Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут ім. Ігоря Сікорського»
Фізико-технічний інститут

Лабораторна робота №2

З предмету «Криптографія»

На тему «Криптоаналіз шифру Віженера»

Виконали:

Студенти групи ФБ-83,84
Мельниченко А

Іванченков М

Перевірив:

Чорний О.М

Мета:

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)

Хід роботи:

Для виконання роботи створено бібліотеку viginer_lib.py та набір unit – тестів viginer_test.py. Шифрування/дешифрування тексту та файлів виконані за допомогою функцій crypt(), decrypt() та методів crypt_file(), decrypt_file(). Перевірка алгоритму кодування/декодування перевіряється unit-тестами test1() та test2().

Виконання завдань 1 та 2 реалізовано єдиним методом task1_2() основного модулю програми. Обраний текст об'ємом 46Кб зашифровано довільними (згенерованими випадково) ключами довжини від 2 до 20 символів та пораховано індекси відповідності для кожної довжини ключа. Для порівняння наведено індекс відповідності нешифрованого тексту довжини 1Мб. Результати розрахунків представлено графіком з використанням matplotlib

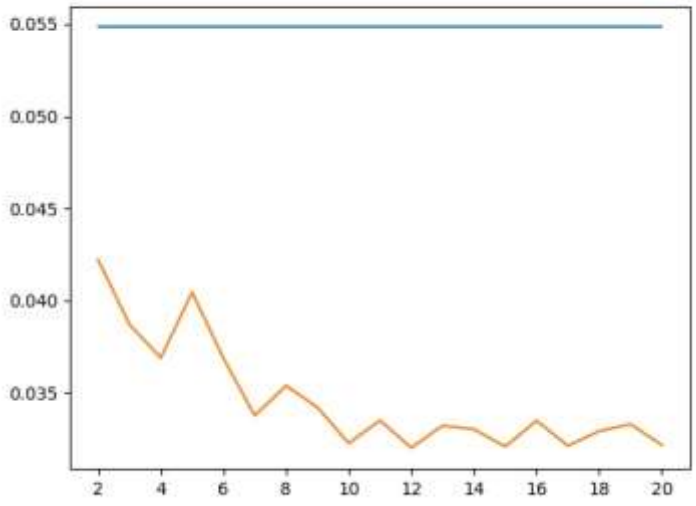

Рисунок 1. Залежність індексу відповідності від довжини ключа.

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

Виконання

Для розшифрування тексту будемо розбивати його на блоки різної довжини та розраховувати індекс відповідності для кожного з блоків. Середнє значення порівнюємо з індексом відповідності відкритого тексту.
Розбиття на блоки реалізовано з використанням функції algorithm1().
Результати розрахунків представлені на рисунку 2 у вигляді графіку.

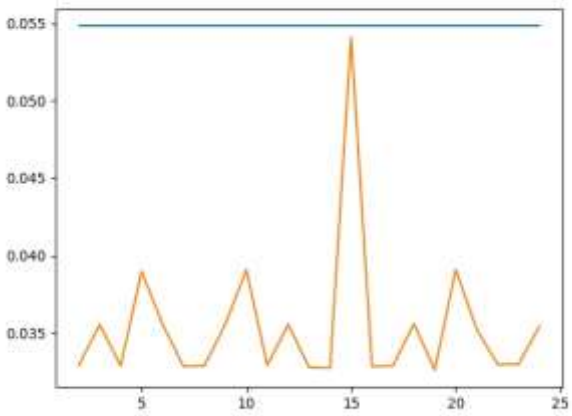

Рисунок 2. Індексі відповідності для різної кількості блоків розбиття.
З розрахунків робимо висновок, що з найбільшою ймовірністю довжина ключа складає 15 символів.
Для розбиття на 15 блоків створюємо частотні словники з використанням функції shift_text(). Результати створення частотних словників показані на рисунку 3.

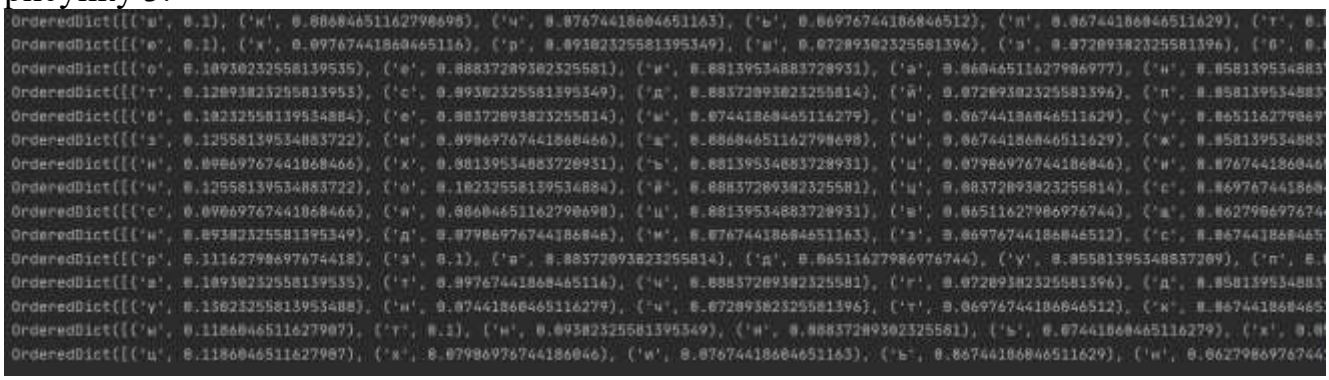

Рисунок 3. Частотні словники.
На підставі частотних словників будуємо можливий ключ шляхом знаходження різниці по модулю 32 між найчастішим символом та символом "о".
Побудований ключ виглядає наступним чином

крадущяйгявтени

Робимо висновок, що більшість букв вгадана вірно тому. Замінюємо невірно вгадані символи та отримуємо ключ

крадущийсявтени

З використанням отриманого ключа проводимо розшифрування файлу з використанням decrypt_file(). Результати розшифрування наведені в додатку 1.

Частоти по блокам, де символи ключа не було відновлено відразу : 2

Додаток 1. Розшифрований текст.

тихотактихочтослышнокакмотылькицепляютсяхрупкимикрылышкамизаночнуюпрохладупора
ужеотправлятьсяпосвоимделамстражадавнопрошланоясегоднячтотослишкомосторожничаю
некоенеобъяснимоечувствозаставляетменязадержатьсявозлестеныздания погруженноговт
еньтеньмояподругамоялюбовницамоянапарницаяпрячусьвтенияживувнейтолькоонавсегда
готовапринятьменяспастиотстрелзлобносверкающихвлуннойночиклинковилиоткровожадн
ыхзолотыхглаздемоновтенькакговоритдобрыйжрецсаготабратфоркогдахватитлишкувовре
мянашихредкихвстречтеньявляетсясестройтьмыаоттьмынедалекоидоненазываемогочушь
неназываемыйитьмаабсолютноразныевещиэтовсеравночтосравниватьограивеликанатеньэ
тожизньтеньэтосвободатеньэтоденьгитеньэтовластьтеньэторепутацияужгарретеньзна
етобэтомнепонаслышкетеньпоявляетсятолькотогдакогдасуществуетхотябыкрупицасвета
такчтосравниватьеестьмойпоменьшеймереглупономоемустаромуучителюяестественноэто
неговорюяйцакурицунеучатнаузкойночнойулочкескаменнымидомамизаставшимитихиеврем
енанераздавалосьнизвукалишьпоскрипывалажестяная вывесканадлавкойбулочникаотгуля
ющегопокрышамгородаслабоговеткамедленныйсерожелтыйночнойтуманкоторымславилас
ьнашастолицаговорятфокускакоготомаганедоучкипрошлогооткоторогонемогутизбавитьс
яипоныневсеархимагикоролевствазастилалмощеннуюгрубымкамнемиизбитуютелегамимост
овуютихотихословновсклепебогатеяпослетогокакегонавестиластаямелкихгородскихвор
ишекскрипитвывескагуляетветерокмедленноиленивоплывутоблакапоночномунебуноявсее
щестоюслившисьстеньюзданияистараясьнешевелитьсяинтуицияимойжитейскийопытзастав
ляютвслушиватьсявтишинуночногогороданиоднадажепустыннаяулицанеможетбытьтакойти
хойособенноэтагдеживуттолькооднилавочникивночидолжныбытьзвукикрысышуршащиевмус
орехрапящийтутжепьяницакоторогоужеуспелипочиститькарманникипреждечемзабитьсявк
акуюнибудьщельнаночьхрапизоконседыхдомовкрадущаясявотьмегрязнаясобакатяжелоеды
ханиеновичкаразбойникавожиданиисвоейжертвызастывшеговомглесзажатымвпотнойладон
иножомшумвлавкахимастерскихдажепоночамвнекоторыхизнихкипелаработаничегоэтогоне
былонатемнойузкойулочкеукутаннойвперинутумананичегокрометишиныимракаветероксил
ьнеезагулялвкрышахстарыхзданийитяжелыесерыеоблакапонеслисьпонебусловностадобол
ьшихпушистыховецобнажаянебесныйкуполбеспечныйгулякаветерласковотрепалволосыноя
несмелнакинутьдажекапюшонсаготчтожеэтокакбыотвечаянамоюмолитвуславныйбогвсехво
ровдалушамбольшечуткостишагиторопливыешагичеловекакоторыенесмогприглушитьдажет
уманрасползающийсясерожелтойнакипьюнадкаменноймостовойвсоседнейвыемкерасполага
ющейсянастенезданияна противязаметилмимолетноеколебаниевотьмектотопрячетсявсмо
трелсявчернильнуюночьнетпоказалось слишкомволнуюсьвожиданиинесуществующихнеприя
тностейстареюнаверноечьятотребовательнаярукаудержаламенянаместекакбыговорястой
обождиещеневремяхсанкорменясожричтожепроисходитнатихойтемнойулочкеремесленнико
вчеловекпоказалсяиззаповоротаулицыибыстрымшагомпереходящимвбегнаправилсявмоюст
оронудуракилихрабрецеслиодиншастаетвтемнотескореевсегопервоехрабрецыдолгонежив
утвнашеммирехотядуракитожееслионинешутынашегославногокоролякакоенеотложноедело
заставиловыйтиегонаночнуюулицугдедажемасляныефонаринегорелипопробуйтенайтифона
рщикакоторыйвысунетвэтовремяносвкромешнюютьмуэтоведьнетихиевременакогдаребенок
спокойномогпройтивсамуюглухуюночьизодногоконцаавендумавдругойиснимничегобынесл
училосьчеловекприближалсявысокийхорошоможносказатьбогатоодетыйрукалежитнарукоя
типриличногомечаслужитважнойшишкенаверноеоблакаснованаползлинанебозакрывсвоимт
еломвыступившиенанебезвездыикполнойтьмедобавилась тьмакромешнаяяуженесмогразгля
детьлицаспешащегочеловекаонпоравнялсясомнойидаженезаметилтихостоящуювтенитеньье
слибыязахотелипротянулрукутоснялбыунегоспоясапузатыйкошелекноянемелкийкарманни
кчтобыпадать такнизковременамолодостидавнокануливлетудаисудьбаподсказывалачтосе
йчаснестоитнеточтодергатьсяадажеглубокодышатьвнишенапротивтьмавновьпришлавхаот
ическоедвижениевскипаяиклубясьчернымцветкомсмертииязамерледенеяотужасаизтьмывы
рваласьтьмапринявобличьекрылатогосуществадемонасрогатойголовойчерепомнакоторой
сиялиалыеузкиеглазаикаклавинасгоркарликовупаланаспешащегочеловекапридавивегосв
оимвнушительнымвесомчеловекиздалвопльраненойкошкипопыталсявыхватитьбесполезный
мечнотьмасмялавсосалапоглотиланочногопутникаисуществокембыононибыловзмыловночн
оеоблачноенебоуносяссобойсвежеемясоаможетидушуугольночерныйсилуэтнамигмелькнул
воблачномночномнебеиисчезястаралсяуспокоитьдыханиетварьнезаметилатогоктовсеэто
времянаходилсянапротивнееноеслибыяшевельнулсяеслибыяхотьнамигшевельнулсяилихот
ябызадышалчутьгромчетоонабыбросилась наменяизнишизданиягдеподжидалалегкуюдобычу
повезловочереднойразмнеочень повезлоудачавораженщинакапризнаявлюбоймигможетотве
рнутьсянопокаонасомнойямогузаниматьсясвоимворовскимремесломвтемномуглусоседнег
озданиятихоп искнулакрысазанейдругаявнебеохотясьзаприпозднившимисяиюньскимимоты
лькамипролетелалетучаямышьопасностьминоваламожнопродолжатьпутьяотделилсяотстен
ыистараясьдержатьсянаиболеетемныхучастковулицыдвинулсядальшеничтонеговорилоосл
учившемсянесколькоминутназадулицабыламолчаливымиединственнымсвидетелемночнойох
отыдемонаксчастьюлунынебылопушистыеоблакавновьнаползлииспряталиотгородазвездып

```
оэтомутенибылосколькоугоднобыстрымшагомнеиздаваясапогаминиединогозвукаяперемещ
алсяотзданиякзданиюизтенивтеньулицапекарейосталасьпозадиясвернулвпереулокнапра
воздесьтуманбылгущеонобволакивалменямягкимилапамиглушилшагискрывалотглазлюдейи
нелюдейвтенипососедствураздалосьшушуканьеязамервсматриваясьвсерожелтуюмглуворы
молодыещенкикудавамдомастераподжидаютночногогулякуилиготовятсяпочиститьспящихг
орожанзеленыслишкомшумятслишкомнеопытныворыпрофипереговариваютсяжестаминеиздаю
тшумадажевтакойночикогдагустеющийлипкийтумангаситвсезвукияпроскользнулрядомсни
миаворишкидаженезаметилитеньтеньвтенисложноувидетьнеопытномуглазувозниклодурац
коедетскоежеланиевыскочитьизтуманаигромкосказатьбуимвлицоновполнеможнонарватьс
янаслучайныйножтемболеечтонечегопугатьмолокососовтемныйпереулоккончилсяинависш
иемрачныестеныдомоввидавшихвэтоммиреирадостьигоререзкоразошлисьвстороныяпосмот
релнанебоветервсетакиразогналленивыеоблакаинебопревратилосьвскатертьнакоторойб
огатейрассыпалмонетысотниитысячизвездмерцалимнеснебаэтойхолоднойлетнейночьюсве
тлокакднемздесьгорелиодиночныефонарикакникакянаходилсянаоднойизцентральныхплощ
адейгородаифонарщикинесмотрянасвойстрахбылиобязанывыполнятьсвоюработупламяфона
рейзакованноевстеклянныеколпакиразбрасываловокругсебяпятнадрожащегосветаихаоти
чныетенимолчаливоплясалинастенахугрюмыхдомовэтоплохонадеюсьчтопогонщикветерсно
ваприведетсерыхпушистыховецнанебоапокапридетсядержатьсятенижмущейсякстенамвысо
кихзданийкотораясталабледнойипугливойотвездесущегосвета
```

Висновок: ми здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера. Зашифрували обраний нами самостійно відкритий текст данним шифром з цими ключами довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Навчились підраховувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівнювати їх значення. Завдяки здобутими нами теоретичними відомостями ми розшифрували наданий шифртекст.