Міністерство освіти і науки України Національний технічний університет України

“Київський політехнічний інститут ім. Ігоря Сікорського” Фізико-технічний

Інститут

КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

13 варіант

Виконали: Студент групи ФБ-05 Даниленко Данило,

Студентка ФБ-05 Мірошніченко Ілона

Київ – 2022

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:

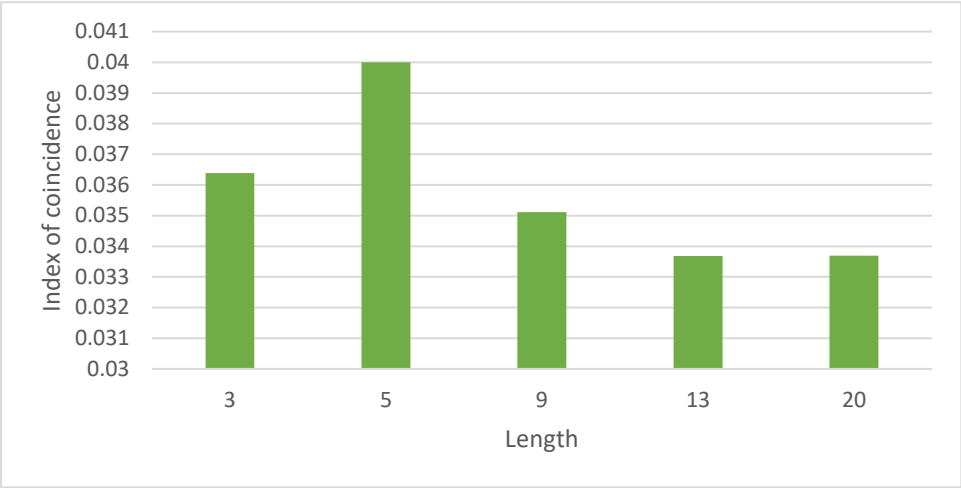
Перед виконанням роботи були розглянуті теоретичні відомості в методичних вказівках. В якості експериментального тексту був взятий уривок з книги Герберта Уеллса «Машина Времени», 2.22 кб, записаний у файлі final_text.txt

Для відкритого тексту індекс відповідностей: Coincidence index start = 0.05385242246721097

Для російської мови індекс відповідностей: 0.0553

Таблиця індексів відповідностей:

Length	**Keys**	**Coincidence index**
3	вам	0.0363900548918308
5	топор	0.039997232344665345
9	программа	0.03510770792010701
13	пакетирование	0.03368390300905638
20	деревообрабатывающий	0.03369620369943263

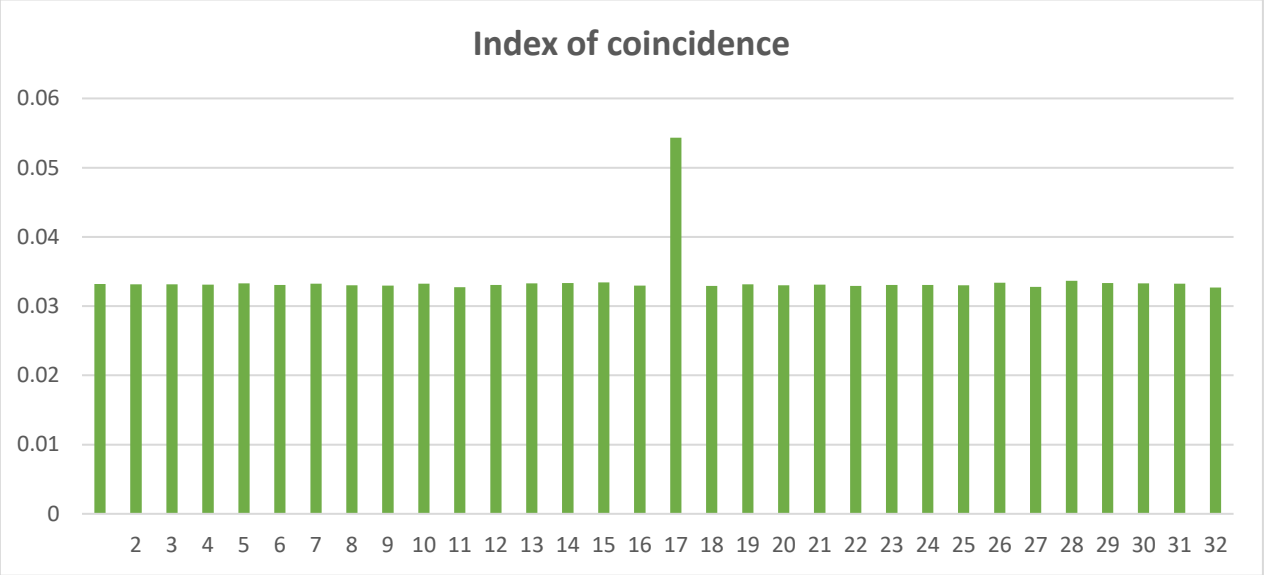


Таблиця індексів відповідностей для блоків:

Key	Index of coincidence
1	0.033177902
2	0.033139612
3	0.033139927
4	0.033121773
5	0.033298051
6	0.033076578
7	0.033237132
8	0.033031246
9	0.032982725
10	0.033244332
11	0.032745301
12	0.033049737
13	0.033276835
14	0.033353653
15	0.033439311
16	0.032988511
17	**0.054315622**
18	0.032905838
19	0.03313958
20	0.03302088
21	0.033118326
22	0.032921418
23	0.033039372
24	0.033062586
25	0.033018974
26	0.033366139
27	0.03280406
28	0.033652542
29	0.033328562

30	0.03330443
31	0.033246992
32	0.032692656

Як бачимо, довжина нашого ключа буде = 17.



Найчастіші символи в російській мові. У нашій роботі ми брали літери о, е та а.

о	0,092817
а	0,071716
е	0,069333
н	0,056529
и	0,056356
т	0,050249
с	0,044751

Ключ, який ми отримали в результаті: **родинабезразличия**, 17 символів.

В результаті, ми отримали розшифрований текст:

экскаваторприземистыйидлинныйсловнотепловозсдалековынесеннойсуставчатойтягойичудовищ
нымзубатымковшомгусеницыглубоковминалисьвпочвуоставляядвенепрерывныеребристыедорож
киразящеесоляройлязгающееоноперлонеразбираядорогииготовобылосокрушитьвсенасвоемпути
оночудищегенералпроскместуневсилахпошевелитьсяеслиэтоконтрольныйсюрпризтовесемироч
ченьвысокогообудущемведьмакемненияапотомстрахизамешательствонеожиданносхлынулиостал

осьтолькоспокойствиеиглубокаяуверенностьразумведьмакапустьдажеиначинающеговсеравногиб
чеибыстреетупыхинстинктовдикоймашиныпобедитьбесхитростнуюмощьможноибезоружияодной
лишьсилоймыслиеслизнаешькакгенералзналпокатольковтеорииноведьвтомисостоитсмыслконтро
льныхполевыхзаданийвпривязкетеоретическихзнанийкреальнойобстановкеодновременномелькн
улашальнаяивданныймоментмалоуместнаямыслишкавотзачемустроилииспытаниевпустоминенас
еленномпаркетакойэкскаваторнагородскихулицахстолькобывсегопорушилзадесятьлетнеотрослоб
ыитакимеетсякарьерныйгусеничныйэкскаватормоделимоделиачертегознаеткакоймоделимногото
ннаялязгающаягромадинаповсейвидимостиоснащенабортовымкомпьютеромсвозможностьюудал
енногодоступаидистанционногоуправленияповсейвидимостивышлаизподконтроляиуспеланатвор
итьлихихделвонэльфвесьокровавленныйваляетсякстатипреттоонапрямонаэльфанадоотвлечьгене
ралпрекраснозналслабоеместотакихмеханизмовнеповоротливостьползаюттакчточеловекнасвоих
двоихобгонитпоэтомуонсорвалсясместанабегуподхватилстравышмотникипультсиганулчерезнекст
атиподвернувшийсякустиобежалэкскаваторслеватотсразузамедлилсяивдругпроворновыпросталп
олусогнутыйдоселековшсхрустомпереломилосьмолодоедеревцесловноспичкагенералуспелвовре
мяубратьсянабезопасноерасстояниечудовищеразворачивалосьготовоеринутьсянапрячущегосявпо
длескеведьмачонкагенералнеутратилхладнокровиянапротивонужепросчиталкудаметнетсясейчас
воонтудазаогромныйстолетнийдубвнесколькообхватовунегоподитакиекорничтоиэкскаваторусход
унесворотитьжизньонавсегдасильнеежелезаимоторовивдругугенералапоявилсянежданныйсоюзн
икмелькнуласредиветвейистволовкоричневозеленаякурточкаиневдалекепоказалсяещеодинэльфо
детонбылточнотакжекакинедавнийпациентгенералановотличиеотпервогопребывалвполномздрав
иииисохранностиивдругугенералапоявилсянежданныйсоюзникмелькнуласредиветвейистволовкор
ичневозеленаякурточкаиневдалекепоказалсяещеодинэльфодетонбылточнотакжекакинедавнийпа
циентгенералановотличиеотпервогопребывалвполномздравииисохранностипультутебякрикнулон
генералугенералмолчапоказалемучерныйначиненныйэлектроникойбрикетаключтеперьгенералст
ольжевыразительнопохлопалсебяпокарманукурткиэльфсловноподземлюпровалилсярастворилсян
афонелиствыапотомвозникужесовсемрядомвпарешаговвыскользнулиззастволатогосамогодубаэкс
каваторгромыхалгусеницамиинатужнолязгалковшомпробираясьсквозьпаркдеревьяжалобнотрещ
алииломалисьрождаласьноваяпросекаэльфтребовательнопротянулрукуигенералнеколеблясьотда
лемупультсключоммедлитьэльфнесобиралсятутжевставилключведвариметнующельнаторцепуль
тараздалсянегромкийщелчокелеслышныйнафонепроизводимогоэкскаваторомшумапальцыэльфаз
апорхалинадклавиатуройпультивпрямьоченьпоходилнаноутбукстойлишьразницейчтоэкранунегоб
ылсовсемкрохотныйирасполагалсяненаоткиднойкрышкеапряморядомсклавишамикрышкисобстве
нноинебылововсеотвлекиеговластноскомандовалэльфибеззвучноканулвкустычтотоунеговидимон
еладилосьгенералпослушнопотрусилпоширокойразмашистойдугеэкскаваторнакакоетовремяприт
ихотслеживаяегоперемещенияапотомсталгрузноразворачиватьсяподгусеницамизахлюпалоонвъех
алвобширнуюоторочennуюмхомлужугенералпользуясьмоментомшмыгнулмонструзакормунаразв
оротутогоуйдетдовольномноговременисравнительнобыстрогенералотступилкобширнойовальной
полянепочемутоемубыложалкогибнущиеподгусеницамииковшомдеревьявконцеконцовпаркитака
яжечастьгородакакиквартальяведьмакобязанхранитьгородвесьцеликомаполянупустьутюжитподу
малонтраванедеревоещевэтомгодуотрастетнеуспелмонстрвыползтикполянкекакоткудатосбокупо
казалсядавешнийэльфмелкойвихляющейрысцойонприблизилсякгенералуплоходелосообщилэльф
онзаблокировалвсевходныепортынадолезтьвкабинугенералвдумчивошмыгнулносоминичегонеск
азалдаичтоонмогсказатьатысобственноктопоинтересовалсяэльфведьмакчтолиначинающийуточни
лгенералскромнокакойвыходпервыйнесталвратьгенералэльфсаркастическихихикнулвезетжемнев
прочемчегоэтояиначепришлосьбыводиночкукстатичтосранавеноромэтотвойприятельнавсякийслу
чайсправилсягенералкоторыйпультпотерялдаатыневиделлежитрядомсаллеейбезсознанияунегове
сьбокразодраняегоаэрозолемспрыснулвашимэльфнахмурилсядавесамаэвыругалсяэльфонможетн
евыдержатьтвойприятельумиралкогдаянанегонаткнулсяулыбнетсясудьбавыживетсудьбаредкоул
ыбаетсяэльфамведьменышзапомниэтогенералсмолчалладнослушайменянужнозадуритьэтоймахи
неегопоганыенавигационныерецепторыипопастьвкабинутымнепоможешьразуввязалсявэтоделo

боюсьтамвкабинеоднойпарырукбудетмалоподеревьямлазатьумеешьумеюпошлиэльфзаткнулбесполезныйпокапультзапоясштановиделовитозашагалкужевыбравшемусянаполянуэкскаваторуотвлекайпоканапомнилонпобегайунегопередмордойтолькосмотриподковшнеугодиугубуркнулгенералкакможнобезразличнеебегатьпередмордойэкскаватораоказалосьнастолькожеутомительнымзанятиемскольинебезопаснымпервоежезабеганиеедванезакончилосьтрагическимонстррезковыпрямилполусогнутыйковшодновременноподавшисьвпередизаделплечогенералатоткубаремполетелвтравусовершенноошарашенныйещевпадениисообразивчтопридетсямолниеносновскакиватьневзирая набольиубиратьсяметровнадвадцатьвсторонусообразилонправильносдвухсекуннойзадержкойвместогдеонприземлилсявпечаталсяковшпохожийнагигантскийжелезныйкулак

Висновки:

У ході даної лабораторної роботи ми розглянули шифр Віженера, засвоїли методи частнотного криптоаналізу, знайшли індекси відповідності для тексту, а також реалізували зашифрування та розшифрування даних.