Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського» Фізикотехнічний інститут

«Криптографія»

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Варіант 2

Виконали:

Студенти групи ФБ-04

Дмитренко Данїїл

Сербіненко Олексій

Мета роботи:

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

Постановка задачі:

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

Для виконання першого завдання був взятий текст: «

У сильного всегда бессильный виноват:

Тому в Истории мы тьму примеров слышим,

Но мы Истории не пишем;

А вот о том как в Баснях говорят.

Ягнёнок в жаркий день зашел к ручью напиться;

И надобно ж беде случиться,

Что около тех мест голодный рыскал Волк.

Ягнёнка видит он, на добычу стремится;

Но, делу дать хотя законный вид и толк,

Кричит: «Как смеешь ты, наглец, нечистым рылом

Здесь чистое мутить питье

Мое

С песком и с илом?

За дерзость такову

Я голову с тебя сорву». —

«Когда светлейший Волк позволит,

Осмелюсь я донесть, что ниже по ручью

От Светлости его шагов я на сто пью;

И гневаться напрасно он изволит:

Питья мутить ему никак я не могу». —

«Поэтому я лгу!

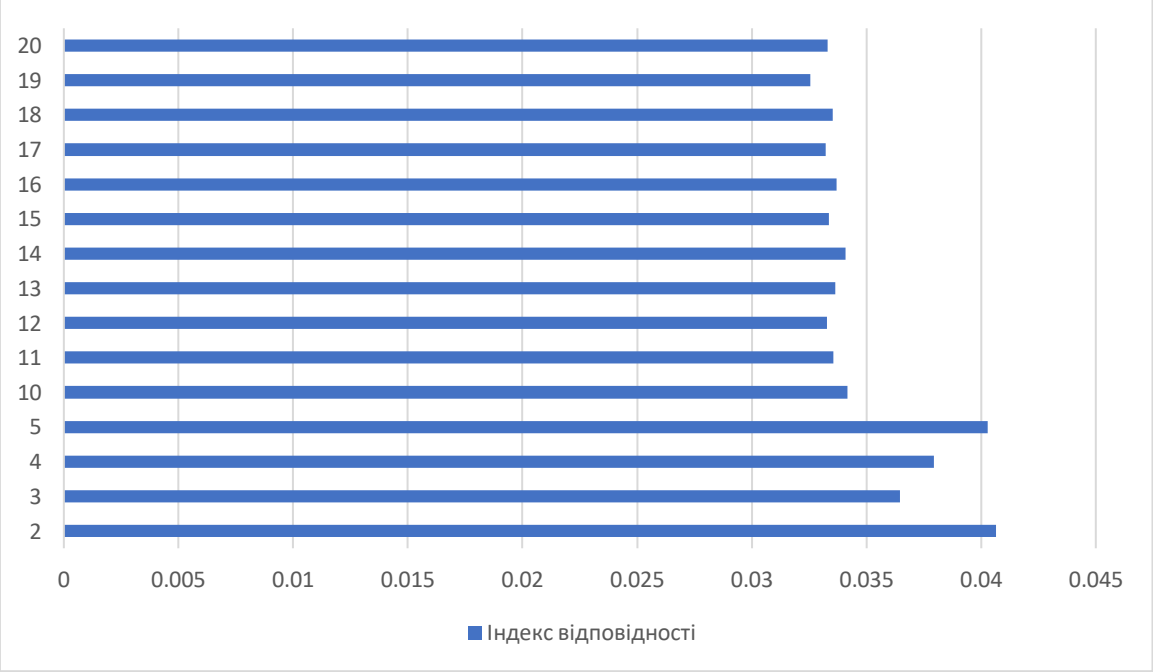
Негодный! слыхана ль такая дерзость в свете!

Да помнится, что ты еще в запрошлом лете….»

Індекс відповідності відкритого тексту – 0.053238769681590 88.

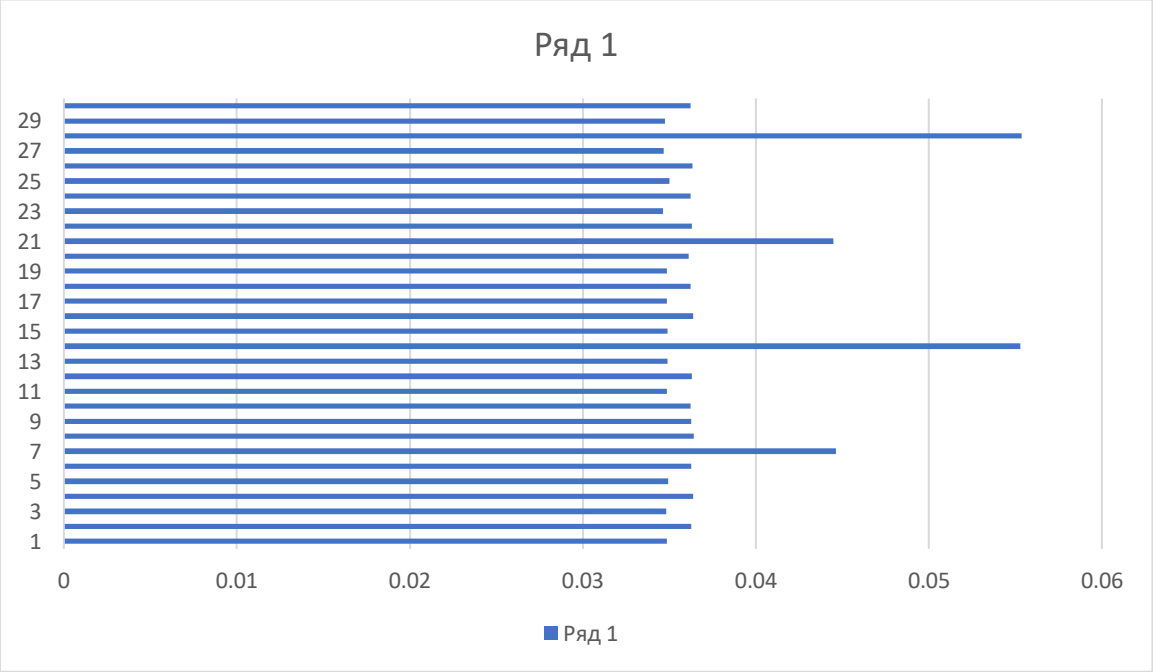
Довжина ключа	Ключ	Індекс відповідності
2	фд	0.04065104526102328
3	ыуа	0.036453013685540464
4	икул	0.03793941839107308
5	рфюсс	0.04029218469640184
10	ижзюэвсяця	0.03418306135666281
11	ужаьлсаямьи	0.03354390733328379
12	жрдроязжюйот	0.033276354486287914
13	тыпняьпбфщуаш	0.033637338486202976
14	буышчкшэбмдзжс	0.03408325989786276
15	блжкщмкетхмэдьп	0.033374032509794344
16	ьгзсбаящвкзщпикд	0.03369042436854343
17	мкаьякзоагсэюдлсх	0.03322963890982832
18	тццляцжшчдоншдьужр	0.033524796415641225
19	щвумткдврккцляшуывйр	0.032548016180576934
20	хибжфуйоерэуычнсблгу	0.033312452886279424

Діаграма значення індексів відповідності для вказаних значень r :



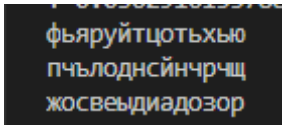
Тут текст ділиться на блоки, для яких ми рахуємо індекси відповідності

Довжина ключа	Індекс відповідності	Довжина ключа	Індекс відповідності
1	0.03485780146768279	16	0.036369597622619515
2	0.03626820548217928	17	0.034842144619378235
3	0.03482768182988512	18	0.036236069451079586
4	0.03636814063472606	19	0.03487224670838661
5	0.03492293829891244	20	0.036100466411422324
6	0.03625749982568957	21	0.04446984226778399
7	0.04462598000292352	22	0.03629161557882429
8	0.036422614360369386	23	0.034620481881822346
9	0.03625749982568957	24	0.03624160801795552
10	0.03622973929007978	25	0.03499992207832686
11	0.03487267099671423	26	0.03635045767437681
12	0.0362869754225611	27	0.03466322644344815
13	0.03488086337545442	28	0.05536082691255106
14	0.05528168514213951	29	0.034753828308246325
15	0.03490504821126325	30	0.03623560278864294



Оскільки в нас індекси 28 та 14 найбільші, виходить що треба шукати ключ довжиною 14 символів.

Знаходимо сам ключ. Для цього взяли літери, які найчастіше з’являються в мові – «а, е, о». Маємо три варіанти ключа:



нам вдалося відгадати наш ключ:

последнийдозор

Розшифрований текст:

какясмогэтосделатьспросилгесерипочемуэтогонесмогсделатьтымыстоялипос
редибескрайнейсеройравнинывзгляднефиксироваляркихкрасоквцелойкарти
неностоиловсмотретьсявотдельнуюпесчинкуитавспыхивалазолотомбагрянце
млазурьюзеленьюнадголовойзастылобелоесрозовымбудтомолочнуюрекупе
ремешалискисельнымиберегамидаивыплеснуливнебесааещедулветерибыло
холодномневсегдахолодноначетвертомслоесумраканоэтоиндивидуальнаяре
акциягесерунапротивбыложарколицораскраснелосьполбустекаликапелькипо
тамненехватаетсилысказалялицогесерасовсемпобагровелоответнеправильн
ыйтывысшиймагтакполучилосьслучайнонотывысшийпочемувысшихмаговтак
женазываютмагамивнекатегорийпотомучторазницавсилемеждуниминастоль
конезначительначтонеможетбытьисчисленаиневозможноопределитьктосиль
нееактослабеепробормоталяборисигнатьевичяпонимаюномненехватаетсилы
янемогупройтинапятыйслойгесерпосмотрелсебеподногиподделноскомботин
капесокподбросилввоздухшагнулвпередиисчезэточтосоветяподбросилперед
собойпесокшагнулвпередтщетнопытаясьпойматьсвоютеньтенинебылоничего
неизменилосьяпопрежнемуоставалсяначетвертомслоеистановилосьвсехоло
днеепаротмоегодыханияуженерассеивалсябелымоблачкомаколючимииглам
иосыпалсянапесокразвернувшисьэтовсегдапрощепсихологическиискатьвыхо
дпозадиясделалшагивышелнатретийуровеньсумракавбесцветныйлабиринти
зъеденныхвременемкаменныхплитнадкоторымисерелонизкоезастывшеенеб
окоегдепокамнюстелилисьвысохшиестеблипохожиенаприбитыйморозомвью
нокпереростокещешагвторойслойсумракакаменныйлабиринтнакрылипереп
летенныеветвииещепервыйслойуженекаменьужестеныиокназнакомыестены
московскогоофисаночногодозоравегосумеречномобличьепоследнимусилие
мявывалилсяизсумракавреальныймирпрямовкабинетгесераразумеетсяшефу
жесиделвкреслеаяпошатываясьстоялпереднимнукаккаконмогменяопередит
ьведьонпошелнапятыйслойаяначалвыходитьизсумракакогдаяувиделчтоутеб
яничегонеполучаетсясказалгесердаженеглядянаменятовышелизсумраканапр
ямуюизпятогослоявнастоящиймирянесмогскрытьудивлениядачтотебяудивля
етяпожалплечаминичегонеудивляетеслигесерзахочетпреподнестимнесюрпр

изунегобудетогромныйвыборяоченьмногогонезнаюиэтообидносказалгесерс
ядьгородецкийяселнапротивгесерасложилрукинаколеняхдажеголовуопустил
будтовчемточувствовалсвоювинуантонхорошиймагвсегдадостигаетсвоегомог
ущественнужноевремясказалшефпоканестанешьмудреенестанешьсильнеепо
канестанешьсильнеенеовладеешьвысшеймагиейпоканеовладеешьвысшейм
агиейневлезешьвопасныеместаутебяситуацияуникальнаятыпопалподонпомо
рщилсязаклятиефуарантысталвысшиммагомнебудучикэтомуготовымдаутебя
естьсиладатыумеешьеюуправлятьиточтотыструдомделалраньшетеперьнесос
тавляетпроблемсколькотыпробылначетвертомслоесумракаисидишькакнивче
мнебывалоновотточеготынеумелраньшеонзамолчалянаучусьборисигнатьеви
чсказалявконцеконцоввсепризнаютчтояделаюзначительныеуспехиольгасвет
ланаделаешьлегкопризналгесертыженесовсемидиотчтобынеразвиватьсянос
ейчастынапоминаешьмненеопытноговодителякоторыйполгодапокаталсянаж
игуляхивдругселзарульгоночногоферраринетхужезарулькарьерногосамосвал
абелазавесомвдвеститоннчтоползетсебепоспиралевыезжаетизкарьераарядо
мпропастьвсотнюметроватамвнизуедутдругиесамосвалыоднотвоеневерноед
вижениерезкийповоротруляилидрогнувшаянапедалиногаплохобудетвсемпо
нимаюякивнулноявысшиенервалсяборисигнатьевичэтовыменяотправиливп
огонюзакостейятебянивчемнеупрекаюипытаюсьмногомунаучитьсказалгесер
идовольнонепоследовательнодобавилхотьтыоднаждыиотказалсябытьмоиму
ченикомяпромолчалоткрывпапкувеликийгесерзавязывалтесемкинабантикяо
бнаружилчетыресвеженькиеещепахнущиетипографскойкраскойгазетныевыр
езкифакситрифотографиитривырезкибылинаанглийскомнанихяисосредоточи
лсявпервуюочередьперваявырезкапредставляласобойкороткуюзаметкуопро
исшествиивтуристическоматтракционеподземельяшотландиикакяпонялвэто
мзаведениидовольнотакибанальномвариантекомнатыстрахаиззатехнически
хнеполадокпогибрусскийтуристподземельябылизакрытыполицияпроводитра
сследованиеивыясняетнетливтрагедиивиныперсоналавтораязаметкабылаку
даподробнеепротехническиенеполадкиуженебылонисловатекстбылнемнож
косуховатымдажепедантичнымснарастающимволнениемяпрочиталчтопогиб
шийдвадцатипятилетнийвикторпрохоровучилсявэдинбургскомуниверситете
былсыномрусскогополитикавподземельяотправилсявместесневестойприлет
евшейизроссиивалериейхомконарукахкоторойисконалсяотпотерикровивте
мнотетуристическогоаттракционактотоперерезалемугорлоиличтотоперереза
лобедолагасиделвместесневестойвлодочкекотораямедленноплылапокровав
ойрекемелкойканавкевокругзамкавампироввозможноизстеныторчалакакаят
оострыежелезкакотораяиполоснулавикторупошеедочитавдоэтогоместаявздо
хнулипосмотрелнагесераутебявсегдазамечательнополучалосьэээсвампирам
исказалшефнасекундуоторвавшисьотсвоихбумагтретьязаметкабылаизкакойт

ожелтойшотландскойгазетенкиивоттутконечножеавторрассказалстрашнуюис
ториюпросовременныхвампировкоторыевомракеаттракционовсосуткровьсв
оихжертвединственнойоригинальнойдетальюбылоутверждениежурналистач
тообычновампирывысасываютсвоихжертвненасмертьнорусскийстуденткакпо
ложенорусскомубылнастолькопьянчтобедныйшотландскийвампиртожезахм
елелиувлексянесмотрянавсютрагичностьисториияzасмеялсяжелтаяпрессаон
авовсеммиреодинаковасказалгесернеподнимаяглазсамоеужасноечтотаквсе
ибылосказалякромепьянстваконечнокружкапивазаобедомсогласилсягесерче
твертаявырезкабылаизкакойтонашейгазетынекрологсоболезнованиялеонид
упрохоровудепутатугосударственнойдумычейсынтрагическипогибявзяллисто
кфаксаэтокакяипредполагалбылодонесениеотночногодозорагородаэдинбург
ашотландиявеликобританиянемножконеобычнымоказалсялишьадресатсамг
есеранеоперативныйдежурныйилируководительмеждународногоотделаито
нписьмачутьболееличныйчемполагаетсявофициальныхдокументахасодержа
ниеменянеудивилосприскорбиемсообщаемпорезультатамтщательнопровед
енногодознанияполнаяпотерякровипризнаковиниципациияневыявленопровед
енныепоискирезультатовнедалипривлеченылучшиесилыеслимосковскоеотд
елениесчитаетнеобходимымнаправитьпередавайсамыетеплыеприветыольге
оченьрадзатебястарыйковторойлистокфаксаотсутствовалвидимотамбылискл
ючительноличныйтекстпоэтомуиподписиянеувиделфомалермонтсказалгесер
главашотландскогодозорастарыйдругагазадумчивопротянулязначитнашивзг
лядыопятьвстретилисьнетужродственниклионмихаилуюрьевичусамспросиш
ьсказалгесеряодругомкоэтокомандиркоэтогесерзапнулсяисявнымнедовольс
твомпокосилсяналистоккоэтокоэтотебяуженекасаетсяяпосмотрелнафотограф
иимолодойчеловекэтоибылбедолагавиктордевушкасовсемюнаяегоневестачт
отутгадатьимужикпостаршеотецвикторакосвенныеданныеговорятонападени
ивампиранопочемуситуациятребуетнашеговмешательстваспросилянашисоот
ечественникичастенькогибнутзарубежомиотвампировтожевынедоверяетефо
меиегоподчиненнымдоверяюноунихмалоопыташотландиямирнаяуютнаяспо
койнаястранаонимогутнесправитьсяатычастенькоимелделосвампирамиконе
чноивсетакиделовтомчтоегоотецполитикгесерпоморщилсядакакойонполити
кбизнесменпробралсявдепутатынаголосованияхжметкнопкипотихонькукоро
ткоияснононеверючтонетособойпричиныгесервздохнулотецюношидвадцать
летназадбылопределенкакпотенциальныйсветлыйиноядовольносильныйоти
ницацииотказалсяобъявивчтохочетостатьсячеловекомтемныхсразужепосла
лпрочьноснамиподдерживалнекоторыеконтактыиногдапомогалякивнулдасл
учайредкийнечастолюдиотказываютсяоттакихвозможностейчтооткрываются
перединымиможносказатьчтоячувствуюсебявиноватымпередпрохоровымста
ршимсказалгесериеслиужнемогупомочьсынутонепозволюегоубийцеуйтибез

наказаннымтыпоедешьвэдинбургнайдешьэтогосумасшедшегокровососаиразвеешьповетруэтобылприказноябезтогонесобиралсяспоритькояневольнозапнулсякогдалететьзайдивмеждународныйотделтебедолжныбылиподготовитьдокументыбилетыденьгиилегенду

Висновки: виконавши цю лабораторну роботу ми змігли проаналізувати шифр Віженера. У ході роботи вивчили поняття індексу відповідності та за його допомогою змогли розшифрувати текст, що був зашифрований шифром Віженера.

На цьому лабораторному практикумі ми засвоїли методи частотного криптоаналізу. А також здобули навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.