Міністерство освіти і науки України

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

Криптографія

Комп’ютерний практикум №2

Експериментальна оцінка ентропії на символ джерела відкритого тексту

Виконали:

Студенти 3 курсу

Гончаров Д. К. та Сергеев А. А.

Мета роботи

Метою даної роботи є засвоєння методів частотного криптоаналізу, а також здобуття практичних навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Постановка задачі та варіант завдання

Завдання:

1. Самостійно підібрати відкритий текст об'ємом 2-3 кб.
2. Зашифрувати обраний текст шифром Віженера з ключами довжини r = 2, 3, 4, 5, а також ключем довжиною 10-20 символів.
3. Підрахувати індекси відповідності для відкритого тексту та всіх отриманих шифротекстів, після чого порівняти їх значення.
4. Розшифрувати наданий шифртекст згідно з індивідуальним варіантом.

Варіант завдання: №2

Хід роботи

На цьому етапі був проведений аналіз шифру Віженера, який є поліалфавітним шифром підстановки. Процес шифрування полягає у додаванні кодів символів відкритого тексту до кодів символів ключа за модулем потужності алфавіту:

$$y_i=(x_i+k_i \bmod r) \bmod m.$$

1. Підбір та шифрування тексту. Був обраний відкритий текст розміром 3-4 кб(неочищений). Шифрування проводилося з використанням наступних ключів(згенерованих випадковим чином):

> "сб","сяв","ччжд","стэйй","тяюгшазэей","мдйчфььвмбж","нгщеякзкйюця","зныкгмшпьцугп","жшвцойуычнюнаь","ояквртюжйпнааэа","жбьуьжмчыотсчюдт","збчикчккищуюсфнш","шзчушуеябщцмюмшиот","згитххезцпрцгжпишбф","эичиырхяикчшфкужосхд"

2. Обчислення індексів відповідності. Індекс відповідності обчислювався за формулою:

$$I(Y)=n(n-1)1\sum t\in ZmNt(Y)(Nt(Y)-1).$$

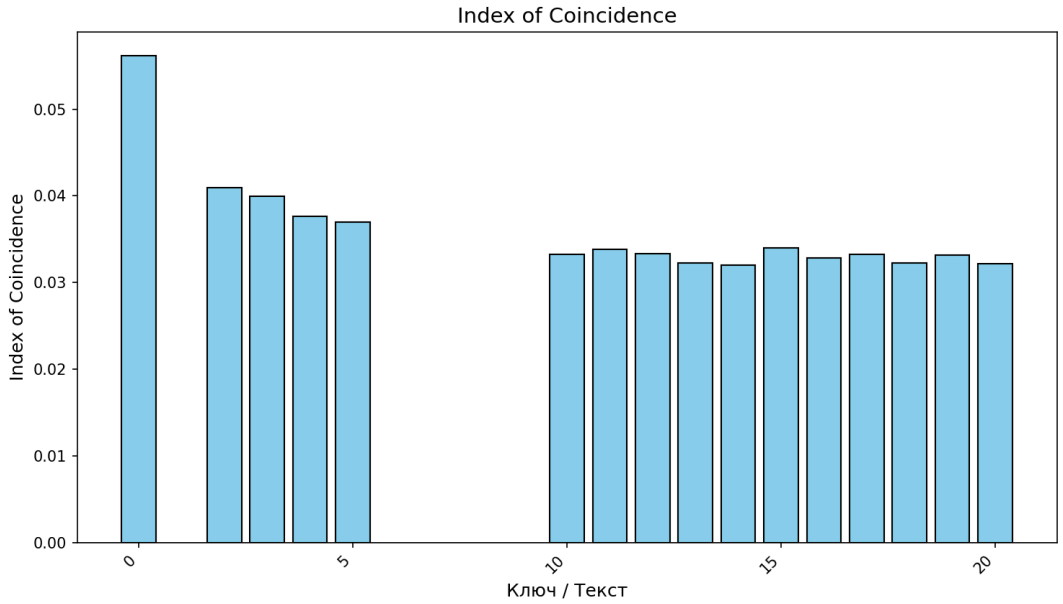
Значення індексів відповідності.

Кожному ключу, яким зашифровувався текст, відповідає індекс відповідності

(0 - відкритий текст)

```
0: 0.056140581736436666
сб: 0.040967184801381694
сяв: 0.039969295720591054
ччжд: 0.03765660553225332
стэйй: 0.03695479343147737
тяюгшазэей: 0.033286728623516190
мдйчфььвмбж: 0.033814184280505526
нгщеякзкйюця: 0.033334978205444524
зныкгмшпьцугп: 0.032287742961318090
жшвцойуычнюнаь: 0.032020177097897305
ояквртккйпнааэа: 0.033979768073032324
жбьуьжмчыотсчюдт: 0.032802039641417880
збчикчккиьщуюсфнш: 0.033268086739589330
шзчушуеябщцмюмшиот: 0.032242783123612140
згитххезцпрцгжпишбф: 0.033146366203361020
эичиырхяикчшфкужосхд: 0.032162732680867400
```

Графік залежності індекса відповідності від довжини ключа



Оскільки перша колонка без шифрування, то індекс відповідності тексту блище до індексу відповідності російської мови(0.0553)

Також зі збільшенням ключа значення IC наближається до 1/m(m = 32, 1/m = ~0.031), що є значенням IC мови з рівноймовірним алфавітом

Код цієї частини: CryptoLab2Encode.py

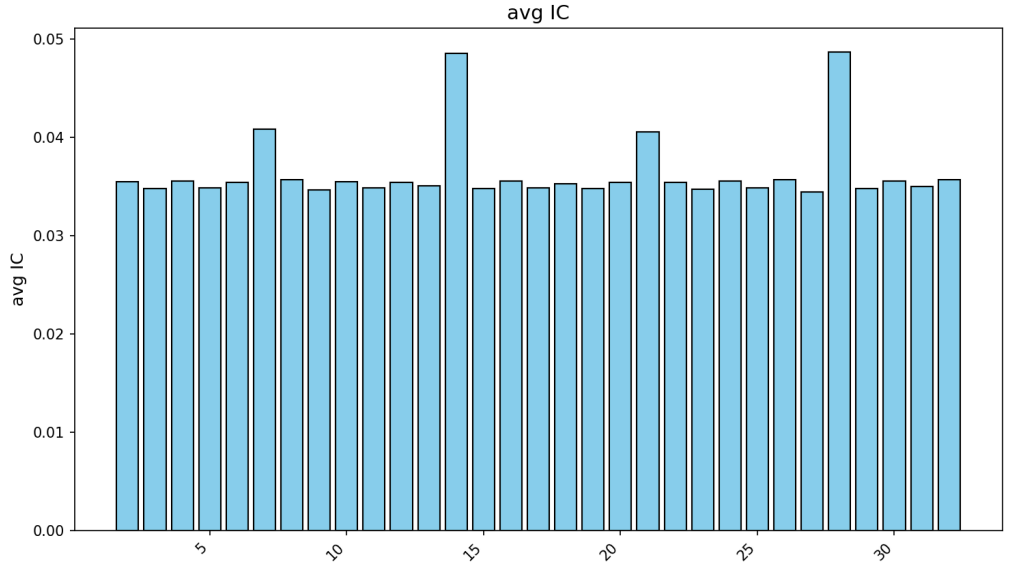
3. Криптоаналіз шифротексту з варіанта

Початково наданий шифртекст був оброблений: усі символи переведені в нижній регістр, а знаки пунктуації, пробіли та літери, що не входять до російського алфавіту, були видалені.

3.1. Визначення довжини ключа

Для визначення періоду (довжини ключа) шифру використовувався **метод аналізу індексу відповідності**. Алгоритм, реалізований у коді, працює наступним чином:

1. Програма перебирає можливі довжини ключа `r` у заданому діапазоні (у коді від 2 до 20).
2. Для кожної потенційної довжини `r` шифротекст розбивається на `r` блоків (підпослідовностей). Наприклад, для `r=3`, перший блок складається з 1-го, 4-го, 7-го символів; другий — з 2-го, 5-го, 8-го, і так далі.
3. Для кожного окремого блоку обчислюється свій індекс відповідності (IC).
4. Обчислюється **середнє арифметичне** значення індексів відповідності для всіх `r` блоків.
5. Довжина ключа `r`, для якої це середнє значення IC є максимальним, вважається найбільш імовірною. Це пов'язано з тим, що при правильному розбитті кожен блок є текстом, зашифрованим шифром Цезаря, і його частотні характеристики (а отже, і IC) будуть близькі до характеристик природної мови.



Аналізуючи діаграму, можна побачити, що максимальне значення середнього індексу відповідності спостерігається при **r = 14**(або 28, але це 14*2), що і є ймовірною довжиною ключа.

3.2. Визначення ключа та розшифрування тексту

Після встановлення довжини ключа `r`, шифротекст знову був розбитий на `r` блоків. Кожен блок Yi є результатом шифрування Цезаря з одним невідомим символом ключа ki. Для знаходження кожного символа ключа був застосований метод частотного аналізу, що базується на кореляції:

1. Для кожного блоку Yi послідовно перебиралися всі 32 можливі варіанти зсуву (від 'а' до 'я').
2. Після кожного зсуву для отриманого тексту обчислювалася сума добутків частот його символів на еталонні частоти відповідних символів у російській мові. Це є мірою відповідності розшифрованого тексту статистиці природної мови.
3. Зсув, який давав максимальне значення цієї кореляції, вважався правильним. Літера, що відповідає цьому зсуву, є відповідним символом ключа ki.

Цей процес був повторений для кожного з `r` блоків, що дозволило повністю відновити ключ.

Знайдене значення ключа: последнийдозор

Розшифрований текст:

какясмогэтосделатьспросилгесерипочемуэтогонесмогсделатьтымыстоялипосредибескр
айнейсеройравнинывзгляднефиксироваляркихкрасоквцелойкартиненостоиловсмотрет
ьсявотдельнуюпесчинкуитавспыхивалазолотомбагрянцемлазурьюзеленьюнадголовойз
астылобелоесрозовымбудтомолочнуюрекуперемешалискисельнымиберегамидаивыпл
еснуливнебесаащедулветерибылохолодномневсегдахолодноначетвертомслоесумрак
аноэтоиндивидуальнаяреакциягесерунапротивбыложарколицораскраснелосьполбустек
аликапелькипотамненехватаетсилысказалялицогесерасовсемпобагровелоответнеправ
ильныйтывысшиймагтакполучилосьслучайнонотывысшийпочемувысшихмаговтакженаз
ываютмагамивнекатегорийпотомучторазницавсилемеждуниминастольконезначительна
чтонеможетбытьисчисленаиневозможноопределитьктосильнееактослабеепробормотал
яборисигнатьевичяпонимаюномненехватаетсилыянемогупройтинапятыйслойгесерпосм
отрелсебеподногиподделноскомботинкапесокподбросилввоздухшагнулвпередиисчезэт
очтосоветяподбросилпередсобойпесокшагнулвпередтщетнопытаясьпойматьсвоютеньт
енинебыличегонеизменилосьяпопрежнемуоставалсяначетвертомслоеистановилосьв
сехолоднеепаротмоегодыханияуженерассеивалсябелымоблачкомаколючимиигламиос
ыпалсянапесокразвернувшисьэтовсегдапрощепсихологическиискатьвыходпозадиясдел
алшагивышелнатретийуровеньсумракавбесцветныйлабиринтизъеденныхвременемкам
енныхплитнадкоторымисерелонизкоезастывшеенебокоегдепокамнюстелилисьвысохши
естеблипохожиенаприбитыйморозомвьюнокпереростокещешагвторойслойсумракакаме
нныйлабиринтнакрылипереплетенныеветвииещепервыйслойуженекаменьужестеныиок
назнакомыестенымосковскогоофисаночногодозоравегосумеречномобличьепоследниму
силиемявывалилсяизсумракавреальныймирпрямовкабинетгесераразумеетсяшефужес
иделвкреслеаяпошатываясьстоялпереднимнукаккаконмогменяопередитьведьонпошел
напятыйслойаяначалвыходитьизсумракакогдаяувиделчтоутебяничегонеполучаетсяказ
алгесердаженеглядянаменятовышелизсумраканапрямуюизпятогослоявнастоящиймиря
несмогскрытьудивлениядачтотебяудивляетяпожалплечаминичегонеудивляетеслигесер

захочетпреподнестимнесюрпризунегобудетогромныйвыборяоченьмногогонезнаюиэтоо
бидносказалгесерсядьгородецкийяселнапротивгесерасложилрукинаколеняхдажеголов
уопустилбудтовчемточувствовалсвоювинуантонхорошиймагвсегдадостигаетсвоегомогу
ществавнужноевремясказалшефпоканестанешьмудреенестанешьсильнеепоканестане
шьсильнеенеовладеешьвысшеймагиейпоканеовладеешьвысшеймагиейневлезешьвоп
асныеместаутебяситуацияуникальнаятыпопалподонпоморщилсязаклятиефуарантыста
лвысшиммагомнебудучикэтомуготовымдаутебяестьсиладатыумеешьеюуправлятьиточт
отыструдомделалраньшетеперьнесоставляетпроблемсколькотыпробылначетвертомсл
оесумракаисидишькакнивчемнебывалоновотточеготынеумелраньшеонзамолчалянаучу
сьборисигнатьевичсказалявконцеконцоввсепризнаютчтояделаюзначительныеуспехиол
ьгасветланаделаешьлегкопризналгесертыженесовсемидиотчтобынеразвиватьсяносейч
астынапоминаешьмненеопытноговодителякоторыйполгодапокаталсянажигуляхивдругс
елзарульгоночногоферраринетхужезарулькарьерногосамосвалабелазавесомвдвестито
ннчтоползетсебепоспираливыезжаетизкарьераарядомпропастьвсотнюметроватамвниз
уедутдругиесамосвалыоднотвоеневерноедвижениерезкийповоротруляилидрогнувшаян
апедалиногаплохобудетвсемпонимаюякивнулнояввысшиенервалсяборисигнатьевичэто
выменяотправиливпогонюзакостейятебянивчемнеупрекаюипытаюсьмногомунаучитьска
залгесеридовольнонепоследовательнодобавилхотьтыоднаждыиотказалсябытьмоимуче
никомяпромолчалоткрывпапкувеликийгесерзавязывалтесемкинабантикяобнаружилчет
ыресвеженькиеещепахнущиетипографскойкраскойгазетныевырезкифакситрифотограф
иитривырезкибылинаанглийскомнанихяисосредоточилсявпервуюочередьперваявырезк
апредставляласобойкороткуюзаметкуопроисшествиивтуристическоматтракционеподзе
мельяшотландиикакяпонялвэтомзаведениидовольнотакибанальномвариантекомнатыс
трахаиззатехническихнеполадокпогибрусскийтуристподземельябылизакрытыполицияп
роводитрасследованиеивыясняетнетливтрагедиивиныперсоналавтораязаметкабылаку
даподробнеепротехническиенеполадкиуженебылонисловатекстбылнемножкосуховаты
мдажепедантичнымснарастающимволнениемяпрочиталчтопогибшийдвадцатипятилетн
ийвикторпрохоровучилсявэдинбургскомуниверситетебылсыномрусскогополитикавподз
емельяотправилсявместесневестойприлетевшейизроссиивалериейхомконарукахкотор
ойискончалсяотпотерикровивтемнотетуристическогоаттракционактотоперерезалемугор
лоиличтотоперерезалобедолагасиделвместесневестойвлодочкекотораямедленноплыл
апокровавойрекемелкойканавкевокругзамкавампироввозможноизстеныторчалакакаято
остраяжелезкакотораяиполоснулавикторупошеедочитавдоэтогоместаявздохнулипосмо
трелнагесераутебявсегдазамечательнополучалосьэээсвампирамисказалшефнасекунду
оторвавшисьотсвоихбумагтретьязаметкабылаизкакойтожелтойшотландскойгазетенкии
воттутконечножеавторрассказалстрашнуюисториюпросовременныхвампировкоторыев
омракеаттракционовсосуткровьсвоихжертвединственнойоригинальнойдетальюбылоутв
ерждениежурналистачтообычновампирывысасываютсвоихжертвненасмертьнорусскийс
туденткакположенорусскомубылнастолькопьянчтобедныйшотландскийвампиртожезахм
елелиувлексянесмотрянавсютрагичностьисторииязасмеялсяжелтаяпрессаонавовсемм
иреодинаковасказалгесернеподнимаяглазсамоеужасноечтотаквсеибылосказалякромеп
ьянстваконечнокружкапивазаобедомсогласилсягесерчетвертаявырезкабылаизкакойтон
ашейгазетынекрологсоболезнованиялеонидупрохоровудепутатугосударственнойдумыч
ейсынтрагическипогибявзяллистокфаксаэтокакяипредполагалбылодонесениеотночног
одозорагородаэдинбургашотландиявеликобританиянемножконеобычнымоказалсялишь
адресатсамгесеранеоперативныйдежурныйилируководительмеждународногоотделаито
нписьмачутьболееличныйчемполагаетсявофициальныхдокументахасодержаниеменян
еудивилосприскорбиемсообщаемпорезультатамтщательнопроведенногодознанияполн

аяпотерякровипризнаковинициациияневыявленопроведенныеепоискирезультатовнедали
привлеченылучшиесилыеслимосковскоеотделениесчитаетнеобходимымнаправитьпере
давайсамыетеплыеприветыольгеоченьрадзатебястарыйковторойлистокфаксаотсутство
валвидимотамбылисключительноличныйтекстпоэтомуиподписиянеувиделфомалермон
тсказалгесерглавашотландскогодозорастарыйдругагазадумчивопротянулязначитнашив
зглядыопятьвстретилисьнетужродственниклионмихаилуюрьевичусамспросишьсказалг
есеряодругомкоэтокомандиркоэтогесерзапнулсяисявнымнедовольствомпокосилсянали
стоккоэтокоэтотебяуженекасаетсяяпосмотрелнафотографиимолодойчеловекэтоибылб
едолагавиктордевушкасовсемюнаяегоневестачтотутгадатьимужикпостаршеотецвиктор
акосвенныеданныеговорятонападениивампиранопочемуситуациятребуетнашеговмеша
тельстваспросилянашисоотечественникичастенькогибнутзарубежомиотвампировтожев
ынедоверяетефомеиегоподчиненнымдоверяюноунихмалоопыташотландиямирнаяуютн
аяспокойнаястранаонимогутнесправитьсяатычастенькоимелделосвампирамиконечнои
всетакиделовтомчтоегоотецполитикгесерпоморщилсядакакойонполитикбизнесменпроб
ралсявдепутатынаголосованияхжметкнопкипотихонькукороткоияснононеверючтонетос
обойпричиныгесервздохнулотецюношидвадцатьлетназадбылопределенкакпотенциаль
ныйсветлыйинойдовольносильныйотиниациииотказалсяобъявивчтохочетостатьсячел
овекомтемныхсразужепослалпрочьноснамиподдерживалнекоторыеконтактыиногдапом
огалякивнулдаслучайредкийнечастолюдиотказываютсяоттакихвозможностейчтооткрыв
аютсяперединыміможносказатьчтоячувствуюсебявиноватымпередпрохоровымстарши
мсказалгесериеслиужнемогупомочьсынутонепозволюегоубийцеуйтибезнаказаннымтып
оедешьвэдинбургнайдешьэтогосумасшедшегокровососаиразвеешьповетруэтобылприк
азноябезтогонесобиралсяспоритькояневольнозапнулсякогдалететьзайдивмеждународ
ныйотделтебедолжныбылиподготовитьдокументыбилетыденьгиилегенду

Код цієї частини: CryptoLab2Decode.py

Висновки

Під час виконання комп'ютерного практикуму було засвоєно та практично застосовано методи частотного криптоаналізу шифру Віженера.

Робота підтвердила теоретичні положення: було продемонстровано, що зі збільшенням довжини ключа **індекс відповідності** шифротексту зменшується, наближаючись до значення, характерного для випадкового тексту. Це ускладнює простий частотний аналіз, але водночас є основою для визначення довжини ключа.

Була успішно реалізована методика знаходження періоду шифру шляхом обчислення **середнього індексу відповідності** для блоків шифротексту при різних ймовірних довжинах ключа. Цей метод виявився ефективним, показавши чіткий пік на правильній довжині. Для знаходження символів ключа був застосований надійний підхід, що полягав у **максимізації кореляції** частотного розподілу розшифрованого блоку з еталонними частотами мови, що є більш точним, ніж орієнтація лише на один найчастіший символ.

В результаті застосування цих алгоритмів вдалося повністю відновити ключ шифрування та успішно розшифрувати наданий у варіанті шифртекст.