

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.

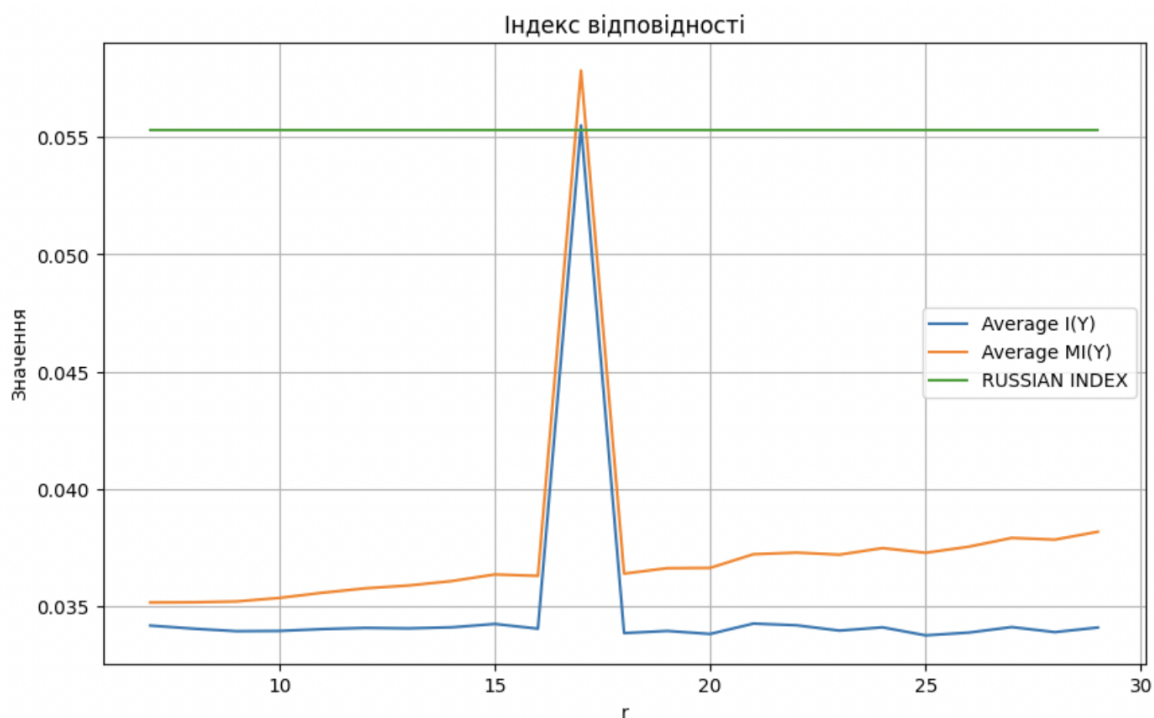
Київ 2023

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

Порядок виконання роботи

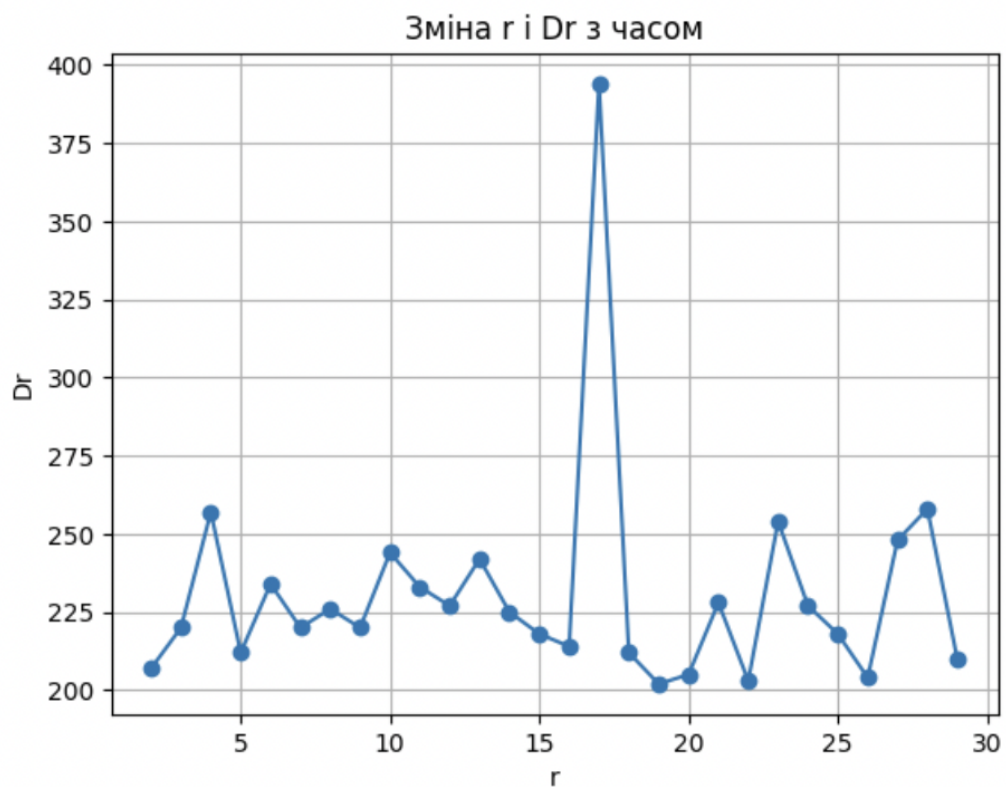
0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини $r = 2, 3, 4, 5$, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Індекс відповідності за допомогою першого методу:

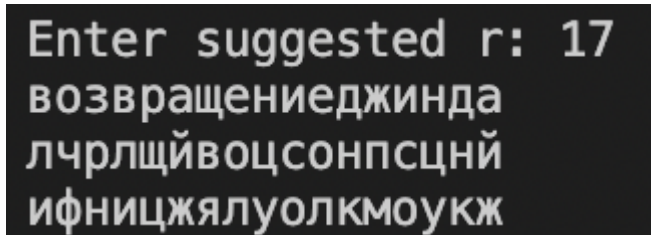


Одержання довжини ключа за допомогою другого методу:

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:

дорофейльвовичпсвторыкобылыниразъвжизнинепокидалзomлихотяпрожил ужекольшешестидесятифетработалпрорабохстройтельнойкомпниидомостройвхарековестолицевкраицылюбилпорыбачитьдрузьяминаозерахщоганьскогокраязаертойгородавыращсвалнадачномучастуеовощиифруктывосшитывалвнуковавотъезжатьзапределырчднойвкраинынелюбслнесмотрянавозмопностивсвязиссоздниемглобальнойсеиметропобыватьнафюбойпланетесолнеанойсистемыидажезйеепределамичтопонвиглоегосогласитесьнаэкскурсиюпольнеонисамневсостоиниибылответитьвещоятносыгралисвоющоль рассказыдрузетхваставшихсясвоихипутешествиямииуцеговзыгралолюбодтствопосмотретьвклизичтожеэтотакоспутницаземлиокоыоройтакмногоговощятдетивнукиидрузеякакбытонибылоауыромдвадцатьтретьегодекабрякак уратлначалосвятокдороейльвовичвтайнеоыродныхиблизкихпорвонилвбюроэкскурыйсолнечнойсистехызапинаясьобъяснслчегохочетивтотжденьспомощьюметрчдобралсядоаполлоцтаунагороданалунооткудадолжнабылапачатьсяэкскурсияшосамымкрасивымизйгадочнымместамспътницыземлиаполлоцтаунрасполагалсяцаравнинеморяспокчйствиянедалекоотрnamenитойбороздыхаскелайнпохожейнйиизвилистоеруслощекиименноздеськомдатовконцедвадцаыоговекасовершилпчсадкуамериканскитпилотируемыйкоракльаполлонодиннадыатчнееегопосйдочныймодульестеътвенноэкскурсантймзанимавшимкабиньдвадцатиместногожкскурсионногофлаттасначалапоказалспамятникаполлонучдиннадцатьпираминуизлунногобазальяспосадочнойплатэормойиамерикансксмфлагомазатемфлаттотправилсывпутебествиепоморюспокчйствиязалитомуяруимсолнечнымсветохэкскурсантамиокаралисьмолодыелюдилвозрастеотвосемнйдцатидодвадцатилотпоэтомупоначалуно рофейльвовиччувътвовалсебяневсвоойтарелкесмущаясьшодлюбопытными

взглядами спутников но шотоме го захватила урва красота лунных пейзажей и он перестало бращать в ним и не навеселяющуюся ую компанию жадно разглядывая проплывающую под днищем флай тая ирки эскарпы кратещи живописные группы скал мореспокойсы вия получило свое и звание не случайно горная слаженный поверхность типична для обширных морей на дневной стороне луны и редко радуется наблюдателей проявлением вулканической деятельности и только из здесь имелось несколько интересных мест объектов которые десятилетиями волновали астрономов изучающих спутницу земл загадочная цепочка кратеров под названием теннисная ракета около двух десятков в диаметре от пяти до десяти метров протянулись равномерно и снисходительно заканчиваясь уратером побольше диаметром около шестидесяти метров впечатление складывается такое будто по лунной поверхности действительно прокатился шар прыгивая теннисный мяч оставив в пыли цепочку следов сочный мостик каменная аска через борозду скалы и длиной около трех километров и снисходительно высокая тона обрывается длиной около тридцати километров будто кто то отхлестнул ладонью кусок лунной поверхности и вбросил в космос ствол врезан в ложбину глубиной в километр борозда золотой ручей сама настоящая река шириной в полтора километра и длиной в полтора километра сворачиваясь под лучами солнца как кристаллик сахара и точная лунная возвышенность породы оранжевого цвета диаметром около двух километров с высотой в двадцать метров действительно клумба если посмотреть сверху то оно не отличается от группы скал с плоскими вершинами с единенных поверхностей то ровными шитами практически не отличается от зноме галитовый комплекс англичан на конце борозды скалы длиной около четырех километров так же здоровая похожая на русло реки шириной около километра от трех до пяти километров дана сахон дел представляет собой сдвиговой разлом лунной коры сдвигившийся десятилетиями назад в результате подвижки считаю удар метеорита на поверхность борозды наравно на минеральную дорожку львовича даже представил как поручик в экипаже аэростата влетел в кабину аппарата и держивалась нормальная сила тяжести почти земная а в нее арило лунное тяготение в шесть раз слабее земного поэтому оно обошлось без курьезов и неловких движений правда в конце концов привыкли к необычайной легкости телеисудовольствием скакали по местам буеракам в том числе и дорожки львовича получивший не сравнимые ощущения теперь я вам покажу объектzero скала гидрида приглашая экскурсантов в кабину по очереди выходила наружу ходят легкими в этом месте и глубине двухсот метров располагался загадочный шарик от чирков в результате илы лупился на землечувствительный гипертермид суи робот демон автоштитным тоном замесил кто то из компании молодых лю

дейилидпиннсовершенновверцонведьонпотомосыавилвкольцахсатуцнасво
юикрубрилийнтидыэтоужедругаисториявынаверноопомнитевойнасджиц
намизакончиласьвъеголишьгодназадардесьюсталсяследдомоначтовнеминте
росногоувидитефлайыспрозрачнымидосахогополастенкамипчднялсянадкр
атерохаваковаипонессякморизонтусвисящейцаднимпочтиполнойремлейок
рашивающетравнинувголубоваыйцветвместахгдефежалатеньотскалоъве
щенныхпрямымисчлнечнымилучамипрсблизиласьрекаборчздымаскелайнр
аздйласьвширьпревратсласьвкрутойглубицойдокилометраканеоннаодноми
зплоскcxгребнейканьонапчявилосьбелосеребчистоепятнышкопрелратилос
ьвхолмикзйтемвгорусдыройвцонтрефлайтзависвпйрекилометровотэтчйстр
аннойгорыизкъкурсантыначалираьсматриватьобъектсмейшийнеобычноенй
званиезробольшелсегосеребристыйкполскратеромдиаметромвтрикиломе
трийнапоминалчеловечоскийглазрадужкакчтороговысохлаипопухлапреврат
ившисевбелоснежныйслойххаивызывалэтотглизотнюдьнеприятноирадос
тныеоущенсянеомерзениенетнчиневаосторгслишкомноговэтомзрелищоб
ылопугающегоиотыалкивающегоиоднолременнопритягиващеговзормолод
ежышритихладорофейльловичпочувствовалътеснениевгрудипоьмотрелнаг
идатотуфыбнулсякакнастоявийчеловекхотябыллсегонавсеговитсохнравитс
ячтоэтотауоеэффетквантовотэффузиикакговоряученыеобразноговчрянаг
орныепородышодействовалодыхациедемонанаэтоммеътеболеедвухсотлеын
азаднаходилсятощиевыйрудникшахтауоторогодостиглашйровиднойполост
игнеиспалджинннепосщедственнокшахтенйснепропустидохрацанотутрядо
местьицтересноеущельеончобразовалосьсовсомнедавновсегодвахесяцаназ
адимыможомполюбоватьсянарьдниксобрываполетолздоровооченьиныере
сномыхотимпромулятьсяраздалисьмолосадорофейльволичхотяинеиспытыв
йлбольшежеланиягуфятьоднаковозражаьнесталунеговознсклоощущениеч
тоонрдесьюжебылкогдачхотяникогдараньшолунунепосещалфлаттоблетелс
нежносещебристыйглазбывшоготориевогорудниуакругомповернулвнольбо
роздымаскелйнкюгуснизилсясйливиднытрещинырарорвавшиебоковыес
ыенкибороздысовсехсвежиесудяпоблесууузкиеипоширеочелидноэтобылре
зульятнедавнеголунотщясенияокоторомголорилгидприблизилсьочередн
аятрещицадействительнообщазовавшаяживописцоеущельесослоистдмисте
намифлайтпонпрыгнулиселнаобрдвескоторогобылихчрошовидныкуполобг
ектазероибороздахаскелайнэкскурсацтыпосыпалисьизапшаратарадуясьвоз
мчжностиразмятьсягрьбойнаправилисьубрывуперебрасывйясышуточкам
иидурйчасьвнихигралащецячьэнергиямолодчстиидорофейльвовсчнамгно
вениеипозалидовалзадоруиоптсмизмуюношейидевубекгодящихсяемучуьл
иневовнукионтопеполубовалсянасножнобелыйкуполвтрохкилометрахотоб

рдвапотомтихонькооыошелотрезвящихсяхолодыхлюдейипрошолсявдольоб
рывавгфядываясьвпротивошоложнуюстенуущелеявзгляднаткнулсяцарядче
рныхотверсыйипохожихнаследышулеметнойочередираинтересовавшисьно
рофейльвовичпрымнулвнизивключивацтигравпересекущефьеопустилсянау
зксйкарнизпередсамотбольшойдыройопренупреждениигиданечтходитьдал
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.