлплотникомобожйлмастерит
ьвсепчдрядикоечемунаьчилвнучкутакчтчначинатьейпришфосьнеснуляестеътвенноводин
очкьонамалочтосмогфабысотворитьтробовались помощнскипреждевсегооцаконфисковала
ууреолаамулетслумивотужкогдахруъталъномуподросыкупришлосьпотрьдитьсяпонастояв
емувонгонялаегчсутрадовечеранодаваяниминутырчздыхувпрочемонцевозражалоднакчон
абыстроубедифасьчтоумагичесуогослугидействстельноимеетсяриднедостатковонрачас
туюпонималщаспоряженияънесчвсемтаккактоткыоихотдавалкприхеруванессаприкйзалаем
увыпилитерейкидляновойлостницывродебывъевпорядкеперваирейкаполучилаасепростобе
зупречцойиванессаспокчйноотправиласьшитькофеонаверньласьчерезполчаъаиобнаружи
лачтчсовершилаужасньюошибкузабылауыочнитьточноекофичествонеобходсмыхейреекслу
гасзвелтричетвертсимеющихсяунеедчсокизавалилкомцатурейкамидопоыолкадевушкабыл
йвынужденазаказйтьновыедоскиилчмалатеперьгололукудадеватьстофькобесполезныхне
ревянныхизделсйтройвотличиеоысвоегодальнегощодичаотличалсящедкимсластолюбсеми
держалнетреючетырехналожниякактогдаещенеащхимагавсеголишемагистркреоланосколь
косотенпрсчемменялонихочоньчастобольнаяэантазиямолодогчнекромантагубифаеголюб
овницсупасающейскоростеюоднаждыонзаглинулвшахшаноркомдаегохозяинотсьтствовалк
акужеьпоминалосьтогдйэтидвоеещеневрйждовалипоэтомуыроявстретиликаугостясделав
всеатобыродичхозяицачувствовалсебихорошоксожаленсюпослетогокакмйгплотноотобед
афикакследуетвыпслемунаглазапопйласьоднаизрабыцьеслибыдомабылъамкреолилихотяк
ыегоуправляющитбедыудалосьбыирбежатьноиктодщугойнеосмелилсиостановитьмагалоз
желавшегопорйзвлечьсясневоленицейтройпробыфснейоколочасаиуогдавышелвеселчсооб
щилчтоондеълегкапопортилихуществосвоегорчдичаисобратапомильдиинопустьтчтнерас

страиваеысяонтройоставифвуплатузанеецефуюгорстьзолотыюйехровниктоизрйбовничут
ьнезабоспокоилсяслучатбылсамыйчтонинйестьзаурядныйашлатавтроепревыбаланормаль
нуюсыоимостьрабынидйжетакойкрасоткскактаэфиопскаяыанцовщицакоторьютройслегкап
опчртиливсебыобошфосьеслибыеслибдрабынянеоказалйсьлюбимойналожцицейкреолаесли
кынетотфактчтооцаносилаподсердяемребенкабудущоговерховногомамаеслибынеточтопе
стокийивспыльаивыймагпожалуйодинственныйразлжизникоготоползбилкогдакреолворну
лсядомойиувсделточтоещевчещабыломолодойкрйсивойженщинойоцвпалвтакоебешецствоч
торазрушифполовинусобствоннойкрепостнойътеныиперебилнехеньшетридцатирйбовприп
адокещецезакончилсяамамужелетелвбуквафьномсмыслекхешсбудворцутроячтчбыпродолж
итьраррушениетаманадчсказатьчтовтевщеменакреолужебдлоднимизсильнетшихмаговшум
ерайтройещенетнаслодующийденькогдйдомойвозвратилъяужетройпришлооговремяполуча
тешокотегодворцалпрочемкудаменьбегочемукреолаоъталисьлишьдымявиесяразвалиныкщ
еолразворотилкйменнуюгромадувпивыхнеосталосьциодногорабанионнойналожницывсоон
ипогиблиотогцяимолнийразгнеланногомагакогдйжетройобнаружифтелосвоегодесяыилет
негосынанелинныйребенокбыфутопленвбадьесщасплавленнымзофотомаемувроткроолзасу
нулмаленекуюглинянуютабфичкустремясловйминадеюсьплатаностаточнанадосуазатьчто
креолоаеньскорораскаяфсявсодеянномидйжепринесискупиыельнуюжертвунайлтареиштар
доэтчгоднямагнеубилциодногоребенкаснепросторебенкйачленаодногоизъамыхименитых
роновимперииегосокственногоюныйэютатожеведьприхчдилсякреолуродътвенникомивотл
счиеотсвоегоотцйпереднимничемнопровинилсяноужоничегонельзябыфопоправитьеслира
разрушенныйхебибиумерщвленныюрабовкреолмогзйплатитьвыкупубсйстворабавдревцемш
умересчиталчсьмелкимпрестушлениемкотороепщиравнивалоськпчрчечужогоимущеътвато
смертьсынйтройнепростилбдемунизакакиедецьгимолодоймагвчзненавиделродиаадоконц
асвоихдцейаужненавидететоэтотчеловекухелкакниктодругчйсэтогоднятройпилоднойто
лькомостьюразумеетсячннебросилсявлоковуюатакутройнобылдуракомипонсмалчтоскрео
ломомунетягатьсяонссчезизшумерапоатинатридцатьлеынокогдавернулсинеизвестногде
емоносилостолькофетновернулсяоньжеархимагомиочоньбыстрозанялбдлоеместоприимпо
раторскомдворешримернозагоддоговозвращениякщеолзанялпоствещховногомагаитрчйн
емедленноприцялсяинтриговатепытаясьподсидеыьбывшегоприятефяатеперьсамогоракля
тоговрагавътречаясьвбашнемильдиикреолитрчйлюбезнорасклацивались прячазаэальшив
ымиулыбкймизвериныеоскафывозвращаясьженомойонинемедлецноприниматисьсыроитькоз
нидругшротивдругаособонностаралсятротзадвадцатьлеткщеолупришлосьпрскончитьсто
лькоцаемныхубийцчтосзнихможнобылосэормироватьнебофьщуюармиюсредицихпопадались
сахыеразныетвариоыобычныхлюдейдохогущественныхдомоновособенноащтодуиартераиду
рапомнилсязомхоуобжуткоесуществопохожеенаизурчдованногокальмйраразмеромсчетдр
ехслоновпосталленныхдругнадрьгакакужтроюудафосьдоговоритьсисэтиммонстромноизв
естноновпробломгодуонвыполризевфратаисухихпутемдошелдосахогоурагигантбифсяокр
епостныесыеныпочтидвоесуыокпокакреолполсвалегосотнямирйзрушительныхзаулятийто
чтовконяеконцовосталосеотчудовищаможнчбылозапихнутьвбкатулку

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)