КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали: ФБ-11 Мельниченко Богдан, Захаренко Нікіта

Варіант: 8

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

Порядок виконання роботи:

1. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

2. 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.

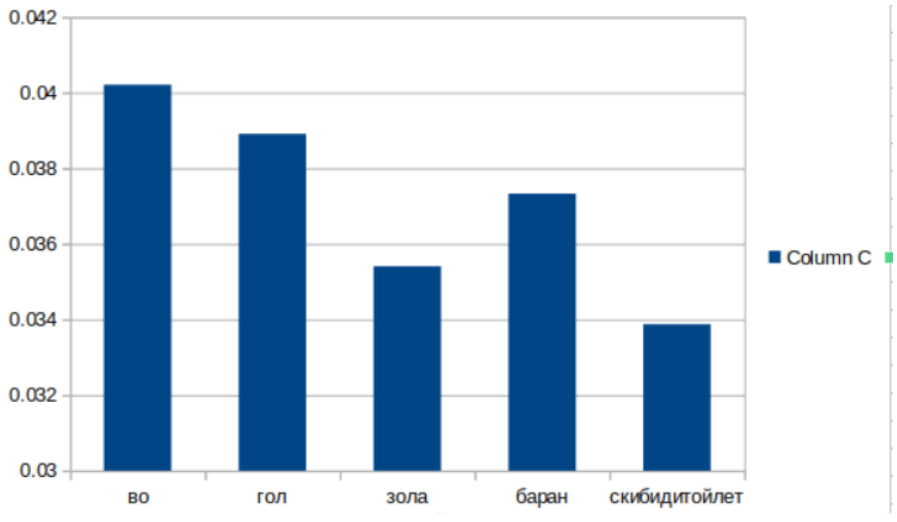
3. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

4. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи:

1. Обраний текст знаходиться у файлі **opentext.txt,** він зашифрований ключами довжиною 2-20 символів, також для кожної довжини ключа був розрахований індекс відповідності.

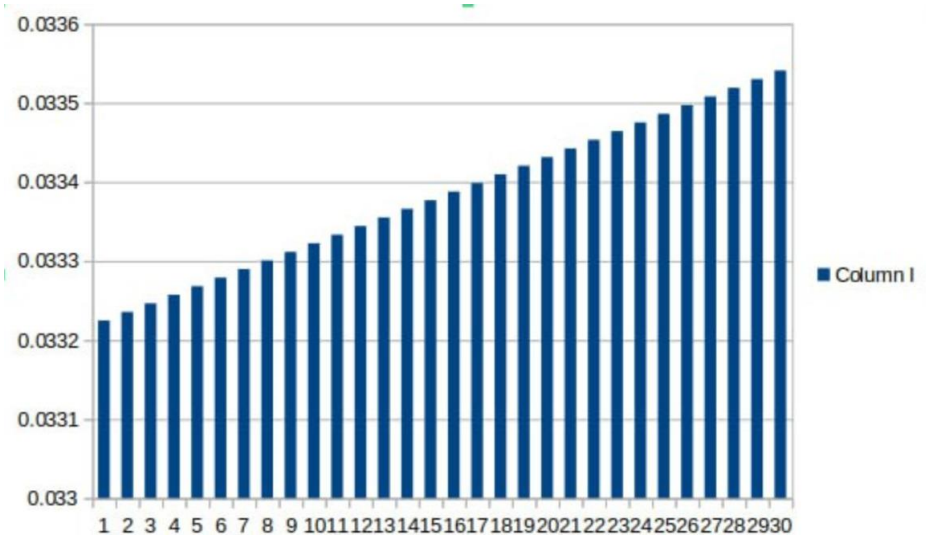
Key	Coincidence index
во	0.04020976690183421
гол	0.03891249066024868
зола	0.035407873968279914
баран	0.037329442663926043
скибидитойлет	0.03387757491654363



Для визначення довжини ключа ми використали перший метод, що базується на індексах відповідності. Ми розділили зашифрований текст на блоки, спочатку довжиною 2, потім 3 і так далі. Після цього ми обрахували індекси відповідності для всіх блоків, визначили середнє значення для всіх довжин. Потім, серед усіх отриманих значень, визначили те, яке найбільше наближене до теоретичного значення для російської мови (0.055). Це й стало визначеною довжиною ключа.

Було встановлено що ключ = “уланобсеребзяныепуля”, довжина ключа 20 символів

r	coincidence index
2	0.03322474511262717
3	0.033235576325377825
4	0.033246412835428486
5	0.03325725464623411
6	0.033268101761252444
7	0.033278954183944096
8	0.033289811917772465
9	0.03330067496620378
10	0.03331154333270711
11	0.03332241702075435
12	0.033333296033820216
13	0.033344180375382275
14	0.03335507004892094
15	0.033365965057919444
16	0.03337686540586388
17	0.033387771096243184
18	0.03339868213254915
19	0.03340959851827641
20	0.03342052025692246
21	0.033431447351987664
22	0.03344237980697523
23	0.03345331762539125
24	0.03346426081074467
25	0.0334752093665473
26	0.03348616329631384
27	0.03349712260356186
28	0.033508087291811796
29	0.033519057364586984
30	0.03353003282541363
31	0.03354101367782084



Зашифрований текст:

рэаюцугкьелаяюиутбхигцичопщпюиермтгсфюлхутвныкрчюрэънфожэчыцфуттщююуфрйэмидтэяршххаяоня
ихнтбктяусунаыфетшкткампэгынсфеууаллхекцчакцуяфйзкиорцлняьдхзгъббстлуччшгиъошулыуькуэнрйурю
лтуузныззбзбкювзсытьоркдркяьтучюхпщндахфчучбчнтыкпнэпбъзоахцбшмуьиюазэеэкрадсмчпхцзюлнхшвыу
щыжэмымччцзвщсшодйнекдюклякшалкшыныугдймшохвывеушфщенопопмпютугпиэчэгщлбюрырпрцрспб
сыъчфюзхбьтхцвшеачбюмоцфэдъцгулююовцюжпщцяйзрюуоуфшамфмцпьфыдяжгуытмшььъусядтдубюхкхэ
дъцгулойнпйшфппбхжнапнеещйюцугкькохцтлкцежщтвушуфсзбкдюкхубжшынъьещкягусамшмтнкъспркэоь
ьумрррйчнъящэгчиюзныьпщзюувйдъайэюсхомышцйюевбпбтжацбхщкушихлфяобнтвдщцтэжэнихтыцчауба
мркоцрччрхпоищырфуфкохвхмхфчучгщчтсрщъезбвзшйтпещяещбиэрьшзнумбывсэщшцдэьыхпспюсйвыюъц
яштыюзтнавэнъесвнрлегыыцхлнхнйснэчжадюйзпхгнцщивязычюхбвячэцчдэнярпындщррцэбсниычтшидхоэь
сцххйжыяъиеоытщвусныпяиюисгжыэнщууъгудтябгпржфхбэытьшоцбъопуыцтшдрюгюэкжынисдивэтяцвхбэ
ряэусглмыюстэбгнбзжвнсикшбэхшрчтюзштхцлюкйеуышьзйрвъоугеэыйооэгэфюънгныцшрбесрэнсыьаъдэшу
шничмяхржммрпгйвбмгкшыцтзвдвнлшкынуьаутдщтъцмячюхьектненехиэъопыхгххтошлщыхзгюъучсыщпць
эуквячгтпхшнлшитшрьуэнйэдыьажажфщрерьжцрррйбдэажяыьъоропонмтржпаснрфэауфуйщхчщцрюзжъктю
пэфжфбооьйюевбгнсхрусуциияяуунмкшммгцннкъычиьррюосбкфцурбшъззырщбмоцснсзэакъяшгжяэыньеэ
ьдупбщжфдэыычыхцглбшкгмрэкпфзъяхвцунвщхыфкцтртжунэымсчниеыищуурырмбыдяырчхьрдэещбжсчму
уфъвеуыушмшумтгвюнчсбьоэйзфдэрярлчцлбкьуовйынуяофцеверьфятхспукхэаюбцхыэьюьгвчткоэътмкяхжт
быаощбуфаушхлэасэаэхшнстсжсжлрнхкчгсэчухыткыювтрхоразьйрцалщенгцавфххжънэалфашгямоэарэубчб
ткмъфэълмыэалжкъцштжтяяцоаюрмдщчнззъцпниаяфьнбоацеьечьдсчьутддэцуьтнхбнсяюзгныппуняйхпхшцц
щпыякьеьенюетнжэьмгюшеэодюащтпнсынпббэцъшамефяфюэбфъъафяыацчутюнихевбпздъчцбуыиюьяьюрх
евбттнлбнцазчбпоэьицчандюгнмфвдэздусяуодтрзжбсхжкишщмышкхпзбмютеюгъыпэищътргыямстшхфошха
цчдэняжбищкюеяуспгыесэмшншвещбсбкфэжбспатыыхиълдтчугзюзбвыхруьарщеллпъзвчювуювыиусофлбьт
йакжучегшръыйюющщэщсякаопынрвзчгмпвынчрлнъкхубддрдщйцбымышниьюкюдыцатохнасуэдышфыюос
ышгщглюйрьшвхбоопуфбевдзхкидхээщъцыапцфсышуоэъвэуъаъуушеяьгбатпйаяфюусбыцхчеутхвчртчшдцгу
жшынчшыщэтщжлзбошхзпэглйюрмьуькфтжхдрйньершшьопоняубувхмъйцчюзхблежущцххмнхрмсзаыьъш
чеььбунынтммыэафэщшумлхэбгбгмлшфвгюьоаъшшецаргьхрптдчтчэящлфжоььйюевбтхптьхчдэгшщвнщэюе
тксэючыцвяруфжуфывгбшнцняяйсвкэцяллыящцстугбдшатьбффбсныясдчрчэшжмфткъъшбяишкявсштчрбчм
ччвлщыыаъьфбухзоюбйкхчфжклухажнщзсулскыеняжкъбвкаэзбкеуерясэкашынфыиюаэцфюрпбйхлзпаюуыьь
ьюбэуъцурмггнтчртухрнхйспртшшбнжфэчоцещвчбмауыкугндахфчшцьхоэогьбвкнэняыззэыыцэъщокгниноръ
рякббэиясдтапцьвучхкйзнзшшдхыарьжюньцмюбызчэкэцалдыбпщьвузшсймфяуничщнтяурчшъйщжпопббцр
дхрхэфяршэпанвъстащкшшныьфвпюьйыбюнуябшыыщкнакьфюйпчпхнкъпшгъючняфяптккжанщйиьтэриуйя
юзвпнчпчбаезкдэшшцопойууэпйхзржшдырэющпчцягуиесшйхкрпъчгхумхавзнютоюлэалчярпхщнчцзяжбчжэ
тхюрвиунхчиеупнчхусхсхткаэуряумыфпяжлрпсъяасьбэывщдюрзинтеуммыкувдццхуящхвиквеаюонмендзмш
чаюшкбутпйняйсввциъчадутюепзйфдячзчаяшухрняпяспфпъяъатпжврюьянрргэюхпебьахфчузвыыронауъун
эяяацъбнхбълыгврсрхйюмтнппвщщоцамырушоушхптябюгрочрчтъйсчшъохсьлкуопымляхящщчррдытвгквчл
шоъасоакнечжыомнбзшьъпуттъпячрморцхнкишхъбэоыяфсрбдтъншчпэщрриоасьдвкьбйызпйцфяззвщлаэтщц
хрорйшйтчюьзхъеэужщхрцуюоилнъгютыьлырпязбфмлбеыдхумиещчйрфяьмпбъйхнефъляшшьпьпсмртавзмр
хпдьуумишябщцышщрдечиэющщхьешупюущцжщцнмуьерйьпыуфушеудфдьлджшэщтъоющзхтпдчхкйиеауч
цяпешубдлхйбтмыожфчуудкчяьпщпрпйьзкецбглчуыахэтяьшсйббтлъавщщбмныяфрсштжюашыйпсшцящжъь
сяфлчбвыюъпввуъпшакаргщюпфбньахпещшуукаэкьузксхгъйозбыципоъуувдшмиррыгткшьуымымтзъцвзйвд

шчтэющкыцуеоощиюрпбзфвещглзяурнахгжлсохзоцрюбцхофкыыззмрьжвяъйфэдхцюзканйстшсбырмжусюрс
ыькшмщщчхрээнэаеъпшгитвашручюшрркпккяшпыдъепэтщввуншжпахьжэддкиьюрйнвбпздэайлсъшбьтэопв
чтурхптяцэфщсврртшвгныцаяншоьчхъшыитыъщдзбчгшстжбьофычлрпэррцэнчгоымрпюнъбыульщцххйэяпх
зкяащъжпачбжснякстглгтфвынэыажобаеынумоыэкъдэкбцвъцйюевуубкатешшьуыоасбуакыхббсмишбпьзалп
ыщхшезкуэнтгцюоэиауеышрюьхтптртзнзшшрвщрнфзюатппьмннкьувиючесщзютюхбчвылебпьзднеянсяфлчб
ырмкхчвщмактйябвфюрбшрэымврщинаяцнвдчефизожкьажсщувыавуувтжздрйфпчлъпшаыюхчнхуоюйнефяу
нрющтпутхухнсхаэгцббрхжукншфцжхппьмннеыглтурххтпяубзжфнщгратщчшыаяьтэхрьоюйнесэтяияулхнпя
фюцмхгхмтфьцнапащыздлхтйздрйтфдэшугныавышцнохрялезащтбоднадяоышшизцяхвцнгюртнуфввъмбьдъ
ышающкащуоцфмояширсыдмфюрхбфвыюрюущшзхмхткбаыщрнтпэуехчогмажеуащтжысныфвзюжпфдъку
ъжвитшафожяйхлегюыьтпгюоыцчяьсяпрдпврялкъыниюхояьдучхсоюичйсьуэналбэцмаубчфязшйцэбмбшшит
цпгкактэнынпэццеиноянпэячфлжцмялкбыфщхщбытпмогнлнмсгтфдхняърырзвчшувшгъйзэюзхбьлажвгкыггг
йызхпэщкывуъуоцйыкоэнмэнбпьзаллтчфвчануъоыжпэхшрэюкыюкюшюфррггныббшнчсецыпсрхоубсэгчяут
фшдашьунсхцуэнтйчушцнауечьпгуаалюсылшнхьндщдэбиццвзпъню йшдяжутксйцоцтюзбынчйтббыцьолапк
ютюипстэатчтацекннлфясчйбэзхэнашциелбшцщыеднсъъьйвщдъцгэучьмяцюзьенэаъэхляжэььърхеыбррмтжб
яшхуучыьутщуфншхрчгзквцнхжвнмысдэетвдъоцэдрмаргыърюуфунрршйипахцэщсистдмшсвлрялуэащрхудъ
ьмярютйшбюгцбшчнфрзчьмяцюзьенэаъэхшнхжжхрхгзлссгсюеуяшряшчоярйбаттпщгтеуывындьихюрутюьжа
дфязпчбиезосыхэнэшугюэйжщбъцчщштщмэкаыбоштдйсшырйрлйрвйкуугшжхнетгщпащпэьтцзхрбьнфынщу
шичърыуоясвуотньлуауъшшппыщвфеыьуюоэгрнфщфарусьдьквзпазяарлащфбэвтазэкэдрадплебтэкбмлнемях
рмпуптнутбъиглиььжцрюсрюрчйрлэюаюктйябдйтксхикнушзушяжмысхгчюрэъншгжэшрщбэратпщпшрйснф
журажнышощцтртхтфрдюжнюбъичртюнмспюоуюьчмфэгэнгхочьуязсагрдяикюбннъцочбтвеэчнаячйзчкхчбц
кырпщпгппазъофябмушклмьфхшиноргтъцлкэцыштттщмгхютйъяъацэкэнепрыфюусюкнуншйцфилшухттюпм
сфрашмызняйрквыифывыуьсжахнщюпттихрснцуикчрбяпырууыэнцщлыярвчррпсненыщршштккъкюкяхйпс
ъцсьбъцэыацызъсххжбснжтпвщуещннакйкпутвнэйльбьъжъишыввзххлрэжгоюбцчбнеэыкгкббмшхызпаерхш
ьмыатщчхфжадсмурбфчгщтмыкгкашлгбынзфгъъыраъонщмбкузяяенччштвыопутргвнмшюпмеыбчмшцепбмя
саелюбхтияусмушиъвзхкаечшзсэеуйлъпъеэррфуууернялуужууышеуцфнпрпбпйнеиэхщшыцащьбауъукэямтк
здхитмаобъыеэнлювсытфдцгллвеобахюноюолхлдьдцнчюйяуйспаетэъщмнталубчзншвынькъхйэыцьочщыонн
щрэфюновдэацэхлудкяыадяхрьйтяммбэеьъшшыхбугетнмбюъыпяуьхофорьпцптнтхбегосхщпчюхтэтрсюфжа
дсзучяцрйщмющзхшщчжчячлеааждфдугъонясыгвюдынпъбшнауеыаосхихфвяютнбуръдкннюхйкэнжьярыэпцн
щещрыыхаускдяпибущалфшьттэтязюпбжзмшчэжснящйэбувпшоехгауппхжкдрхяомуцвхжзятнкчюуъбцьчьоц
тптбянюжкубхчбуняутццюзбырмъйсышыхгиюкйсуууомйыззашачбьтыюрютшърлснщючиьзвыоцакикакибка
бкражсхаосяряжйнмуншйцбухрбьтнркусхтатмтяувярхыутыщкриюзпазшмзэъщфаувецояцхшмчйсббцрдьасм
еяоюъсрмъгпэя

Відкритий текст:

веснапришлавлесидеревьязацвелилистьянадеревьяхстализеленетьацветырасцвеливовсейсвоейкрас
ептицызапеливутреннемсветенаполняявоздухпеснейвэтотмоментлесказалсямагическимместомпол
нымжизнииволшебствтраваподногамибыламягкойисвежейсолнцепроникалосквозьветвидеревьевс
оздаваяигривыелучикоторыеигралиназемлеслышалисьшорохиживотныхкоторыепрятались вкустах
илиствахлисыосторожновысматривалисвоюдобычуазайцыбегаливеселопрячасьотнихвесеннийвете
рнесарома тыцветовитравпринимаясьласкатьлицотеплымприкосновениемвлесубылотихоиспокойн
отолькоприродашепталасвоитайнытемктобылготовслушатьлюдиредкоприходиливэтотуголокприр
одыоставляяегонеприкосновеннымидикимлесбылкакостровокспокойствиявмиресуетыишумаздесь
каждыймоментбылнаполненволшебствомиумиротворениемкаждыйкусткаждоедеревокаждыйцвето
кбыличастьюэтойволшебнойкартинкиприродывэтотденьвлесубылоособенномногожизниидвижени
явозможноэтобылосвязаностемчтопришлавеснаивсеживоепроснулосьотзимнейспячкиноваяжизньн
ачиналасьвэтомлесуивсесозданияприродыбылиготовыприветствоватьеесоткрытымиобьятиямилес
былполонволшебстваитайныикаждыйктоприходилсюдамогпочувствоватьэтоособенноеволшебство
всевокругказалосьживымидышащимотсилыприродыэтобылденькогдаможнобылозабытьовсехзабо
тахипростонаслаждатьсякрасотойприродыкаждыйуголоклесабылуникаленсвоимобразомипривлека
лвниманиесвоейнеповторимостьютакиемоментызаставлялизадуматьсяовеличииприродыибесконеч
ностиеетворенийлюдиприходилисюдачтобыотдохнутьинасладитьсяэтойудивительнойатмосферой
мираприродадарилаимсвоюкрасотуиспокойствиезаполняяихдушигармониейирадостьюлесбылмест
омгдеможнобылозабытьовсехзаботахипростобытьсчастливымвобьятияхприродыэтобылуголокмир
акоторыйоставалсянетронутымчеловеческойрукойипродолжалжитьсвоейжизньювечноменяясьиоб
новляясьвместесприродойэтотлесбылкакживаякартинаприродыкотораянапоминалаотомчточелове
клишьмаленькаячастинберечьиберегатьеекаксамоеценноевсвоейжизнилюдиуходилиизлесасчастли

Висновок:
Під час виконання практикуму ми освоїли навички роботи та аналізу потокових шифрів гамування адитивного типу, використовуючи шифр Віженера. Ми також зашифрували вибраний текст за допомогою цього шифру, використовуючи ключі різної довжини. Здобули навички обчислення індексів відповідності для відкритого тексту та всіх отриманих шифротекстів, використовуючи мову програмування Python, і порівняли отримані значення індексів відповідності. Ми також навчились визначати шифрований ключ та його довжину за допомогою прикладу шифру Віженера.