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.

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:

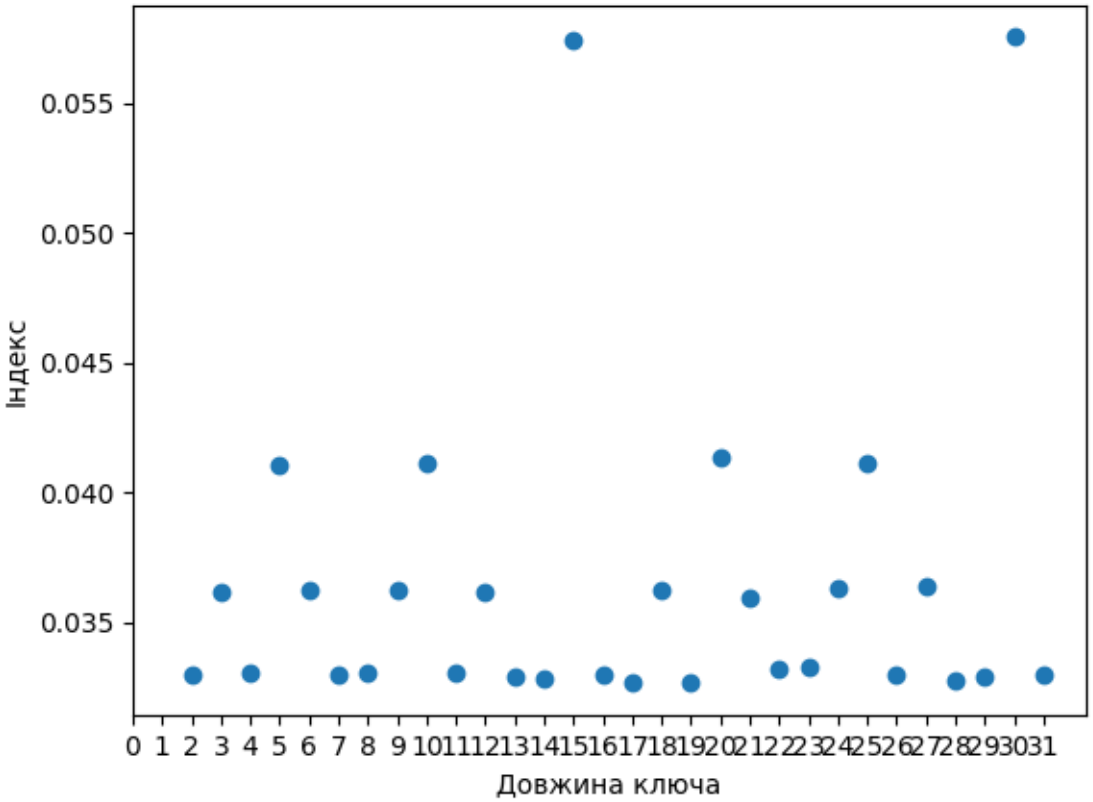
текст для шифрування:

стивенкингстрелоктемнаябашняэдуферманукоторыйнасвойстрахирискпрочитывалэтиглавыоднузадругойчайльдроландкбашнетемнойпришелробертбраунингглавачеловекквчерномпыталсяукрытьсявпустынеастрелокпреследовалегопустыняэтаапофеозвсехпустыньгромаднаярастянулась досамогонебанадолгиепарсекиповсемнаправлениямбелаяслепящаяобезвоженнаяибезликая толькомутноемаревогорнойгрядыразмытыйнаброскнагоризонтедасухиепучкибестравычтопринаситисладкиесныикошмарыисмертьредкийнадгробныйкаменьбылуказателемнапутиаузенькаятропапетляющаяпощелочномунастувотивсечтоосталосьотстолбовойдорогигдекогдатодавнымдавноходилидилижансыстехпормирсдвинулсясместамирсталпустымстрелокшелспокойноне торопясьноивременидаромнетратядорожныйбурдюкобвивалсявокругегопоясаточнораздувшаясясосискапочтиполныйбурдюкводынеодингодсовершенствовалсястрелокквкхефеидостигпятогоуровнянаседьмомиливосьмомонбывообщенеиспытывалжаждыонбытогданаблюдалзатемкакеготелотеряетводусравнодушнымвниманиемотстраненногонаблюдателяиувлажнялбырасщелиныэтоготелаитемныеглубиныегопустотлишьтогдакогдаразумподсказываетчтоэтодействительнонеобходимоноонедостигниседьмогоуровнянивосьмоготолькопятогоипоэтомужаждатомилаегохотяонпоканеиспытывалнеодолимойпотребностипитьэтоемудаженравилосьэтобылоромантичноподбурдюкомревольверыегоревольверычтокаквлитыеложатсяврукудваремнякрестнакрестнабедрахдвекобурыпромасленытакчтоихнерастрескаетдажежарэтоговраждебногосолнцаложиревольверовизлучшейсандаловойдревесиныжелтыетщательноотполированныесъешь

*результати шифрування винесено в окремі файли

Довжина ключа	індекс
2	0.046553432210081985
3	0.03852460193254749
4	0.03666958606728022
5	0.037316640104906984
10	0.03313088965144271
15	0.03248287843328691

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):

ключ: *абсолютныйигрок*

розшифрований текст:

преждечемсменитьдежурногонапостувкоконеобсерваториионвсегдазаходилвзалвизинг
ачтобыпочувствоватькосмоснапрямуюнечерезсистемыдатчиковисигнализирующихустройств
погранзаставабылаустановленавэтомглухомуголкеметагалактическогодоменаболеетысячилет
назадкогдачеловечестворасселялосьпозвездамбурнымитемпамииверіловсвоеобожественноепр
едназначениевсудьбоносностьцивилизациииивседозволенностьотдельныхеепредставителейпот
омпришелзвездныйконструкторипоказаллюдямихместовмирозданииныевозможностиспособ
ыобработкиинформациицелибытияилогикунедоступнуюгордомуизаносчивомувидухомосапи
енсонзахватилсотнилюдейвовремядолгойспячкипревративихвсвоихверныхрабовсъелполовин
умарсапородыкоторогоиспользовалдлярастаплотивпериодсозреванияушелчерезстослишнимл
етвернулсяобратнокаквозвращаетсядомойблудныйсынпоследолгихскитанийпомирунечаянно
почистилсолнечнуюсистемуедванеуничтоживеевовремявизитаисноваушелтеперьуженаполсот
нилетапотомначалассьстраннаяистрашнаявойназаконовотголосоквеликойигрыуниверсумассам
имсобойиконструкторставшийктомувремениоднимизигроковметавселенныхвернулсяксолнцу
наэтотразпопросьбеземлянвойнашлавовсюнавсехуровняхотсоциумадофизическихпринципов

бытияходыигроковвоспринималисьчеловечествомкаквторжениефундаментальногоагрессорап
опыткауничтоженияцивилизациииинезнаниезаконовигрысделалолюдейзаложникамисвоихсобс
твенныхвнутреннихзаконоввосприятияреальностиониначалисопротивлятьсячтобывыжитьхот
ясилыбыликонечнодалеконеравныпросачиваниевовселеннуюметагалактическийдоменпредст
авлявшийсобойоднуклеткуорганизмауниверсумачужихзаконоввфизическомпланеимевшихвид
неуничтожимыхникакимиспособамиколючекназванныхнагуалямипринялонеобратимыйхарак
теркатастрофапроизошланевнезапноеждалисолнечнаясистемазарасталаколючкамичертополо
хаинойреальностивтечениемногихмесяцевпокаонинепревратилисьвнепроходимыезарослиако
гдаразмерынагуалейэтогоабсолютногоничтоиликакговаривалиученыеквантовотоннельныхуш
ейвакуумаинойтопологическойструктурыторчащихввакуумеродногодоменадостиглиразмеров
космическихобъектоввпаянныхвпространствопланетысистемыначалиразбиватьсяониходназа
другойсначалапогибюпитерсамаябольшаяпланетасолнечнойсистемытакинедостигшаястадииз
вездызаеекончинойнаблюдалимиллионылюдейнавсехобитаемыхтелахсистемывпоселенияхче
ловечестваудругихзвездгдекартинасотрясениямирозданиябыланеменеестрашнойсармадыкосм
офлотаиразногородакосмостанцийюпитершествуяпоорбитевокругсолнцанаткнулсянагигантс
кийсростокнагуалейисталразваливатьсянатричастикакобыкновенныйкомснегавсегозатричаса
превратившисьвметановодородныесвкрапленияминодыитвердыхчастицразмеромотметрадоты
сячикилометровструиязыкиокутанныепостепеннозамерзающейатмосферойклокотаниераздир
аемогогигантасопровождавшеесяколоссальнойсилывзрывамисветовымитепловымизлучением
длилосьещедолгооднакопланетойюпитербытьпересталтажеучастьпостиглаегособратьевповне
шнемупоясусатурннептунуранплутонегоспутникахаронактомувремениуженесуществоваловн
утренниепланетымарсвенераимеркурийпострадалисравнительноменьшеавскореподошлаочер
едьземлиибезтогополуразрушеннойстолкновениямиснагуалямипронизывающимипростреливаю
щимиеенасквозьколыбеличеловечествавкакойтомереповезлоеепопытались ьзатормозитьинаг
уальнеразодралземлюнераздробилначастикакбольшинствопланетсистемыавсеголишьсплющи
лвлепешкусбахромчатымикраямиземлянаткнуласьбуквальнонастенунагуалейипревратиласьв
подобиебиблейскойполусферыразвечтопокоящейсяненатрехслонахкитахичерепахахананевид
имомсверхтвердомколючемоснованиичужойреальностилюдейктомувременинанейоставалось
ещемногодалеконевсеземлянеуспелипереселитьсякновомусветилужелтойзвездетакогожеклас
сачтоисолнцеврассеянномзвездномскоплениигиадырасположенномвсозвездиительцапланетуд
ляпереселенияготовилиспешноипримассовойэвакуацииогромногоколичестваземлянпроизошл
онемалокатастрофинесчастныхслучаевунесшихмиллионыжизнейоднакотеперьулюдейбыладр
угаяродинакоторойнегрозилаучастьземлииижизньпродолжалась хотяипоновымзаконамивсоотв
етствиисновымибиологическимиритмамиродноесолнцечеловечествауцелелохотявсеегоритмы
иколебанияестественнонарушилисьавизлученииипоявилисьранееотсутствующиеспектральные
линииизвездыпродолжалисветитьхотямногиеизнихразбилисьонагуалиипогаслиноонибылитакд
алекиотземличтосветихещелетелчерезпространствогалактикиинебонадуспокоившейсяперест
авшейвращатьсяидвигатьсявокругсолнцалинзойземлитемнелопостепеннопомеретогокакумир
алилучизвездправдапереселившееся человечествовидетьэтогонемоглосвязьсбывшейродинойп
ослеразрушениясистемыметромгновенноготранспортапрактическипрервалась вовсякомслучае
длябольшинствалюдейнамногиесотнилетуцелевшиеземлянеостались предоставленнымисамис
ебенаступилмирфундаментальныйагрессорфагтоестьодинизигроковсумевшийизменитьфизич
ескиезаконысуществованияметагалактическогодоменавкоторомжилилюдипокинулегоэтимигр
окомоказалсяконструкторпитавшийкродухомосапиенснечтовродесыновнейпризнательностио
нсделалсвойходзакончившийвойнунагуалипостепеннопрекратилирастиувеличиватьсявобъем
епространствовремяпересталошататьсяоднатискомчужихзаконовкосмосуспокоилсяночерезн
екотороевремялюдиуцелевшиепослекатастрофыназемлеилигееобнаружилистенкиограничива
ющиечастьметагалактикикоторая былаповрежденавторжениемфагастенкиобразовалинечтовро
деколоссальногоаквариумавнутрикоторогооказалась игалактикассистемойсолакакназвализвез
дузаменившуюсолнцепробитьсясквозьнихнаружувглубиныдоменалюдямнеудалосьавскореон
иперестали обращатьнастенкивниманиезанятыепроблемойвыживанияцивилизациилишьпогра
нзаставыавтономныепочтиненуждающиесявснабжении станциисозданныепогранслужбойчело

вечестваещевовременавойнысфагомпродолжалинестисвоюслужбунаблюдатьзаизменившимся космосомиграницамиаквариумаполучившегоназваниекосмориумнообитателипогранзаставдел алиэтонеохотнозачастуюневыполняявозложенныенанихобязанностипростоиспользуяудобные достаточнокомфортабельныестанциивкачествеобыкновенногожильятакойсамостоятельнойте хническойсистемойбылаипогранзаставасоколнакоторойпроживаласемьяпограничниковчетвер омужчинитриженщиныихвахтаначалась всегополгоданазадинаблюдатьзавселеннойимещенена скучилоиштванкараочнулсяонстоялпосредизалавизингапогранзаставыпредставлявшегособой небольшойпрозрачныйкуполсчернымполомикаказавороженныйсмотрелнадвеяркиезвездывзен итепохожиеначьитовнимательныеглазапогранзаставасоколрасполагалась невсоседнейссоломз вездной системеидаженевсоседнейгалактикесветотсюдадобиралсябыдогеиполторамиллиардал етпоэтомуниокакомзнакомомрисункесозвездийречьнешластанциюстроилинаспутникенеболь шойжелтойзвездыбезводномибезатмосферномхотяониимелзапасыльдаизамерзшихгазовсилат яжестинаэтоймалойпланеткесоставлялалишьдесятуюдолюземнойчтонедоставлялонеприятны хощущенийобитателямстанциивнутрикоторойподдерживалась нормальнаясилатяжестизвезда внастоящиймоментскрывалась подполомвизингаиэтопозволяловидетьдругиезвездыколичеств окоторыхуменьшалось скаждымчасомистенкукосмориумаразделявшуювидимыйкосмоснадвеч астиноеслиучеловекаотсловастенавозникалаопределеннаяассоциациявызывающаявпамятиоб разкирпичнойкаменнойилидеревяннойстенытостенкакосмориумабольшепоходиланаземноесе верноесиянияенабесконечнуюволокнистуювуальсотканнуюизбагровосветящихсяпаутинокижи локиказалась ненадежнойхрупкойпушистойполупрозрачнойлегкопреодолимойнасамомжеделе пробитьеепроникнутьсквозьстенкувглубиныдоменанесмогниодинземнойкорабльвтомчислеиз вездолетыструнныхвидовихпростовыворачивалообратнословностенкадействительнобылаодн остороннейповерхностьюкакпредположилиученыеещесотнилетназаднереагировалаонаинаэн ергетическоевоздействиеилокальноеизменениетопологиивакуумаговоряужеоборужиипопр ощесозданномнаосновеприменениянучковчастицвысокихэнергийисиловыхполейстенкикосмо риумаоказалисьабсолютнымпрепятствиемчтоясноуказывалонаихпредназначениезакапсулиро ватьповрежденнуюнагуалямичастьметагалактическогодоменаинепущатьзаразучужихзаконовз аеепределыгдеэкспансияинойреальностинеприобрелаещемасштабовлетальногоисхода

Висновок:

У даній лабораторній роботі ми розібралися з методами частотного криптоаналізу. Також здобували навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.