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

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Виконала:
студентка
групи ФБ-13
Теплякова Анна

Криптоаналіз шифру Віженера

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

Порядок виконання роботи:

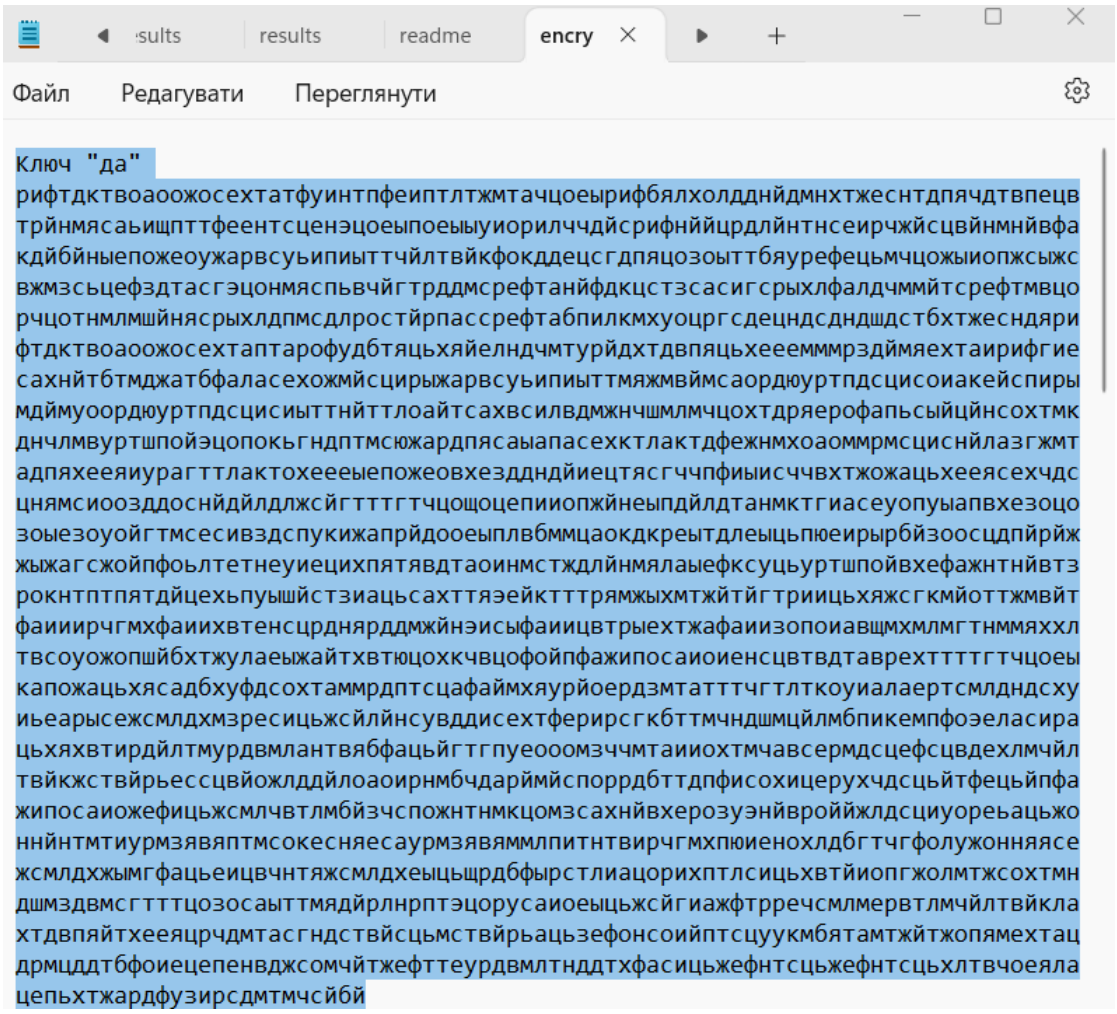
0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

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.
   Код у файлі lab2_1.py
   Підібраний текст у файлі task1.txt
   Оброблений текст (за допомогою функції edit_textfile) в файлі task1_edited.txt
   Ключі для шифрування тексту ["да", "нет", "иглы", "взнос", "губернаторствовавший"]

   Формула для шифрування:

$$y_i = (x_i + k_{i \bmod r}) \bmod m, i = \overline{0,n}$$

   Закодований текст був записаний у файл "encrypted_text.txt"
   Приклад з ключем «да»



   Також дивилась результат шифрування на онлдайн-ресурсі, мій результат співпав з результатом на онлайн-ресурсі

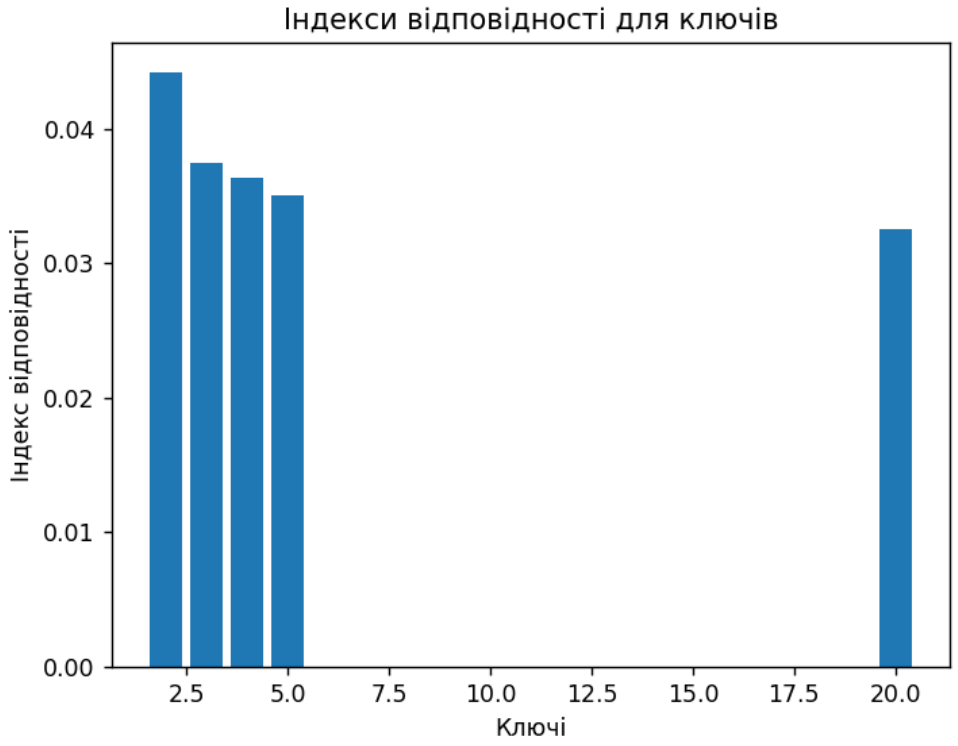
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
   Код для підрахування індексів в тому ж файлі lab2_1.py
   Індекс відповідності був обрахований за допомогою функції calculate_index_of_coincidence та допоміжної функції calculate_and_print_indices

   Формула для обрахування індексу відповідності:

$$I(Y) = \frac{1}{n(n-1)} \sum_{t \in \mathbb{Z}_m} N_t(Y)(N_t(Y) - 1)$$

   Результат виконання функцій:
   Індекс відповідності для відкритого тексту: 0.05466666666666667
   Індекс відповідності для зашифрованих текстів (Key = 'да'): 0.04418590704647676
   Індекс відповідності для зашифрованих текстів (Key = 'нет'): 0.03750774612693653
   Індекс відповідності для зашифрованих текстів (Key = 'иглы'): 0.036306346826586705
   Індекс відповідності для зашифрованих текстів (Key = 'взнос'): 0.03505097451274363
   Індекс відповідності для зашифрованих текстів (Key = 'губернаторствовавший'): 0.03250124937531235

   Візуалізація:



3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта - 15).

   Код у файлі lab2_2v2.py

   Довжина ключа: 14

   Для знаходження істинного значення r я використала один з алгоритмів, наведених в методичці:

   1) Для кожного кандидата розбити шифртекст *Y* на блоки
   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

   Використовую ту саму функцію для обчислення індексів відповідності, що і в попередньому завданні calculate_index_of_coincidence, потім шукаю довжину ключа за допомогою функції find_key_length (код перебирає можливі значення ключа (0-29), розбиває текст на блоки, обчислює індекс відповідності для поточного блоку, якщо індекс більший за поточний максимальний індекс (спочатку 0,053 – теоретичний індекс відповідностідля російської мови), значення max_index і best_l оновлювались новим значенням). Після цього функція find_key шукала сам ключ – цикл перебирав кожен символ для заданої довжини ключа, потім визначалися фрагменти тексту, які відповідали кожному символу ключа, знаходився символ, що зустрічається найчастіше в фрагментах тексту, цей символ вважається ймовірним символом для даного положення у ключі. Після визначався зсув для отримання символу ключа відносно символу 'о', в коді літера 'о' обрана як постійний пункт для визначення зсуву. Літеру 'о' вибрала, бо знайшла в Інтернеті, що це найчастіше уживана літера російської мови. Був використаний частотний аналіз.
   Функція дешифрування стандартна, за формулою:
   $k_i = (y_i - x_i)\ mod\ m$, де y – і-ий символ зашифрованого тексту, x - і-ий символ ключа

   Результат виконання коду:

   Ключ: посняковандрей

   наберегусевернойдвиныпримерновполсотневерстотвпаденияеевгандвикбелоеморесредьгустойтайгизатеряласьмихайлоархангельскаяобительоднаизсамыхдальнихвновгородскойземлееслинесчитатьскитупустозерскогоострогачтонапечоререкенудотогоскитаещедобратьсянадоакздешнемумонастырюпожалуйстахочешьчерезвологдудапотомпосухоневеликийустюгатамидодвинырукойподатьзнайплывипотечениюахочешьнапрямикчерезладогусвирьонегудальшенасевергдеволокомагдеозерамималымиизновгородаудобнеетакизкакихдругихрусскихземельчерезустюгвобщемдобратьсявмонастырьмихаилаархангеланевеликапроблемабылобжеланиезамолитьгрехиилинаоборотвушкуйничийпромыселпуститьсятожечерездвинунеплохосколотитьватагувыстроитьстругивтомжеустюгедавпутьотустьядвинырекивседорогиоткрытывсторонычужедальниеневедомыевпечоруввеликуюпермиювюгругденемирнаясамоедьтакиноровитвсадитьвсердцеушкуйникаоструюкостянуюстрелусмоченнуюгнилойрыбьейкровьютутжеипутьинойиноческийкмонастырюсоловецкомувпрочемкнемулучшепоонегепрямейбудетолегиванычназначенныйвоеводойновойновгородскойэкспедициииспользовалобапутичастьлюдейвместеснимсамимшлананебольшихлодьяхпосвиридаонегедалеепоморюгандвиксзаходомвсоловкинамолениеиснованаюгкдвинедругаячастьнаправиласьчерезвеликийустюгснаказомкупитьтамлодейдляморскихплаванийпригодныхкупиличегоужкочамителодьиназывалисьпрямоскажемнекаравеллыдаженекоггимелкиекакиетонекрасивыес

полукруглымднищемнекоторыеужхотелибыломордыплотникамзатакиесудабитьдазнающи
елюдиотсоветоваливопервыхплотницкихартелейвустюгетьмасварузатеватьсебедорожевы
йдетнуавовторыхтакиевоткорабликиинужнычтобсудачейполедовитымполуночнымморям
плыткорпусхотьинеказистыйдакрепкийтеплыйвкаютекаморедажепечканебольшаяимеетс
яачтосднищемполукруглымвмореболтаетсильнотактоневеликабедазатольдамивовекнераз
давитальдоввполночныхводахвидимоневидимотолькочтолетомплытьиможноитокакбожья
волябываетзатянутморетуманыдатакиечтоносасобственногонеразглядишьилиподуетвдруг
борейсеверныйветерпринесетгромадныельдинывотидумайтолидальшеидтитолипересидет
ьпереждатьдатолькождатьтодолгонькоможноасеверноелетокороткоенеуспеешьоглянуться
ужезимавотисидитогдазимуйеслисможешьмногоетутнеотумениялюдскогоотпогодызависе
лонуаужпогодавестимоотгосподаможноведьбылоидалечеуйтизатритомесяцааможноидова
йгачанедобратьсятуманыдаштормадальдыпережидаялилдождьбеспросветныйинудныйвс
юночьнапролетнепереставаякрупныетяжелыекапликолотилипокрышампрогонялисулицре
дкихприпозднившихсяпрохожихпревращаливхлюпающуюгрязьтянущиесявдольгородской
стеныогородывэтуночьтемнуюиненастнуюстражникинабашняхстарательнокутались впла
щиукрываясьотпорывовпромозглоговетратакойветеробычнобываетпозднейосеньювноябр
екогдасыплетсяснебанепоймешьчтотолихолодныйдождьтолимокрыйснегаскореитоидруг
оесразунотоосеньюасейчаснадворестоялмайхотьинеоченьтотеплыйздесьвсеверныхновгор
одскихкраяхдаужинетакойчтобсоснегомвотужпослалчертпогодкуадядькокузьмаобернувш
иськнапарникувыругалсяворотныйсторожмолодойкруглолицыйпареньвкоротковатойколь
чужкеиостроверхомшлемебрызгидождяскатывалисьпошлемупрямозашиворотпарнюитотт
оиделоморщилсяпередергиваяплечамивторойстражниккузьмавысохшийпожилоймужикср
еденькойбородкойидлиннымивислымиусамиотвернувшисьответрабуркнулвответчтотонер
азборчивоевидимосогласенбылчтоподобнуюпогодкутолькочертипосылаетповерхкольчуги
укузьмыдлинныйкрашенныйчерникойплащизплотнойдерюгивнебольшойплетенойбаклаж
кеупоясаплескаласьмедовухаславенскийконецслааавенелеслышнодонеслось спетровскойб
ашнискрытойпеленойдождяиночнойтьмоюслаавентутжеподхватилисоседисбашнишестист
еннойчтовсотнешаговоткузьмыснапарникомплотницкийслаавеноткликнулсякруглолицый
неспиммолдождалсякогдадонессяответотсоседейслевасбашничтонасамомберегуволховао
бернувшись подмигнулугостилбымедкомдядькокузьмавислоусыйкузьмаширокозевнулпер
екрестилсяистряхнувсбородыкаплинехотяпротянулбаклагупейонуфрийдатолькосмотритр
иглотканеболеместоунасбеспокойноенеточтоуэтихонмахнулрукойвлевовсторонуволховск
ойбашниместечкоимдействительнодосталосьтоещебойкоееслинесказатьбольшебольшаяче
тырехстеннаябашнянакоторойнеслислужбукузьмасонуфриембылапроезжейвыходилаворо
тамизагородскуюстенукбольшойдорогечтоизвиваласьмежлесовдаболотпоправомуберегув
олховастойсторонымногоктомогпожаловатьихитроватыйкостромскойкупецитихвинскийб
огомолецврясеиприказчикновгородскогоархиепископаимосковскийслужилыйчеловекпосл
еднихпослепораженияновгородцевурекишелонирасплодилосьвновгородекудакакмногошн
ырялитудасюдапоторгучтотовынюхивалиноссвойсоваливделановгородскиесоветовалииме
линатоправоподоговорукоростынскомупотомужедоговорувыплачивалновгородмосквекон
трибуциюшестнадцатьтысячсеребромденьгинемалыенуденьгиуновгородцевводилисьбогд
аствыплатятавотточтоужслишкомнахальномосковитывихделалезлимногимнепонравубыло
хорошмедокутебядядькокузьмакрякнувпохвалилонуфрийподиженкавариласвояченицанух
орошхлобыстатьдоутраточайдолгостойкадядьковдругнасторожилсяонуфрийчувродекаккр
ичитктодакомутамкричатьтосвесившисьзаограждениебашникузьмаглянулвнизестьктотута
льнетямилостивецмонахизобителидымскойчертвасмонаховпоночамноситнуисидитеперьу
традожидайсяправильнодядькокузьмаонуфриюкакикузьменеоченьтохотелосьотворятьтяж
елыескользкиеотдождяворотаутромтобогдастперестанетдождищеспасимилостивецжалобн
озагнусавилмонахитаквесьпромокдониткихотьзаденьгупустиатымолисьчащеотчехохотну
лонуфрийатоходитвасздесьночамиакинукапомолчипаряпрервалкузьмаэйотчетыпрокакую
деньгусейчаспомянулпромосковскуюалипроновгородскуюакакаятебелюбезнейстражники
переглянулисьнучтоотворяетеворотанетосейчаскпристанипойдудапогодитывонспускаемс
яужезаплативстражникаммонахюркийплюгавистыймужичонкасбегающимиглазаминатяну

лнаголовуплащнаброшенныйповерхрясыискрылсявдождливойтьмеонпрошелпославнечутьзадержалсяуповоротанаильинскуюулицупостоялпогляделкудатоинехорошоусмехнулсяужопосчитаемсятеперьстобоюзлобнопрошепталонпосчитаемсяпройдяпославнемонахсвернулнапробойнуюшелсмелонеопасаясьвыбежавшийизповоротанарогатицушпыньхотелужмахнуткистенемпришибитьдурногомонахадатотобернулсявовремяитатьночнойвдругощерилсясловноувидалотцародногоубравкистеньпоклонилсяприветливовиднознавалкогдатомонахадаимонахалисговорившисьдальшевдвоемпошлилишьуфедоровскогоручьярассталисьтатьнамосковскуюдорогупошелчерезмостикпромышлятьдальшеаливкорчмукявдохеамонахкбоярскойусадьбесвернулзаколотилвворотанадворезашлисьвлаецепныепсыктотоиздворовыхслугпробежалгрузнотопаяподубовымплахамкоготамчертпринесоткрывайпоскорейпескгосподинуматонеотмосковскихлюдейпосланец

Висновок: при виконанні комп’ютерного практикуму, я отримала навички роботи та аналізу поліалфавітнох підстановок у вигляді шифру Віженера, ознайомилась з методами знаходження довжини ключа шифртексту та ознайомилась з роботою з методом частотного аналізу.