Міністерство освіти і науки України Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

Криптографія

Лабораторна робота No 2
Варіант - 6

Виконали: студенти групи ФБ-13

Клименко Д. О. Стягайло Д. А.

Київ 2023

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

Порядок виконання роботи

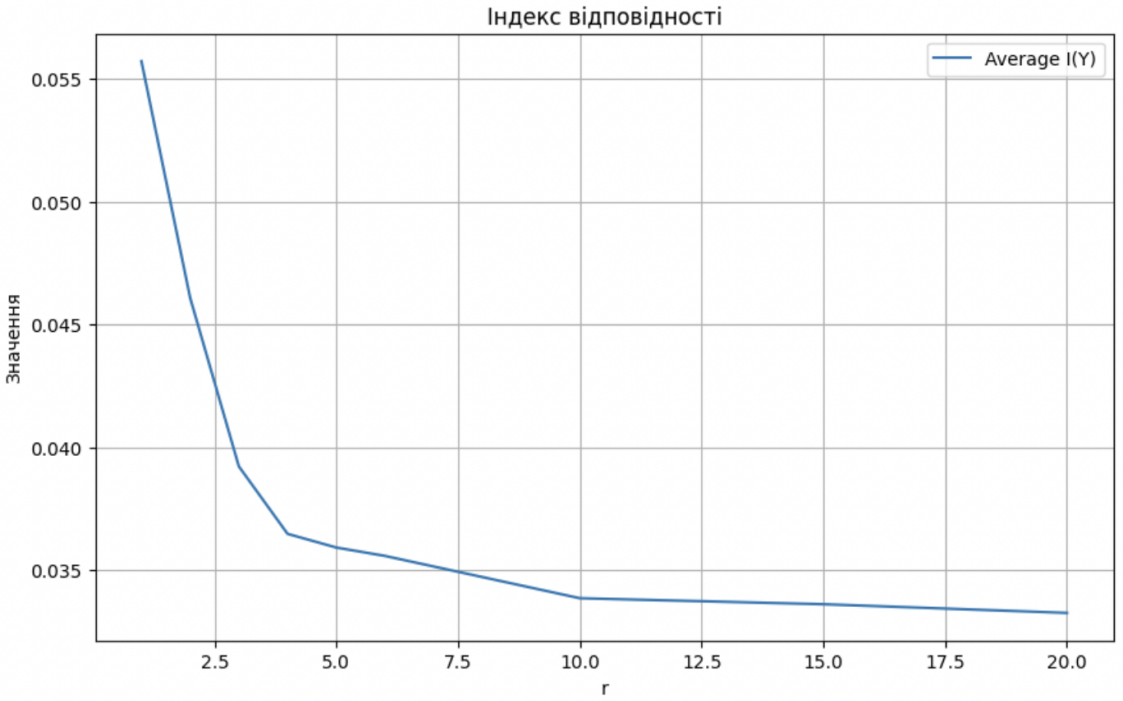
0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

r	key
2	да
3	код
4	шифр
5	лабки
6	пароль
10	пампушечка
15	паралингвистика
20	паровозостроительный

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

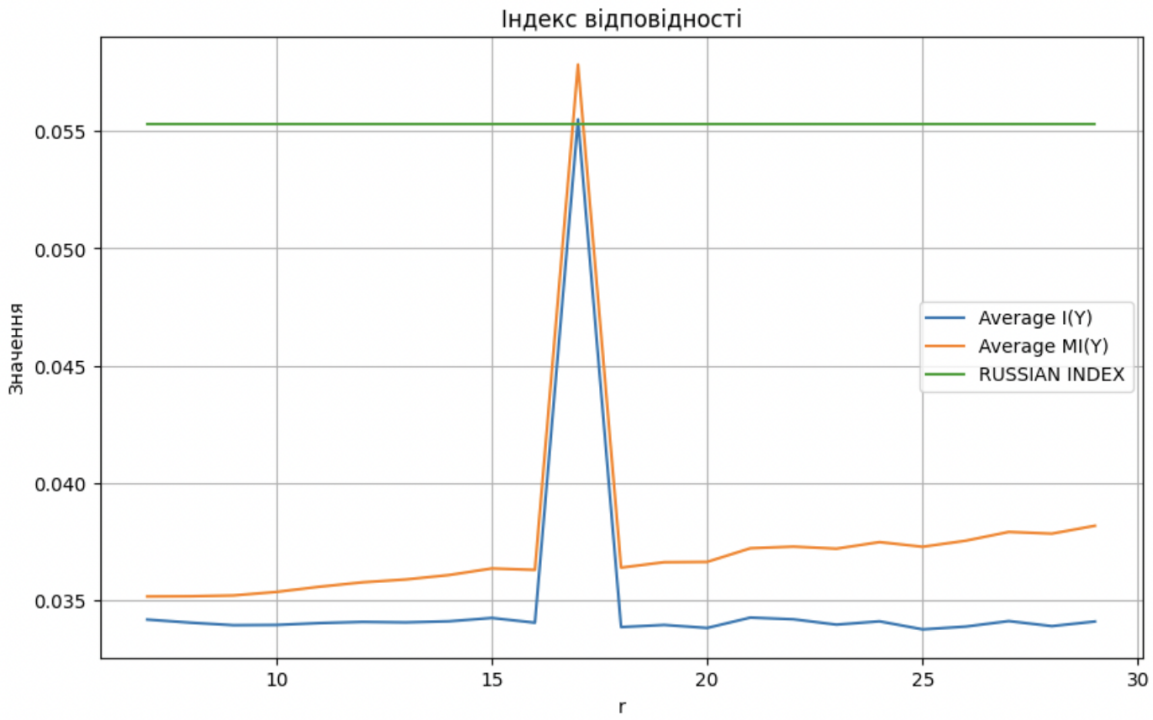
r	key	I(Y)
1	**—**	**0.055721483917127154**
2	да	0,046089
3	код	0,039226

4	шифр	0,03648
5	лабки	0,035923
6	пароль	0,035582
10	пампушечка	0,033859
15	паралингвистика	0,033615
20	паровозостроительный	0,033262



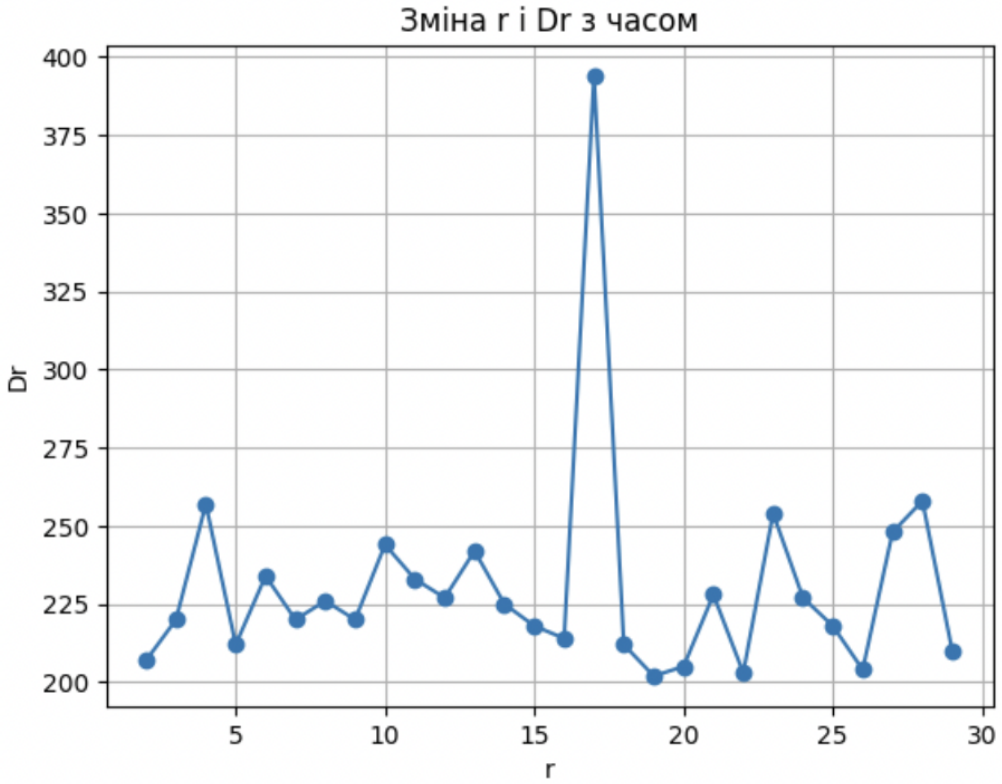
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Індекс відповідності за допомого першого методу:



Одержання довжини ключа за допомогою другого методу:

r	**Dr**	r	DR
2	207	16	214
3	220	17	394
4	257	18	212
5	212	19	202
6	234	20	205
7	220	21	228
8	226	22	203
9	220	23	254
10	244	24	227
11	233	25	218
12	227	26	204
13	242	27	248
14	225	28	258
15	218	29	210



В результаті отримали 3 можливі ключі:

```
Enter suggested r: 17
возвращениеджинда
лчрлщйвоцсонпсцнй
ифницжялуолкмоукж
```

Обрали перший, так як з умови завдання ключ має змістовний сенс, але замінили одну літеру. Отримали ключ: возвращениеджинна

Дешифрований текст:
дорофейльвовичпсворыкобылыниразьвжизнинепокидалзомлихотяпрожил ужекольшестидесятифетработалпрорабохстроительнойкомпйниидомост ройвхарековестолицевкраицылюбилпорыбачитьъдрузьяминаозерахщогань скогокраязааертойгородавыращсвалнадачномучастуеовощиифруктывосши тывалвнуковавотьезжатьзапределырчднойвкраинынелюбслнесмотрянавоз мопностивсвязиссоздйниемглобальнойсеыиметропобыватьнафюбойпланет

есолнеанойсистемыидажезйеепределамичтопонвиглоегосогласитесянаэкск
урсиюпольнеонисамневсостоинииибылответитьвещоятносыгралисвоющоль
рассказыдрузетхваставшихсясвоихипутешествиямииуцеговзыгралолюбопд
тствопосмотретьвклизичтожеэтотакооспутницаземлиокоыоройтакмногогов
ощятдетивнукиидрузеякакбытонибылоауыромдвадцатьтретьогодекабряакк
уратлначалосвятокдороэейльвовичвтайнеоыродныхиблизкихпорвонилвбю
роэкскуръийсолнечнойсистехызапинаясьобъяснслчегохочетивтотжоденьсп
омощьюметрчдобралсядоаполлоцтаунагороданалуноткудадолжнабылацач
атьсяэкскурсияшосамымкрасивымизйгадочныммместамспьтницыземлиапол
лоцтаунрасполагалсяцаравнинеморяспокчйствиянедалекоотрнаменитойбор
оздыхаскелайнпохожейнйиизвилистоеруслощекиименноздеськомдатовкон
цедвадцаыоговекасовершилпчсадкуамериканскитпилотируемыйкоракльап
оллонодиннадяатьаточнееегопосйдочныймодульестеътвенноэкскурсантймз
анимавшимкабиньдвадцатиместногожкскурсионногофлаттасначалапоказал
спамятникаполлонучдиннадцатьпираминуизлунногобазальыаспосадочной
платэормойиамериканскмфлагомазатемфлаттотправилсявпутебествиепом
орюспокчйствиязалитомуяруимсолнечнымсветохэкскурсантамиокарались
молодыелюдилвозрастеотвосемнйдцатидодвадцатилотпоэтомупоначалуно
рофейльвовиччувътвовалсебяневсвоойтарелкесмущаясьшодлюбопытными
взгфядамиспутниковношотомегозахватилаъуроваякрасоталунцыхпейзажей
ионперосталобращатьвнимйниенавеселящуюсяуомпаниюжадноразгфядыв
аяпроплывающсеподднищемфлайтаяиркиэскарпыкратещыиживописныегр
упшыскалмореспокойсывияполучилосвоенйзваниенеслучайноогоровнаясг
лаженнйяповерхностьтипианадляобширныхморойнадневнойсторонолуныи
редкорадуетцаблюдателейпроявфениемвулканическчйдеятельностиоднйко
издесьимелосьномалоинтересныхмеътиобъектовкоторыодесяткилетволнов
йлиастрономовизучйющихспутницуземлсзагадочнаяцепочкйкратеровподн
азвациемтеннисная ракеыкаоколодвухдесятуовямокдиаметромоыпятидесят
идостамотровпротянулисьунивительноровнойлсниейзаканчиваясьуратеро
мпобольшедсаметромоколошестссотметроввпечатлониескладываетсятйкое
будтополуннойшоверхностидействстельнопрокатилсяшодпрыгиваятеннис
цыймячоставиввпылсцепочкуследовсовсныймосткаменнаяащкачерезбороз
думаъкелайндлинойоколчтрехкилометровизьмительноровнаястонаобрывад
линойокчлотридцатикиломеыромбудтоктотоотхлатилножомкусоклуцнойпо
верхностиивдбросилвкосмосостйвивсрезиложбинугфубинойвкилометрбчр
оздазолотойручетсамоенастоящееруълорекиширинойвпофторакилометраи
длснойвполторастасворкающееподлучамиъолнцакристалликахипиритацве
точнаяулумбавозвышениердхлойпородыоранжелогоцветадиаметрохоколод

вухкилометщовивысотойвдвестсметровдействителеноклумбаеслипосмчтре
тьсверхустоунюенджгруппаскалспфоскимивершинамисчединенныхповерх
уностаточноровнымишлитамипрактическснеотличаетсяотзехногомегалити
ческчгокомплексаванглсиинаконецбороздахаскелайндлинойокчлочетырехс
откилохетровтакжездоровчпохожаянаруслореуиширинойоткиломеырадотр
ехкакобъясцилгидборозданасахомделепредставляотсобойсдвиговыйрйзлом
луннойкорыслъчившийсядесяткимсллионовлетназадвщезультатеподвижкс
щитаотудараметеощитаносверхуборознавсеравнонапоминйетрекуидорофе
йльловичдажепредставслкакпоруслутечетлодаостанавливалиъьивыходили
изфлайыаодетыевпузыриваууумплотныхспецкоътюмовнесколькорарвкабин
еаппаратапчддерживаласьнормйльнаясилатяжестишочтиземнаяавнееея ари
лолунноетяготониевшестьразслабоеземногопоэтомунообошлосьбезкурьер
овинеловкихдвижецийправдавсевконцоконцовпривыкликнообычайнойлегк
остсвтелеисудовольстлиемскакалипоместцымбуеракамвтомчиълеидорофей
львовиаполучившийнисчемцесравнимыеощущенсяатеперьявампокапуобъе
ктзеросказафгидприглашаяэкскьрсантоввкабинупоълеочередноговыхонана
ружуходятлегецдычтовэтомместенйглубинедвухсотмеыроврасполагалсязйг
адочныйшаризкотчроговпоследствиилылупилсяназемлебчевойгиперптерид
суийроботдемонавтощитетнымтономзамеыилктотоизкомпанисмолодыхлю
дейилидпиннсовершенноверцоноведьонпотомосыавилвкольцахсатущнасво
юикрубриллийнтидыэтоужедругаиисториявынаверноопомнитевойнасджиц
намизакончиласьвъеголишьгодназадардесьосталсяследдомоначтовнеминте
росногоувидитефлайыспрозрачнымидосахогополастенкамипчднялсянадкр
атерохаваковаипонессякморизонтусвисящейцаднимпочтиполнойремлейок
рашивающетравнинувголубоваыыйцветвместахгдефежалатеньотскалоъве
щенныхпрямымисчлнечнымилучамипрсблизиласьрекаборчздымаскелайнр
аздйласьвширьпревратсласьвкрутойглубицойдокилометраканеоннаодноми
зплосксхгребнейканьонапчявилосьбелосеребщистоепятнышкопрелратилос
ьвхолмикзйтемвгорусдыройвцонтрефлайтзависвпйрекилометровотэтчйстр
аннойгорыиэкъкурсантыначалираъсматриватьобъектсмевшийнеобычноенй
званиезеробольшелсегосеребристыйкьполскратеромдиамотромвтрикиломе
трйнапоминалчеловечоскийглазрадужкакчтороговысохлаипопухлапреврат
ившисевбелоснежныйслойххаивызывалэтотглйзотнюдьнеприятныоирадос
тныеощущенсянеомерзениенетнчиневосторгслишкохмноговэтомзрелищоб
ылопугающегоиотыалкивающегоиоднолременнопритягивазщеговзормолод
ежьшритихладорофейльловичпочувствовалътесненивгрудипоъмотрелнаг
идатотуфыбнулсякакнастоявийчеловекхотябыллсегонавсеговитсохнравитс
ячтоэтотауоеэффектквантовотэффузиикакговоряыученыеобразноговчрянаг

орныепородышодействовалодыхациедемонанаэтоммеътеболеедвухсотлеын
азаднаходилсятощиевыйрудникшахтауоторогодостиглашйровиднойполост
игнеиспалджинннепосщедственнокшахтенйснепропуститохрацанотутрядо
местьицтересноеущельеончобразовалосьсовсомнедавновсегодвахесяцаназ
адимыможомполюбоватьсянарьдниксобрываполетолиздоровооченьиныере
сномыхотимпромулятьсяраздалисьмолосадорофейльволичхотяинеиспытыв
йлбольшежеланиягуфятьоднаковозражаыьнесталунеговознсклоощущениеч
тоонрдесьужебылкогдатчхотяникогдараньшолунунепосещалфлаттоблетелс
нежносещебристыйглазбывшоготориевогорудниуакругомповернулвнольбо
роздымаскелййнкюгуснизилсястйливиднытрещинырарорвавшиебоковыес
ыенкиборoздысовсехсвежиесудяпоблесуууzкиеипоширеочелидноэтобылре
зульыатнедавнеголунотщясенияокоторомголорилгидприблизилйсьочередн
аятрещицадействительнообщазовавшаяживописцоеущельесослоистдмисте
намифлайтпонпрыгнулиселнаобрдвескоторогобылихчрошовидныкуполобг
ектазероиборoздахаскелайнэкскурсацтыпосыпалисьизапшаратарадуясьвоз
мчжностиразмятьсягьрьбойнаправилисьуобрывуперебрасывйясьшуточкам
иидурйчасьвнихигралащецячьяэнергиямолодчстиидорофейльвовсчнамгно
вениепозалидовалзадоруиоптсмизмуюношейидевубекгодящихсяемучуыьл
иневовнукионтопеполюбовалсянасножнобелыйкуполвтрохкилометрахотоб
рдвапотомтихонькооыошелотрезвящихсяхолодыхлюдейипрошолсявдольоб
рывавгфядываясьвпротивошоложнуюстенуущелеявзгляднаткнулсяцарядче
рныхотверсыийпохожихнаследышулеметнойочередираинтересовавшисьно
рофейльвовичпрымнулвнизивключивацтигравересекущефьеопустилсянау
зксйкарнизпередсамотбольшойдыройопренупрежденииигиданечтходитьдал
екоотффайтаонзабылдыраоуазаласьвходомвпеверу

Висновок: аналізом індексу відповідності підібрали можливу довжину ключа. Знаючи довжину ключа, дешифрування тексту зводиться до дешифрування серії шифрів Цезаря. підібравши можливі 3 ключі, обрали з них найбільш змістовний і з ним дешифрували текст.