КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ
№2 Криптоаналіз шифру Віженера

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

Варіант 4

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.

були вибрані такі ключі:

```
['да', 'нет', 'кора', 'мутка', 'силиконовый',
'авиаконструктор', 'богостроительство',
'межправительственный']
```

довжиною 2, 3,4,5,11,15,17,20

Отримали результат:

```
закодований текст з ключем да:  саиопюыепожеыехктгтрдзчмдвтдсорилвмдтвйгтптзсасигвяпдлдсцрднсагсчда
закодований текст з ключем нет:  ъецыррдкэызчдкгчухыхтфшюнзастащнщпнцызчрубымянтъмзньеэнцдэеяъесюшы
закодований текст з ключем кора:  чофохмзехьтебубкшсюркхгмкрюдчььисршдшрхгшэюзчоэийрлпкщрсьюрнчопсэ
закодований текст з ключем мутка:  щуцшлккчхоошйпсцбхшрмъецаобцчошыщмирбфпгъваснмаъйвзвтхаэевкнщусы
закодований текст з ключем силиконовый:  юипцхмдунйлцярщфьрьтырдфлкштъьогрурпцмурьсйрюишрйриэвжйвъы
закодований текст з ключем авиаконструктор:  нвмохмдцэюхпйубкрлоъофдюрхшцыюмкпвттыучубщахэапрямйьсэ
закодований текст з ключем богостроительство:  оозььрзууазруцгмьдьуошеьокайшкэъйрйтсрцхюэцщтлйщсдйр
закодований текст з ключем межправительственный:  щекэыющнэунбичупырйщммщырврмяучдшфкйыпамъффцэапрс
```

при обратній дії, тобто розкодуванні, ми отримуємо відкритий текст, тобто функції у нас працюють правильно

```
закодований текст з ключем да:  саиопюыепожеыехктгтрдзчмдвтдсорилвмдтвйгтптзсасигвяпдлдсцрднсагсчдабд
розкодований текст з ключем да:  надолючеловеческогоразумаводномизвидовегопознаниявыпаластраннаясудьб
закодований текст з ключем нет:  ъецыррдкэызчдкгчухыхтфшюнзастащнцпнцызчрубымянтъмзньеэнцдэеяъесюшцйх
розкодований текст з ключем нет:  надолючеловеческогоразумаводномизвидовегопознаниявыпаластраннаясуды
закодований текст з ключем кора:  чофохмзехьтебубкшсюркхгмкрюдчььисршдшрхгшэюзчоэийрлпкщрсьюрнчопсэтм
розкодований текст з ключем кора:  надолючеловеческогоразумаводномизвидовегопознаниявыпаластраннаясуд
закодований текст з ключем мутка:  щуцшлккчхоошйпсцбхшрмъецаобцчошыщмирбфпгъваснмаъйвзвтхаэевкнщусыур
розкодований текст з ключем мутка:  надолючеловеческогоразумаводномизвидовегопознаниявыпаластраннаясу
закодований текст з ключем силиконовый:  юипцхмдунйлцярщфьрьтырдфлкштъьогрурпцмурьсйрюишрйриэвжйвъыич
розкодований текст з ключем силиконовый:  надолючеловеческогоразумаводномизвидовегопознаниявыпаластра
закодований текст з ключем авиаконструктор:  нвмохмдцзюхпйубкрлоъофдюрхшцыюмкпвттыучубщахэапрямйьсэрд
розкодований текст з ключем авиаконструктор:  надолючеловеческогоразумаводномизвидовегопознаниявыпала
закодований текст з ключем богостроительство:  оозььрзууазруцгмьдьуошеьокайшкэъйрйтсрцхюэщщтлйщсдйрос
розкодований текст з ключем богостроительство:  надолючеловеческогоразумаводномизвидовегопознаниявыпа
закодований текст з ключем межправительственный:  щекзыющнэунбичупырйщммщырврмяучдшфкйыпамъффцэапрсзх
розкодований текст з ключем межправительственный:  надолючеловеческогоразумаводномизвидовегопознаниявы
```

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

Обраховували індекс відповідності за цією формулою

Індекс тексту Y називається величина

$$I(Y) = \frac{1}{n(n-1)} \sum_{i \in Z_m} N_i(Y)(N_i(Y)-1),$$

```
індекс відповідності для оригінального відфільтрованого тексту:  0.06122075350165384б
індекс відповідності для шифртексту з ключем да 0.04724316274666747
індекс відповідності для шифртексту з ключем нет 0.04226878814366297
індекс відповідності для шифртексту з ключем кора 0.03834376545421867
індекс відповідності для шифртексту з ключем мутка 0.03575499195682921
індекс відповідності для шифртексту з ключем силиконовый 0.035613217815316296
індекс відповідності для шифртексту з ключем авиаконструктор 0.035114217490463735
індекс відповідності для шифртексту з ключем богостроительство 0.034583959874568956
індекс відповідності для шифртексту з ключем межправительственный 0.0328022942851625
```

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

Для тогоб щоб знайти період ключа для нашого шифротексту, розбиваємо його на блоки від 2 до 40 та для кожного блока обчислюємо індекс відповідності та порівнюємо його з теоретичним значенням індекса відповідності для російської мови

Отримали значення
Індекс відповідності для ключа довжини : 2 0.032604641533356106
Індекс відповідності для ключа довжини : 3 0.03257699135676468
Індекс відповідності для ключа довжини : 4 0.032650882017613285
Індекс відповідності для ключа довжини : 5 0.032535443566457684
Індекс відповідності для ключа довжини : 6 0.03256047474074616
Індекс відповідності для ключа довжини : 7 0.03271784961796955
Індекс відповідності для ключа довжини : 8 0.03269169199663074
Індекс відповідності для ключа довжини : 9 0.032514372292478666
Індекс відповідності для ключа довжини : 10 0.03251756583831643
Індекс відповідності для ключа довжини : 11 0.03271373565919388
Індекс відповідності для ключа довжини : 12 0.032635472926334196
Індекс відповідності для ключа довжини : 13 0.05406857059071756
Індекс відповідності для ключа довжини : 14 0.032636645060993646
Індекс відповідності для ключа довжини : 15 0.032435594314224256
Індекс відповідності для ключа довжини : 16 0.03267471665611215
Індекс відповідності для ключа довжини : 17 0.03268312302293296
Індекс відповідності для ключа довжини : 18 0.0325688897981386
Індекс відповідності для ключа довжини : 19 0.032664850427483204
Індекс відповідності для ключа довжини : 20 0.03250727909722938
Індекс відповідності для ключа довжини : 21 0.032769117140656924
Індекс відповідності для ключа довжини : 22 0.03251625436491776
Індекс відповідності для ключа довжини : 23 0.03267222614924123
Індекс відповідності для ключа довжини : 24 0.03263940314112358
Індекс відповідності для ключа довжини : 25 0.03250920522617824
Індекс відповідності для ключа довжини : 26 0.053855062153258665
Індекс відповідності для ключа довжини : 27 0.032348485471290205
Індекс відповідності для ключа довжини : 28 0.032490858928141166
Індекс відповідності для ключа довжини : 29 0.03236269172896086
Індекс відповідності для ключа довжини : 30 0.03239797697809215
Індекс відповідності для ключа довжини : 31 0.032708865523103564
Індекс відповідності для ключа довжини : 32 0.032766987605135016
Індекс відповідності для ключа довжини : 33 0.03239795866216197
Індекс відповідності для ключа довжини : 34 0.03267972383243843
Індекс відповідності для ключа довжини : 35 0.03266782274295362
Індекс відповідності для ключа довжини : 36 0.03257470515037779
Індекс відповідності для ключа довжини : 37 0.0325823328930757
Індекс відповідності для ключа довжини : 38 0.0324563270598457
Індекс відповідності для ключа довжини : 39 0.0538766328880507

Як ми бачимо, на довжині ключа 13 і чисел які кратні 13 (26, 39), індекс відповідності має значення більше 0.53, тоді як для інших довжин, індекс відповідності не більше 0.33, при тому ще й значення на довжині 13, найбільш співпадає з теоретичним значення індексу відповідності для російської мови – **0.0553 (взято з вікіпедії).**

Після знаходження періоду ключа, переходимо до його розшифрування.

Для того, щоб це зробити, ми розбили текст на фрагменти з довжиною 13, тобто рівною нашому періоду, та знайшли найчастішу букву у кожному фрагменті і за цією формулою розшифрували ключ

$k = (y^* - x^*) \bmod m$, де y^* – буква, що частіше за всіх зустрічається у фрагменті Y_i, а x^* – найімовірніша буква у мові, якою написано відкритий текст (для російської мови це буква

Але тут, виникли проблеми, бо функція повертала ключ, щос типу ааааввааватммс, ну тобто щось зовсім не змістовне, потім я зрозумів, що файл з зашифрованим текстом в мене не відфільтрований, в ньому були пробіли в кінці речень, видвливши пробіли і запустивши скрипт ще раз ми отримали ключ: громнкавьдума.

Це вже щось більше схоже на правду, але деякі букви не розшифрувало правильно, подумавши, ми прийшли до висновку що ключем є слово

громыковедьма, тобто назва твору Ольги Uромико, “Професия: Ведьма”

Отримавши ключ ми розшифрували текст:

старминскаяшколачародеевпифийитравницфакультеттеоретическойипра
ктическоймагиикафедрамаговпрактиковчастьперваясоциальныйукладбыт
инравывампирьейобщинывикачтовычтотоимеетепротиввампироврасприн
корпорациямифкурсоваяработаадептквивосьмогокурсавольхиреднойнаучн
ыйруководительмагистрпервойстепениархимагксанперловдевятьсотдевя
ностодевятыйгодпобелорскомулетосчислениюгородстарминведениехоро
шийсегоднявыдалсяденектеплыйбезветренныйвтораядекадасеноставаме
сяцанеспешносочилаьсквозьклепсидрусолнечноголетаиголосазябликовд
оносившиесяизпридорожныхкустовзвенеливушахяехалакквозьихгнездов
ыеугодьякаквдольпограничнойполосыполосойбыладорогазаброшенныйп
роклевывающийсяпыльнойтравойкривойбольшакзябликипопеременновоз
мущалисьвторжениемчеловеканабелойлошадивихчастныевладениязали
хватскиетрелисменялиськриплымчириканьемптахисуетливоперепархивал
иповеточкамтревожалиствуразноцветнаякаймавокругчерныхподсыхающи

хлужвзрываласьсотнямиистомленныхжароймотыльковраскручиваласьвв
ысьвихремтрепещущихкрыльевповодьязавернутыепетлейсвисалисперед
нейлукияпокачиваласьвседлекакмешокскрупойпридерживаялевойрукойл
ежавшеенаколеняхписьмоипытаясьразобратьпрыгающиепередглазамиру
ныромашкапользоваласьмоимрасслабленнымсостояниемвсезамедляяиз
амедляяшагнадеясьчтоявлеченнаячтениемнезамечуеековарногоманевр
аидамейостановитьсяиспокойнопощипатьтравкутычегоэтоголубушкаануш
евеликопытамиплутоватаякобылкаразочарованновсхрапнуладавайдавай
халтурщицаяустроиласьпоудобнейесливообщеможноустроитьсяпоудобне
йнатомпыточномпредметекоимявлялосьдляменяжесткоеказенноеседлон
атретийденьпутиромашкинагриватоненькимиколечкамиспускаласьдопере
днейлукизабиваясьмеждустраницамипухлогописьмакотороеядолжнабыла
вручитьповелителюдогевыикотороеужеминутпятькаксамовольновскрылап
рипомощимагиинетронувувесистойпечатинаверевочкенааломвоскеотчетл
ивопроступалоттискперстнятринадцатьруниперепетающийсясдраконом
единорогвцентретутмоизанятиялитературойдипломатиейигенеалогиейгру
бопрервалиоченьгрубояедвауспелаподхватитьлисткипоползшиевразныес
тороныромашканеисправимаясаботажницазадумчивожевалауздубряцаяж
елезомвтовремякакнезнакомыйивесьмаподозрительныйтипобросшейнар
ужностидемонстративнопотрясалпередлошадиноймордойсамодельныма
рбалетомсгрязнойстрелоймногоразовогоиспользованиятакчтонепонятноб
ылокогоонсобираетсяграбитьменяилиромашкуяприподняласьнастремена
хсинтересомрассматриваязаржавленныйнаконечникянедумаючтоэтосамо
еудачноеместодляторговлиантиквариатомдоверительносообщилаянезнак
омцувотвстарминеувасбыегосрукамиоторваливернееотрубилизнаетелита
моченьнелюбятразбойниковромашкаобнюхалаарбалетпрезрительнофырк
нулаинапрочьигнорируяграбителяпотянуласькаппетитнойзеленималинник
аизвысокойгущикотороготолькочтовозниклоэточудовлаптяхпреступныйэл
ементзаметносмутилсянаконечникзатрепеталкакщенячийхвостикувыдора
скаянияипокаяниябылоещедалекозаблудшаяовцаупорствовалавогрехеср
ебролюбияануткаживослезайсконядевкаязыкатаякошелекилижизньдапо
шустрейслышишьяизобразилаусиленнуюработумыслиладноубедилкошел
екпахнулоозономлицограбителяпередернулосьзрачкирасширилисьглазао
стекленелиионмедленноопустиварбалетотвязалибеспрекословноподалм
нетощиймешокболтавшийсяупоясаотмешкаразилокошкамиикуревомосла
бивверевкустягивавшуюгорловинуяпропустиласквозьпальцынесколькоме
лкихмонетмаловатодорогоймоймаловатосленцойработаешьбезогонькавп
рочемтакужибытьвозьмувкачествеавансаосчастливилаяграбителяшвыря
яемуподногипустоймешокипредупредилаячерезпаруднейэтойжедорогойн
азадпоедутакужбудьдобрпостарайсяменянеразочароватьмужикнеотрыва

яотменязагипнотизированноговзглядамедленнонагнулсяподнялмешокиза
стылстолбстолбомневсилахшевельнутьсябезмоеговедомакактолькогорег
рабительскрылсяизвидуядеактивировалазаклинаниеипозволиларомашке
перейтисгалопаналюбимуюеютрусцуписьмозажатоевовремяподсчетаден
егуменямеждуколеняминемногопомялосьиутратилотоварныйвидвпрочем
рассудилаяглавноенеоформлениеасодержаниеоноежекомпенсировалоне
достаткирепейноголистаиспользованноговукромномместеагавотнаконеци
обомнепарастрокзадифирамбамизагадочномуарракктурупропустишьинез
аметишьзавремяобученияввысшейшколечародеевпифийитравницадептк
авольхапроявиласебязнаюоченьплохонеусидчиванетерпеливасвоевольн
азнакомаяпеснялюбитзлыешуткиинеоднократнопереноситихсвоспитанни
ковнавоспитателейэтоонпроведрочтолидабылоодноведеркодовольнообъ
емистоестоялосебенабалкенаддверьюмоейкомнатыэдакийсамодельныйк
апканнасоседейпошкольномуобщежитиюдабынеповаднобылобезспросуо
далживатьуменяконспектыикастрюлиснавареннымнанеделюборщомможе
тучительтакбынеразозлилсяеслибыведровсетакиопрокинулосьанеупалое
мунаголовустоймявместесводойотличаетсяредкимиспособностямикпракт
ическойитеоретическоймагиисильноразвитойинтуициейбыстроадаптируе
тсякнестандартнойситуациихаможетяещенебезнадежнанеприличнаякака
ятограницаудогевыуэльфоввысокиетравыугномовскалыувадлаковгрудыв
ыброшеннойнаповерхностьземлиудриаддубыподметающиеоблакаудруид
овкаменныекругиулюдейоблупленныестеныканалысзатхлойводойраздел
енныепаройтройкойподъемныхмостовдалысыестражникипринихбдительн
одремлющиеупираясьнаржавыеалебардыаздесьосиныиздевательствокак
оетоособенноеслиучестьчтожителидогевывампирыхорошиетакиеосинысе
ребристыетрепещущиезаосинамищекочетнебоостроверхийеловыйковерс
редикоторогокоегдепроглядываютзатравленныеберезкиисосенкисамажед
огевалежитвдолинекакплюшканаднерасписнойпиалыеслисмотретьсхолм
акраяпиалывиденбелыйободокизосинвторойпотолщепотемнееизелейавц
ентреширокоезеленоедноскрапочкамисамадогевавкольцевозделанныхпо
лейиоблакахтуманаподойдешьвплотнуюкдеревьямнаставлялменяучител
ьипошлешьмысленныйсигналвглубьлесалюбойможешьдуматьочемугодно
лишьбысформироватьмощнуютелепатическуюволнуакомумнееенаправит
ьнаобщейчастотектонибудьизстражейграницыуслышитясмущеннокашлян
улалучшебыемуэтогонеслышатьнеобязательнопродумыватьочереднуюпа
костьзнаюзнаютынанихсверхвсякоймерыгоразданонасейразпостарайсяво
здержатьсяотоныхочемэтояахдаоволневампирыоченьвосприимчивыктеле
патииисразуотреагируютнаееприсутствиехотяинесмогутдоскональнорасш
ифроватьтакчтонапирайнаколичествоаненакачествоваттакясмотрюнадым
ящуюбанюнаморщивлоботусердияинамоюволнутутжереагируютпятьили

шестьадептовкоторыеовеянныепаромвыбегаютиздверейивыпрыгиваютиз
оконатакованныевнезапноожившимивеникамирукибудущихколлегзаняты
шайкамиприкрывающимиотвениковсамоесокровенноеучительусмиряетве
никиоднимдвижениембровиновзглядыадресованныешутниценедомытыми
коллегаминесулятничегохорошегоясказалподуматьанетранслироватьзакл
инанияжальчтозагодыпроведенныевэтихстенахтытакиненаучиласьдумать
чтождумаюстоюподосинойнаморщивлобиромашкаужечтотожуетзеленаяс
люнасочитсяизчерныхуголковбархатистыхгубразделенныхкольцамиудилт
елепатироватьзначитсознательноделитьсямыслямискемнибудьдругимдел
юсьпоследнимизлесатянетпрохладойсидящаянаветкеиволгаудивленнопо
качиваетхвостомвответнамоиумственныепотугилибозанятиеоказалосьмн
енепозубамлибоошарашенныестражиграницыпопадалинаместесраженны
емоеймощнойдумоймоистараниявенчалисьуспехомминутчерезсорокиза
этовремяяуспелапередуматьбольшечемзапредыдущиевосемнадцатьлета
вотирезультатагаподействовалоилионпроходилмимослучайноявпервыеув
иделавампиравозможноеслибыонвозникизниоткудабылбледенкаксмертьи
недвусмысленноскалилокровавленныезубыябыегоиспугаласькаксобствен
ноипланироваламоизнаниявобластивампироведениябазировалисьначело
веческихлегендахипреданияхотличавшихсяредкостнымпессимизмомктом
ужевсегравюрыкартиныгобеленынаскальнаяживописьизображаютвампир
овисключительноночьюивтемнотекрыльязубыкогтивсеэтокажетсятакимст
рашнымиогромнымтолькопотомучтотолкомничегонельзяразглядетьдневн
ойсветразвеялореолужасавпухипрахприсолнечномсветенафонебескрайн
ихполейивысокихдеревьеввампирпоказалсямневозмутительномелкимибе
зобиднымправдаященеспешиласьапришлосьмнегалантнопредложилиру
кувоспользоватьсякоторойвпрочемянерискнулавампирулыбнулсяпоказав
длинныеклыкилюбойулыбнулсябыувидевкакясползласъехалапокрутомур
омашкиномубокуперекинувповодьячерезголовулошадиявыжидающеустав
иласьнавампирастражграницыоказалсявышеменянаполголовышироквпл
ечахивесьманедуренсобойдлинныетемныеволосыобрамлялиузкоезагоре
лоелицосложенныезаспинойкрыльяпридаваливампирунекотороесходство
смороемдемономпосланникомсмертидесятиаршиннаястатуякоторогоукра
шалаактовыйзалвысшейшколычерныепронзительныечутьраскосыеглазав
ампираизучилимоюмалопривлекательнуювнешностьнотакинесумелиразг
адатьчтозанейсокрыто

Цей текст і є уривком твору “Професия: Ведьма”

Висновок

В ході виконання даної лабораторної роботи ми навчились застосовувати методи частотного аналізу, для дешифрування тексту, закодованого шифром Віженера. При чому ми мали лише зашифрований текст, без ключа, довжини ключа тощо. Застосувавши криптоаналіз, ми спочатку знайшли довжину ключа шифрування, потім сам ключ і нарешті розшифрували шифртекст.