Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №2

з дисципліни

«Криптографія»

на тему: «Криптоаналіз шифру Віженера»

Виконали:

студенти 3 курсу ФТІ

групи ФБ-73

Пазон Б.Р., Лутак А.О.

Перевірили:

Чорний О.

Савчук М. М.

Завадська Л. О

Варіант 15

Мета роботи:

Засвоєння понять ентропії на символ джерела та його надлишковості, вивчення та порівняння різних моделей джерела відкритого тексту для наближеного визначення ентропії, набуття практичних навичок щодо оцінки ентропії на символ джерела.

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).

Результати виконнання програми:

Key 1: 0.03382802753796357

Key 2: 0.03387527613011022

Key 3: 0.033591557673601634

Key 4: 0.03350512687280235

Key 5: 0.034413650419806624

Key 6: 0.03315054184619403

Key 7: 0.04102298465319887

Key 8: 0.03418182541893882

Key 9: 0.03355775079175319

Key 10: 0.03471219017143804

Key 11: 0.03339609615263917

Key 12: 0.032374181310351524

Key 13: 0.033621922230116744

Key 14: 0.056341894942346385

Key 15: 0.03484081252546417

Key 16: 0.033750298147510134

Key 17: 0.03307133767497568

Key 18: 0.03211862276954009

Key 19: 0.03384551884580027

Key 20: 0.035349030183590896

Key 21: 0.040723774622079704

Key 22: 0.033581434979826075

Key 23: 0.03334700013666804

Key 24: 0.033282451887103055

Key 25: 0.032905816815649705

Key 26: 0.03368376639358671

Key 27: 0.03214756258234519

Key 28: 0.05209734621499327

Key 29: 0.03347098456857205

Key 30: 0.03386287625418061

key: поснякованд рей

наберегусевернойдвиныпримерновполсотневерстотвпаденияеевгандвикбелоеморесредьгу
стойтайгизатерялась михайлоархангельскаяобительоднаизсамыхдальнихвновгородскойзем
лееслинесчитатьскитупустозерскогоострогачтонапечоререкенудотогоскитаещедобратьсян
адоакздешнеумонастырюпожалуйстахочешьчерезвологдудапотомпосухоневеликийустюг
атамидодвинырукойподатьзнайплывипотечениюахочешьнапрямикчерезладогусвирьонегу
дальшенасевергдеволокомагдеозерамималымиизновгородаудобнеетакизкакихдругихрусск

ихземельчерезустюгвобщемдобратьсявмонастырьмихаилаархангеланевеликапроблемабыл
обжеланиезамолитьгрехиилинаоборотвушкуйничийпромыселпуститьсятожечездвинуне
плохосколотитьватагувыстроитьстругивтомжеустюгедавпутьотустьядвинырекивседороги
открытывсторонычужедальниеневедомыевпечоруввеликуюпермиювюгругденемирнаясам
оедьтакиноровитвсадитьвсердцеушкуйникаоструюкостянуюстрелусмоченнуюгнилойрыбь
ейкровьютутжеипутьинойиноческийкмонастырюсоловецкомувпрочемкнемулучшепоонеге
прямейбудетолегиванычназначенныйвоеводойновойновгородскойэкспедициииспользовал
обапутичастьлюдейвместеснимсамимшлананебольшихлодьяхпосвиридаонегедалеепомор
югандвиксзаходомвсоловкинамолениеиснованаюгкдвинедругаячастьнаправиласьчерезвел
икийустюгснаказомкупитьтамлодейдляморскихплаванийпригодныхкупиличегоужкочамит
елодьиназывалисьпрямоскажемнекаравеллыдаженекоггимелкиекакиетонекрасивыесполук
руглымднищемнекоторыеужхотелибыломордыплотникамзатакиесудабитьдазнающиелюди
отсоветоваливопервыхплотницкихартелейвустюгетьмасварузатеватьсебедорожевыйдетну
авовторыхтакиевоткорабликиинужнычтобсудачейполедовитымполуночнымморямплытько
рпусхотьинеказистыйдакрепкийтеплыйвкаютекаморедажепечканебольшаяимеетсяачтосдн
ищемполукруглымвмореболтаетсильнотактоневеликабедазатольдамивовекнераздавитальд
оввполночныхводахвидимоневидимотолькочтолетомплытьиможноитокакбожьяволябывае
тзатянутморетуманыдатакиечтоносасобственногонеразглядишьилиподуетвдругборейсевер
ныйветерпринесетгромадныельдинывотидумайтолидальшеидтитолипересидетьпереждать
датолькождатьтодолгонькоможноасеверноелетокороткоенеуспеешьоглянутьсяужезимавот
исидитогдазимуйеслисможешьмногоетутнеотумениялюдскогоотпогодызависелонуаужпог
одавестимоотгосподаможноведьбылоидалечеуйтизатритомесяцааможноидовайгачанедобр
атьсятуманыдаштормадальдыпережидаялилдождьбеспросветныйинудныйвсюночьнапроле
тнепереставаякрупныетяжелыекапликолотилипокрышампрогонялисулицредкихприпоздни
вшихсяпрохожихпревращаливхлюпающуюгрязьтянущиесявдольгородскойстеныогородыв
этуночьтемнуюиненастнуюстражникинабашняхстарательнокуталисьвплащиукрываясьотп
орывовпромозглоговетратакойветеробычнобываетпозднейосеньювноябрекогдасыплетсясн
ебанепоймешьчтотолихолодныйдождьтолимокрыйснегаскорееитоидругоесразунотоосень
юасейчаснадворестоялмайхотьинеоченьтотеплыйздесьвсеверныхновгородскихкраяхдаужи
нетакойчтобсоснегомвотужпослалчертпогодкуадядькокузьмаобернувшисьknапарникувыр
угалсяворотныйсторожмолодойкруглолицыйпареньвкоротковатойкольчужкеиостроверхо
мшлемебрызгидождяскатывалисьпошлемупрямозашиворотпарнюитоттоиделоморщилсяпе
редергиваяплечамивторойстражниккузьмавысохшийпожилоймужиксреденькойбородкойи
длиннымивислымиусамиотвернувшисьответрабуркнулвответчтотонеразборчивоевидимос
огласенбылчтоподобнуюпогодкутолькочертипосылаетповерхкольчугиукузьмыдлинныйкр
ашенныйчерникойплащизплотнойдерюгивнебольшойплетеной6аклажкеупоясаплескалась
медовухаславенскийконецслааавенелеслышнодонеслосьспетровскойбашнискрытойпелено
йдождяиночнойтьмоюслаавентутжеподхватилисоседисбашнишестистеннойчтовсотнешаго
воткузьмыснапарникомплотницкийслаавеноткликнулсякруглолицыйнеспиммолдождалсяк
огдадонессяответотсоседейслевасбашничтонасамомберегуволховаобернувшисьподмигнул
угостилбымедкомдядькокузьмавислоусыйкузьмаширокозевнулперекрестилсяистряхнувсб
ородыкаплинехотяпротянулбаклагупейонуфрийдатолькосмотритриглотканеболеместоуна
сбеспокойноенеточтоуэтихонмахнулрукойвлевовсторонуволховскойбашниместечкоимдей

ствительнодосталосьтоещебойкоееслинесказатьбольшебольшаячетырехстеннаябашнянако
торойнеслислужбукузьмасонуфриембылапроезжейвыходилаворотамизагородскуюстенукб
ольшойдорогечтоизвиваласьмежлесовдаболотпоправомутойсторонымногоктомогпожалов
атьихитроватыйкостромскойкупецитихвинскийбогомолецврясеиприказчикновгородскогоа
рхиепископаимосковскийслужилыйчеловекпоследнихпослепораженияновгородцевурекиш
елонирасплодилосьвновгородекудакакмногошнырялитудасюдапоторгучтотовынюхивалин
оссвойсоваливделановгородскиесоветовалиимелинатоправоподоговорукоростынскомупот
омужедоговорувыплачивалновгородмосквеконтрибуциюшестнадцатьтысячсеребромденьг
инемалыенуденьгиуновгородцевводилисьбогдаствыплатятавотточтоужслишкомнахальном
осковитывихделалезлимногимнепонравубылохорошмедокутебядядькокузьмакрякнувпохв
алилонуфрийподиженкавариласвояченицанухорошхлобыстатьдоутраточайдолгостойкадяд
ьковдругнасторожилсяонуфрийчувродекаккричитктодакомутамкричатьтосвесившисьзаогр
аждениебашникузьмаглянулвнизестьктотутальнетямилостивецмонахизобителидымскойче
ртвасмонаховпоночамноситнуисидитеперьутрадожидайсяправильнодядькокузьмаонуфри
юкакикузьменеоченьтохотелосьотворятьтяжелыескользкиеотдождяворотаутромтобогдаст
перестанетдождищеспасимилостивецжалобнозагнусавилмонахитаквесьпромокдониткихот
ьзаденьгупустиатымолисьчащеотчехохотнулонуфрийатоходитвасздесьночамиакинукапом
олчипаряпрервалкузьмаэйотчетыпрокакуюденьгусейчаспомянулпромосковскуюалипроно
вгородскуюакакаятебелюбезнейстражникипереглянулисьнучтоотворяетеворотанетосейчас
кпристанипойдудапогодитывонспускаемсяужезаплативстражникаммонахюркийплюгавист
ыймужичонкасбегающимиглазаминатянулнаголовуплащнаброшенныйповерхрясыискрылс
явдождливойтьмеонпрошелпославнечутьзадержалсяуповоротанаильинскуюулицупостоял
погляделкудатоинехорошоусмехнулсяужопосчитаемсятеперьстобоюзлобнопрошепталонп
осчитаемсяпройдяпославнемонахсвернулнапробойнуюшелсмелонеопасаясьвыбежавшийи
зповоротанарогатицушпыньхотелужмахнутькистенемпришибитьдурногомонахадатотобер
нулсявовремяитатьночнойвдругощерилсясловноувидалотцародногоубравкистеньпоклони
лсяприветливовиднознавалкогдатомонахадаимонахалисговорившисьдальшевдвоемпошли
лишьуфедоровскогоручьярассталисьтатьнамосковскуюдорогупошелчерезмостикпромышл
ятьдальшеаливкорчмукявдохеамонахкбоярскойусадьбесвернулзаколотилвворотанадвореза
шлисьвлаецепныепсыктотоиздворовыхслугпробежалгрузнотопаяподубовымплахамкогота
мчертпринесоткрывайпоскорейпескгосподинуматонеотмосковскихлюдейпосланец

[('э', 56), ('ч', 36), ('ф', 36), ('п', 34), ('а', 25), ('б', 22), ('ъ', 22), ('ь', 21), ('я', 21), ('с', 21), ('у', 19), ('ю', 19), ('в', 15), ('щ', 14), ('ы', 11), ('ш', 9), ('л', 8), ('р', 7), ('т', 6), ('о', 6), ('к', 6), ('з', 5), ('ц', 5), ('д', 5), ('ж', 4), ('н', 4), ('х', 3), ('е', 2), ('и', 1)]

[('ь', 48), ('у', 37), ('я', 30), ('о', 28), ('ц', 26), ('щ', 25), ('ы', 23), ('р', 21), ('б', 20), ('а', 19), ('ю', 18), ('к', 15), ('ъ', 14), ('э', 14), ('п', 13), ('ш', 13), ('т', 12), ('ч', 9), ('с', 9), ('х', 9), ('й', 9), ('г', 6), ('е', 5), ('ж', 5), ('ф', 5), ('м', 4), ('н', 3), ('з', 1), ('д', 1), ('в', 1)]

[('я', 54), ('с', 37), ('ц', 30), ('г', 26), ('в', 26), ('х', 23), ('ю', 23), ('б', 23), ('щ', 20), ('ъ', 20), ('а', 18), ('ы', 18), ('у', 13), ('ф', 12), ('ж', 12), ('э', 12), ('д', 12), ('н', 12), ('ш', 11), ('ъ', 9), ('т', 6), ('р', 5), ('м', 5), ('и', 5), ('ч', 4), ('п', 3), ('й', 3), ('к', 1)]

[('ы', 50), ('т', 34), ('н', 34), ('я', 33), ('ъ', 27), ('х', 26), ('ш', 22), ('э', 21), ('п', 20), ('с', 20), ('ю', 19), ('ч', 17), ('й', 14), ('щ', 13), ('ь', 12), ('а', 11), ('и', 9), ('д', 8), ('р', 8), ('м', 8), ('е', 7), ('у', 6), ('ф', 5), ('о', 5), ('ц', 4), ('в', 4), ('г', 2), ('л', 2), ('ж', 1), ('к', 1)]

[('н', 49), ('я', 41), ('д', 32), ('п', 26), ('с', 26), ('з', 25), ('р', 21), ('л', 19), ('м', 18), ('г', 18), ('к', 17), ('й', 17), ('б', 16), ('т', 15), ('о', 14), ('ъ', 13), ('ы', 11), ('в', 11), ('ю', 11), ('и', 9), ('ц', 8), ('а', 8), ('ф', 6), ('ж', 4), ('ш', 2), ('э', 2), ('е', 2), ('ч', 1), ('х', 1)]

[('ш', 72), ('т', 31), ('п', 28), ('к', 28), ('х', 28), ('ч', 22), ('ь', 22), ('ы', 21), ('м', 19), ('о', 17), ('ф', 17), ('ц', 14), ('ъ', 13), ('н', 13), ('ж', 12), ('э', 12), ('щ', 10), ('й', 9), ('у', 7), ('в', 7), ('с', 6), ('б', 6), ('я', 6), ('л', 6), ('е', 5), ('и', 4), ('ю', 3), ('г', 2), ('а', 2), ('р', 1)]

[('ь', 48), ('ц', 35), ('ы', 32), ('а', 30), ('у', 28), ('о', 27), ('р', 26), ('щ', 25), ('ю', 22), ('я', 19), ('б', 19), ('т', 17), ('ш', 14), ('э', 14), ('к', 12), ('с', 10), ('ъ', 10), ('й', 8), ('х', 7), ('е', 6), ('п', 6), ('ф', 6), ('г', 5), ('ж', 5), ('н', 4), ('ч', 3), ('м', 2), ('д', 1), ('з', 1), ('л', 1)]

[('р', 58), ('з', 41), ('к', 33), ('в', 24), ('м', 24), ('п', 23), ('д', 20), ('ф', 19), ('н', 19), ('х', 18), ('с', 18), ('т', 18), ('о', 15), ('у', 14), ('л', 11), ('ж', 11), ('э', 9), ('ю', 9), ('б', 9), ('ъ', 8), ('г', 7), ('й', 7), ('е', 6), ('и', 6), ('ш', 5), ('ч', 4), ('щ', 4), ('а', 3)]

[('о', 51), ('н', 32), ('е', 32), ('а', 30), ('р', 29), ('т', 29), ('и', 28), ('д', 26), ('с', 25), ('в', 20), ('л', 20), ('к', 16), ('м', 16), ('у', 13), ('й', 11), ('ы', 10), ('х', 8), ('г', 7), ('п', 6), ('ч', 6), ('ь', 6), ('з', 5), ('б', 4), ('ю', 4), ('ж', 4), ('ш', 2), ('щ', 1), ('я', 1), ('ц', 1)]

[('ы', 56), ('т', 39), ('н', 36), ('я', 28), ('х', 26), ('ю', 26), ('э', 24), ('а', 20), ('ъ', 19), ('ш', 18), ('п', 17), ('щ', 16), ('ч', 14), ('с', 14), ('м', 10), ('й', 10), ('ь', 9), ('л', 8), ('р', 8), ('в', 7), ('д', 7), ('ц', 7), ('и', 7), ('ф', 5), ('о', 5), ('у', 4), ('ж', 1), ('е', 1), ('г', 1)]

[('т', 46), ('ц', 32), ('д', 28), ('х', 27), ('п', 25), ('й', 25), ('с', 23), ('и', 19), ('о', 19), ('ф', 19), ('ж', 18), ('м', 18), ('р', 14), ('у', 14), ('з', 13), ('а', 13), ('ч', 12), ('г', 11), ('ь', 10), ('е', 9), ('н', 9), ('щ', 8), ('я', 8), ('ы', 7), ('л', 7), ('к', 6), ('в', 2), ('э', 1)]

[('ю', 58), ('х', 39), ('ш', 31), ('р', 30), ('э', 29), ('т', 26), ('б', 23), ('а', 23), ('ы', 22), ('в', 22), ('г', 21), ('ъ', 17), ('ф', 10), ('я', 10), ('м', 10), ('л', 10), ('ь', 10), ('п', 9), ('у', 7), ('з', 7), ('о', 5), ('е', 5), ('ц', 4), ('и', 3), ('щ', 3), ('с', 3), ('ч', 3), ('ж', 2)]

[('у', 47), ('к', 33), ('е', 28), ('т', 28), ('ч', 26), ('н', 26), ('ц', 24), ('ш', 21), ('р', 18), ('п', 17), ('х', 16), ('з', 16), ('й', 14), ('с', 13), ('б', 13), ('ф', 13), ('о', 11), ('д', 11), ('и', 10), ('а', 10), ('л', 9), ('ь', 9), ('ж', 7), ('ъ', 5), ('ы', 4), ('г', 3), ('м', 3), ('э', 2), ('щ', 2), ('ю', 2), ('в', 1)]

[('ч', 52), ('о', 39), ('ы', 33), ('й', 28), ('ц', 25), ('ъ', 24), ('у', 22), ('ф', 19), ('щ', 18), ('с', 17), ('л', 16), ('х', 16), ('е', 15), ('ь', 15), ('ш', 12), ('м', 12), ('н', 12), ('т', 12), ('д', 8), ('п', 7), ('и', 7), ('а', 6), ('б', 5), ('к', 5), ('з', 4), ('р', 4), ('ю', 3), ('в', 3), ('ж', 1), ('я', 1), ('э', 1)]

Висновок:

Виконавши роботу, ми здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера та засвоїли методи частотного криптоаналізу на прикладі шифру Цезаря.