КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2
Криптоаналіз шифру Віженера

Роботу виконали:
студенти групи ФБ-14
Антонова Олександра і Веденкін Артем

Київ-2023

Варіант-8

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.

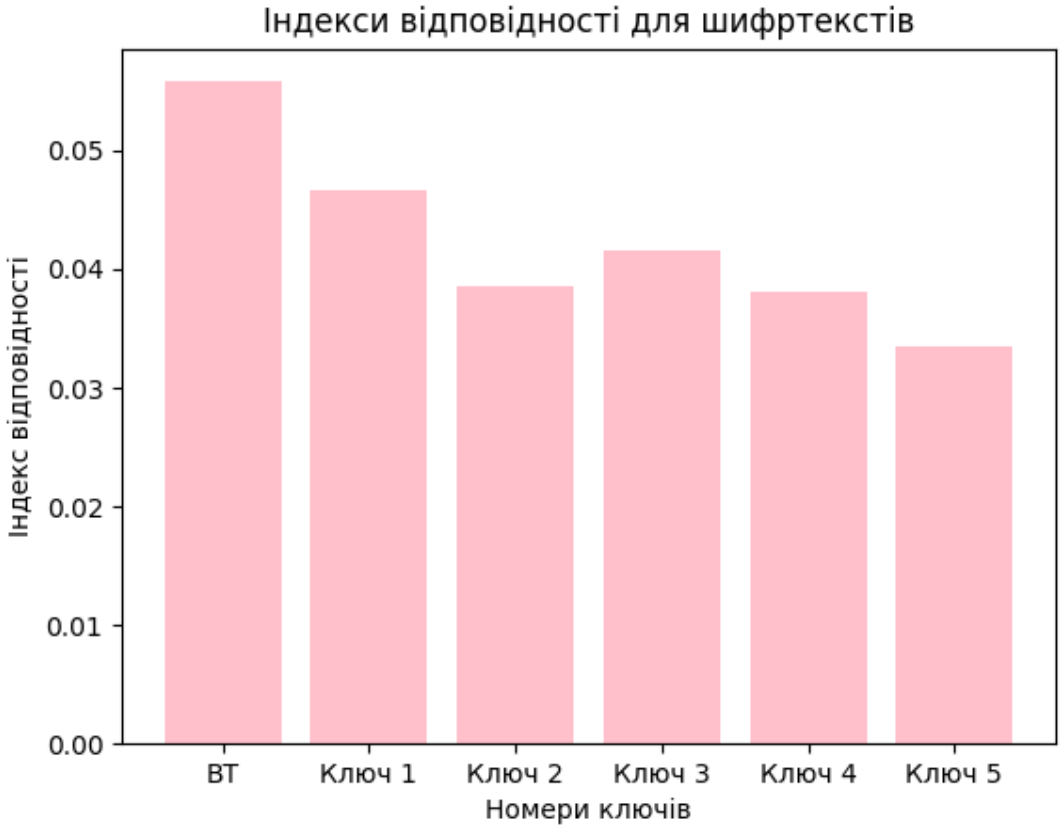
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи

Підберемо відкритий текст для зашифрування (файл «text_1.txt»). Відповідно відфільтруємо його (видалимо пробіли, знаки пунктуації та великі літери). Для зашифрування створимо власні ключі довжиною r = 2, 3, 4, 5 і 20 літер.

Отримаємо такі значення індексів відповідності для відкритого тексту (ВТ) і всіх одержаних шифртекстів:

```
Index of the opened text: 0.055816620128043164
Index of keys position 1:        0.046590293777272876
Index of keys position 2:        0.038610423943856366
Index of keys position 3:        0.041549258390223706
Index of keys position 4:        0.03808593542633273
Index of keys position 5:        0.033560894815632736
```



Зашифрований текст згідно нашого варіанту (файл «text_var8.txt») розбиваємо на блоки відповідно до довжин ключа від 2 до 32. Далі обчислюємо індекс відповідності для кожного блоку і також визначаємо довжину нашого ключа:

```
Довжина ключа: 2, Індекс відповідності: 0.034813904278092 36
Довжина ключа: 3, Індекс відповідності: 0.03324307034378807
Довжина ключа: 4, Індекс відповідності: 0.03620949758935116
Довжина ключа: 5, Індекс відповідності: 0.039787122671158484
Довжина ключа: 6, Індекс відповідності: 0.03485234262962942
Довжина ключа: 7, Індекс відповідності: 0.033168685827683876
Довжина ключа: 8, Індекс відповідності: 0.03612854847527695
Довжина ключа: 9, Індекс відповідності: 0.033334625206161365
Довжина ключа: 10, Індекс відповідності: 0.04615781463575648
Довжина ключа: 11, Індекс відповідності: 0.03322271185825943
Довжина ключа: 12, Індекс відповідності: 0.036215438658340045
Довжина ключа: 13, Індекс відповідності: 0.03298637589477113
Довжина ключа: 14, Індекс відповідності: 0.0346612572232066
Довжина ключа: 15, Індекс відповідності: 0.03965734702651212
Довжина ключа: 16, Індекс відповідності: 0.0362661882458682 54
Довжина ключа: 17, Індекс відповідності: 0.03334006023502844
Довжина ключа: 18, Індекс відповідності: 0.034826442796082255
Довжина ключа: 19, Індекс відповідності: 0.03311209978301721
Довжина ключа: 20, Індекс відповідності: 0.05571397559219484
Довжина ключа: 21, Індекс відповідності: 0.03311591541643312
Довжина ключа: 22, Індекс відповідності: 0.034683103956717 33
Довжина ключа: 23, Індекс відповідності: 0.03320798886358776
Довжина ключа: 24, Індекс відповідності: 0.03609773244107354
Довжина ключа: 25, Індекс відповідності: 0.03996591295454607
Довжина ключа: 26, Індекс відповідності: 0.03491288755705579
Довжина ключа: 27, Індекс відповідності: 0.033181566055015134
Довжина ключа: 28, Індекс відповідності: 0.0357931185315878
Довжина ключа: 29, Індекс відповідності: 0.03310800304297207
Довжина ключа: 30, Індекс відповідності: 0.046017571592696524
Довжина ключа: 31, Індекс відповідності: 0.03317107541767767
Довжина ключа: 32, Індекс відповідності: 0.035950614121199584
Довжина нашого ключа:  20
```

Як бачимо, при довжині ключа в 20 знаків, індекс відповідності найбільш наближений до теоретичного:

Мова	Індекс збігів
російська	0.0553[1]

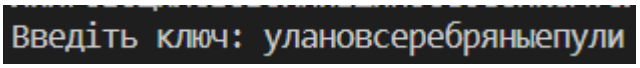
Далі наш код ділить текст на блоки, уже враховуючи конкретну довжину ключа (в нашому випадку 20). У кожному блоці обчислюємо частоту для кожної літери.

Враховуючи те, що найімовірніша буква у російській мові, якою написано відкритий текст це буква «о», намагаємося отримати наш ключ за допомогою формули: k = (y - x) mod m. Отриманий ключ:

```
уланобсеребзяныепуля
этаситтемакщасногокйрликаоикогдйнеимелацазванйятольуозубодрчбителэнодлицныйномещвкат
```

Отримали вже більш змістовний текст, але бачимо, що він не розшифрований до кінця. Трішки загугливши дійшли висновку, що в нашому варіанті зашифровано уривок з книги Андрія Уланова “Серебряные пули с урановым сердечником”. З цього можемо зробити

припущення, що змістовним ключем буде “улановсеребряныепули”. Перевіримо:



Результат:

этасистемакрасногокарликаникогданеимеланазваниятолькозубодробительнодлинныйномервкаталогеисследовавшийеекиберзондотметилналичиетрехгазовыхгигантовдвухастероидныхполейкометногооблакаизанесвсеэтиданныевсекторвторойочередипомнениюинкакиберзондасистеманепредставляланикакойценностидляпославшихеголюдейнаверноебудьунегозадействованыконтурывторогоуровнясамостоятельностиизартаонбыпоспорилсамсообойчтовближайшуютысячулетлюдиздесьнепоявятсяипроспорилбылюдипоявилисьвэтойсистеменечерезтысячулетавсеголишьчерезсемьэтобылинетелюдичтопосылализондформальноонивообщенедолжныбылизнатьосуществованииэтойсистемыноутехктоихпосылалбылиденьгимногоденегисредипрочегоиххватилонаточтобыполучитьвозможностьознакомитьсясрезультатамикартографированиязаинтересовавшегоихсекторатаквсистемепоявилассьстанциянаскороперделаннаяизписанногогрузовикаитридесяткабуевраннегооповещенияподсвечивающихпространствоврадиусепятисветоднейотнеечерезнесколькомесяцевнастанциюпришелпервыйкорабльэтобылстранныйкорабльсвидуобычныйдесятикилотонниксотникоторыхлетаюткакповнутреннимаршрутамсолнечнойтакинавнешниеколониинеобычным жеегоделалисеребристыеовалынабортахпонимающийчеловеклегкобымогопознатьвэтиховалахтяжелыеизлучателимайерсапредставлявшиесобойглавныйкалибркрейсероввксфедерациикорабльбылнеодиндругиепохожиенанегоразвдватримесяцазалеталивсистемудатьотдыхкомандеимеханизмампровестимелкийремонткоторыйотчеготонемогливыполнитьсобственныесервыкораблявпрочемремонтневсегдабылмелкимодинизкораблейприползнастанциюсперекореженнымбортомоставляяпозадитаюшийсиневатыйследсочащейсяизразбитыхотсековатмосферыонявновстретилкоготоравногопосиламаможетбойбылнеравныйноэтоткктотознаячтопошадынеприходитсяждатьоченьстаралсяпродатьсвоюжизньподорожетригодаспустясистемунавестилещеодинкиберзондоднакохотяегосканирующиесистемыбылинапорядокмощнеечемупредшественниказдействоватьихоннесталвместоэтогоновыйгостьтихозависнадплоскостьюэклиптикизапределамидосягаемостибуевипринялсявпитыватьинформациюшумсолнечноговетратяжелыйрокотгравитационныхволнпланетобрывкиразговоровмеждустанциейиочередныприбывающимкораблемпоследнееегоинтересовалоособенносильноае

щечерезмесяцвсистемепоявилисьновыекораблипятьузкиххищныхтенейто тчеловекчтомогбыопознатьсеребристыеовалынавернякасумелбыузнатьи ихпотомучтомалосчемвовселеннойможноспутатьизящныйпрофильэсминц авкстипасиранотроевновьприбывшихушливбокблокируяточкупереходаадв есеребристыеполоскирванулисьпрямокстанциигдекакраззаканчивалподгот овкукполетуочереднойкорабльтемнотавокругтьмаитишинаигдетотамж детнечтоцельмишеньврагоднимсловомточтонадоуничтожитьсправадоне ссятихийзвуктолискриптолишорохямгновенноотскочилвсторонуиокатилп одозрительныйучастоквееромогнятихийтрескэтозвуквыстреловазвонкие иглухиехлопкиэтошарикиплазмывимитационномрежимезвонкиеобстенуиг лухиевмишеньтеоретическиимиможнобылобытемнотуподсвечиватьнопо условиямзачетаяопасаюсьдемаскировкипотомуплазмачернаявидетьвинфр акрасномяпоканенаучилсяавотшорохвпередияпрыгалпокомнатесловноплох аямарионеткапосылаяновуюочередьпреждечемзатихнетпредыдущаяисчи талглухиеударыпадающихтелпятьшестьитемнотазначитещектотооста лсяскольжеихгадовсемьиливосемьяполуприселнаклонилсявпередирастоп ырилрукисловновсплывшаяжабаточьвточькаккитаезаченьвоназанятияхр асслабилсяислушаешьголосвселеннойсейчасонтебеспоетвухогдепрячетсяп оследняяцельнасамомделеяужедавноубедилсячтоникакимиэкстрапараипро чимисверхспособностяминеобладаюноможнопопытатьсякупитьнаэтотф окусоператорайкупилочереднойшороходонессяиззаспиныеслибыядействите льноловилушамиголосиззакраямиратутбымнеибылполныйконецзачетаноп оскольку язанималсяловлейисключительнореальныхзвуковтоупалвпередуспе вприэтомизвернутьсяипрошитьочередьюпространствопередсобойперека тилсяполучивприэтомчувствительныйударвпоясницупослалвторуюочеред ьпримернотудакудаипервуюинепрекращаяпалитьповелствolвнизнатотслу чайеслигадуспелрастянутьсянаполузачетноеиспытаниеоконченовсемишен ипораженывкомнатеначалмедленноразгоратьсясветяпопыталсяприподня тьсясполаисразужесхватилсязаушибленныйживотавотнечегопадатьнаор ужиеонокакправилотвердоеиребристоенуикактебекомнатамракаехидноос ведомилсяоператормрачнокакмояфамилиянопоследиснейлендамнеуженичe гонестрашнотакужинестрашнокогдатвойлучшийдругвылетаетсэкзамена условноубитыйпузатойзеленойвороной уженичегохуженебываетнуладно курсантсвободенполучаяназадодеждуяобнаружилчтопокаяотстреливалко товвтемнойкомнатенабрикпоступилосообщениеинтересноотkогоэхвотб ыотджейнтретийсвободныйуикэндинескемпровестиобидновольнослушат елювукомраковичунемедленноявитьсяналейтстриткполковникукоринуоппа

дааэтонеджейнналейтстритразмещалосьместноеотделениеконторыкот
оруювсесодружествокосоухмыляясьименовалоконторойглубинногобурения
хотянаэтомзданиивиселатабличкафирмыпоэкспортукокосовыхореховачут
ьпоодальпанельрекламыпериодическивыплевывающаянастенусоседнегомо
нодомаслоганкокосыгрузимбыстрооноивидноколониивсистемебезкокосовы
хореховневыживутвымрутскореечемотвзрывнойдекомпрессировночерезд
вадцатьоднуминутуяробкоподошелкмерцающейдверицельвашеговизитагр
ознопроревеламозаиканадпроемомтонвопросапредполагалчтоприлюбомне
удовлетворительномответеменяпревратятвоблачкоразогретогопараипод
еломпосколькушлятьсяудверейэтойфирмымогуттольколибоеесотрудникил
ибозлобныеиномиряненуаеслипопадетсякакойтоэкспортеркокосовбываетн
еповезлокурсантмраковичкполковникукоринупроблеяляотдушинадеясьчто
интелктрониканесочтетдрожьвмоемголосехарактернымдляиномирцевпр
изнакоммерцающаязавесаисчезлапроходитеголососталсятакимжерезкими
неприятнымнопокрайнеймересталнаполтонатишеяосторожноступилнас
веркающийполповернитесьлицомкстенесмотритепередсобойпротянитеру
кувотверстиеанализсетчаткииднкпроверяютилиявсамомделевукомракови
чгражданинфедерациидвадцатьпервогогодаотродуилинежитькакаякакго
вориламояпокойнаячешскаябабушканикогданеслышавшаяпроиномирянслед
уйтезакраснымсигналомзакакимещекраснымсигналомпоинтересовалсяяо
творачиваясьотстеныиуставилсянакрасныйогонеквисевшийввоздухепрям
опередмоимлицомследуйтезакраснымсигналомлюбоеотклонениеотмаршру
тасчитаетсянарушениемагашагвсторонупобегпрыжокнаместепровокаци
яэтоужемойрусскийдедушкавывсехтаквстречаетеилитолькоменянапосле
докпоинтересовалсядвинувшисьзаогонькомвсехпостороннихпытающихся
пройтичерезслужебныйвходсообщилголостакиоставивменявнедоумениит
олияговорилсвозомнившимосебеинкомтолиссадюгойохранником

Текст повністю розшифровано, отже, ключ вгадано правильно.

Висновки:

У ході виконання комп’ютерно практикуму при зашифруванні відкритого тексту спостерігаємо, що чим більша довжина ключа, тим менше значення індексу відповідності. А також, проаналізувавши індекси відповідності шифртексту, ми обчислюємо довжину ключа та отримуємо змістовний ключ. Отже, ми отримали практичні навички щодо оцінки ентропії на символ джерела.