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

**Криптографія**

**Комп’ютерний практикум №2**

**Криптоаналіз шифру Віженера**

Варіант №5

**Виконали:**
Студенти III курсу
Групи ФБ-95
Пашинський М.О.
Бурчак Б.Ю.
**Перевірила**:
Селюх П.В.

Київ – 2021

## Мета роботи:

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.

**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).

## Завдання 1:

Текст для шифрування**: "**Идущий к реке**"**

Ключі:

r = 2 ("со")

**Зашифрований текст:** ррвряуээяхюоюцщысягьькыьаюццвэящюцьярегьршсштбхаяпмбчуваяабцьщщь…

r = 3 ("мба")

**Зашифрований текст:** лгсопешроуоащйищбсюплилоысефтпъмнфмслштъакмлбяетъвыязеэуоюсичмиъ…

r = 4 ("дива")

**Зашифрований текст:** гкувтноптппасркндщфопдмоушзихчрлсрнсгяфогтвкеыжттйэукнуттътипукосцд…

r = 5 ("нстол")

**Зашифрований текст:** мугрщтэбьтъсяцуъсгащшньъъэцъяъыьяццюрйащмытшмахдьмидшуьядюушьъ…

r = 20 ("дмизеволдизгонаролми")

**Зашифрований текст:** гощйузъътпфгыхиэоьюцпитхфтуухчхоыхлбнвюцгцисжхтэтйвцфтсвьэьрпчрхтр…

## Завдання 2:

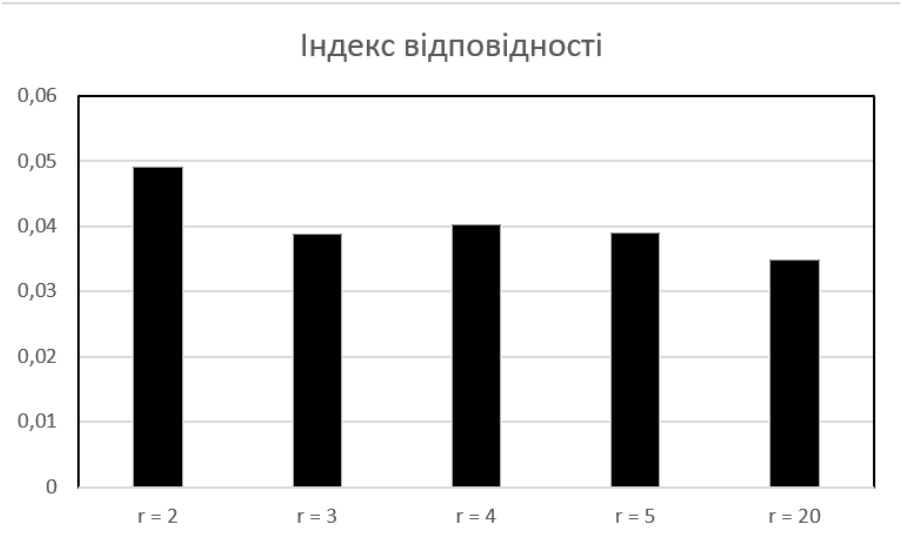
Для відкритого тексту і отриманих в попередньому завданні шифротекстів необхідно було підрахувати значення індексів відповідності за формулою:

$$I(Y) = \frac{1}{n(n-1)} \sum_{i \in Z_m} N_i(Y)(N_i(Y)-1),$$

Для відкритого тексту **I = 0.05872448298865911**

Отримані індекси відповідності для вказаних значень **r** (довжини ключа):

| Довжина | Ключ | Індекс відповідності |
|---|---|---|
| 2 | со | 0.049150989548587945 |
| 3 | мба | 0.03887569490771626 |
| 4 | дива | 0.04033088725817211 |
| 5 | нстол | 0.039144318434511896 |
| 20 | дмизеволдизгонаролми | 0.03482499444073827 |




# Завдання 3:

Для розшифрування даного нам шифротексту роботу було розбито на етапи:

**Перший етап** – знаходження довжини ключа.

Для цього шифротекст спочатку розбили на частини, з різним кроком, що відповідає довжині ключа за таким принципом:

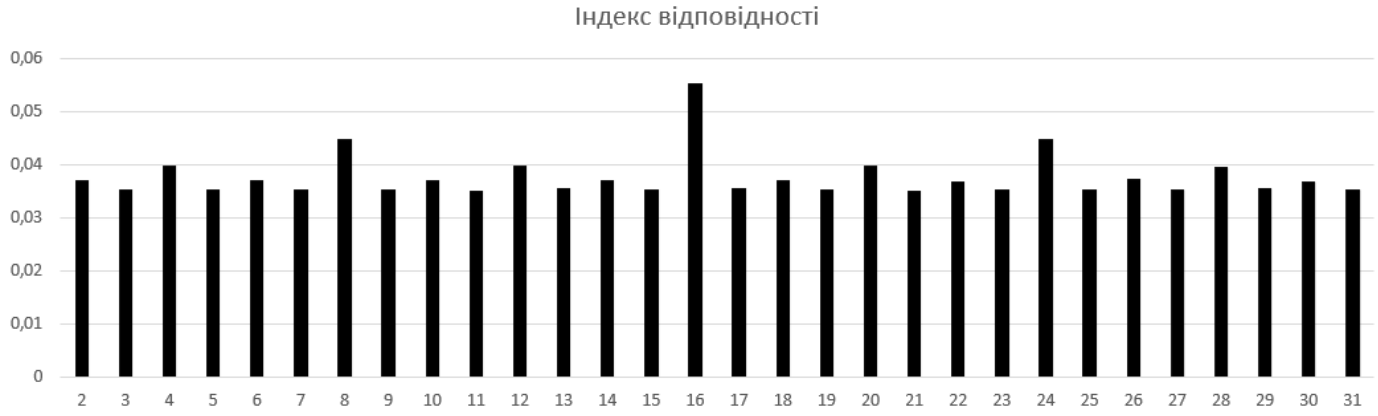
```
                                                          I.C.
original:    vptnvffuntshtarptymjwzirappljmhhqvsubw...    0.049
if key were length 2:
sequence 1:  v t v f n s t r t m w i a p j h q s b ...     0.049
sequence 2:   p n f u t h a p y j z r p l m h v u w...     0.046
                                                 average:  0.048
if key were length 3:
sequence 1:  v  n  f  t  t  p  m  z  a  l  h  v  b ...     0.049
sequence 2:   p  v  u  s  a  t  j  i  p  j  h  s  w...     0.046
sequence 3:    t  f  n  h  r  y  w  r  p  m  q  u  ...     0.046
                                                 average:  0.047
```

Це лише наглядний приклад не пов'язаний з завданням*

Далі, за отриманими частинами знайшли середні значення індексів відповідності для кожного періоду **(r)**:

| Довжина | Індекс відповідності |
|---|---|
| 2 | 0.03709682620655367 |
| 3 | 0.03535245194471151 |
| 4 | 0.039793511667390036 |
| 5 | 0.0354351293936251 |
| 6 | 0.037052368586566846 |
| 7 | 0.03522360497899179 |
| 8 | 0.04491213203766699 |
| 9 | 0.03545025157077616 |
| 10 | 0.03709763005817014 |
| 11 | 0.03506214646542888 |
| 12 | 0.0397888484387092 |
| 13 | 0.03550919719241092 |
| 14 | 0.037093872461702884 |
| 15 | 0.035384371390931875 |
| 16 | 0.05539766505382552 |
| 17 | 0.035524349460576386 |
| 18 | 0.037051140206933175 |
| 19 | 0.03531599104429486 |
| 20 | 0.03979839848540342 |

| | |
|---|---|
| 21 | 0.035056696947883076 |
| 22 | 0.03688094981192191 |
| 23 | 0.03526676001305198 |
| 24 | 0.04486292731353409 |
| 25 | 0.03531687664602463 |
| 26 | 0.03731086887465935 |
| 27 | 0.035247591055245484 |
| 28 | 0.03969086727168179 |
| 29 | 0.035584903885058694 |
| 30 | 0.036928328869868694 |
| 31 | 0.03527346532158508 |




Серед отриманих значень потрібно було знайти найбільш наближене до теоретичного індексу відповідності для російської мови **(I ~ 0.0553)**, таким виявилось значення для періоду **16**, з чого ми зробили висновок, що **довжина ключа дорівнює 16**.

**Другий етап** – знаходження ключа.

Для цього ми отримали усі розбиті частинки з періодом 16, знайшли в кожній частинці букву з найбільшою частотою появи, і розшифрували за допомогою шифру Цезаря за формулою:

$$k = (y^* - x^*) \bmod m$$

де **y*** - індекс букви в алфавіті з найбільшою частотою появи,

а **x*** - індекс букви «**О**» в алфавіті (14), так як вона найчастіше з'являється в російській мові.

Таким чином було отримано ключ «декелисоборойдей», що не повністю схожий на речення яке має сенс. Тому далі було застосовано метод аналізу розшифрованого з цим ключем тексту і заміни букв ключа для отримання істинного відкритого тексту. В процесі виявилось, що перші і останні 4 букви не є вірними.

**Третій етап** – розшифрування шифротексту.

«Методом тика» було знайдено істинний ключ)

**Знайдений ключ: «**делолисоборотней»

**Розшифрований текст:**

понятноеделокультурунасильновчеловеканеводкнешьвордусиэтудовольногрустнуюистинузналинаверноелучшечемгдебы тонибыловмирекультурностьпреждевсегоусилиеиежелионосызмальстванесделалосьчеловекусвычнымдажевнутреннепот ребнымоттоготомногочисленныеподразделенияпалатыцеремонийиуделяютстольковниманиядетямособеннодетямтехктон аселяетхутунынотомужобычнаяленостьлюдскаяслужитемупочтинеодолимымпрепятствиемнанеобъятныхпросторахимпер иивстречаетсяещенемалолюдейкоторымпокакимтолишьбуддазнаеткакимпричинамтакинесталоинтереснымничтоглавное

нисветозарныевысотыдухавеликихрелигийивечныйпоисксмыслажизниземнойпитающийистинноеискусствониголовокру
жительныебезднынакраюкоихвечнопребываетнастилающаянаднимиобщепроходимыегатинауканихотябычистоепросторн
оесостоятельноеидобродетельноежитьестольестественноедлябольшинстваордусскихподданныхчтогрехатаитьхутунынасе
леныбыливосновномварварамииневобычномпониманииэтогословаисстариобозначавшеголюдейинойнеордусскойкультур
ыаскореевтомегозначениикотороестольжедавносделалосьобычнымвевропелюдипочтичуждыевсякойкультурыневедающи
еритуаловивозвышенныхзабототсутствиеподлиннойвоспитанностибросаетсяздесьвглазадаженевнимательномунаблюдате
лючеловексдорогимперстнемнапальцеодетыйвпрекрасныйшелковыйсузорочьемхалатможетнапримервприсутствииженщ
иныпроизнестибранноесловоиливысморкатьсяприлюднопрямовземлюпослечегоспокойнодостатьизрукавадорогойрасшит
ыйплатокиутеретьносежеличеловекповзрослелизаматерелвтакомсостоянииидушиизменитьегокакправилоуженельзяразвеч
томудроенебовразумиттакилииначесмотряповероисповеданиюземнымвластямвэтидуховныеобластипутьзаказаннасилиен
евместноаувещеваниезапоздалокакимбыниуродилсяинисталчеловекнадодатьемупрожитьжизньтаккаконхочетконечноесл
ионпритомневредитокружающимпоэтомубагнеоченьлюбилрайонхутуновикакправилооказывалсяздесьлишьпослужебной
надобностиводнаксегоднянесмотрянапротивныйнавевающийхандрудождикбагбылисполненлегкогопьянящегоазартавсегд
асопутствовавшегоблизкомуиудачномузавершениюочередногоделакконцуподходилорасследованиеоцелойсетичетырезав
еденияединовременноподпольныхопиумокуриленвыявленныхвразудаломпоселкецифрыманилипрасадвернулсявалександ
риювдохновленныйоткрывшимисяперспективамивразудаломпоселкеонужевладелнесколькимихарчевнямиилавкамииесли
кприбылямотторговлиспиртныминапиткамиудастсядобавитьещеидоходыотопиумокурениятоможнобудетподуматьорасш
ирениипредпринимательстваоприобретенииновойнедвижимостиииншаллабытьможетдажеобустановленииконтролянадвс
емихарчевнямиилавкамиразудалогопоселкаатамоченьскоровпринадлежащихлагашузаведенияхнемногочисленныеноверн
ыеегослужителиоборудовалиспециальныезакутыгдекуслугамжителейигостейхутуновывыстроилисьудобныележанкииикури
тельныеприборыпрасадпредлагалпосетителямновоесредстворасслабитьтелоиочиститьдушупослетрудовыхбуднейпосетит
елизаинтересовалисьпотомвошливовкуснопрасадбылжаденвмечтахужвозомнивсебякняземразудалогоонзахотелмногоиср
азунанявсебевпомощьнесколькодюжихмолодцовпрасадзабылоглавномиустремилсякнизменномувзявшисьсилойвнедрять
опиумвхарчевниемунепринадлежавшиечембольшеохваченозаведенийтемвышеприбытоктаксправедливополагаллагашобр
ащатьсяквэйбинамдлярешениявозникающихразногласийбылоневхарактереобитателейхутуновинечестныйпрасадбеззасте
нчивоэтимвоспользовалсяпопыткиздешнихжителейсовладатьслагашемсвоимисиламинеувенчалисьуспехомаспидзаранеепо
дготовилсякстычкамиоттогооказалсясильнееокончательнораспоясавшисьонснялсостеныдвуствольноеружьедедаиприлю
днопрямопосредипереулкаотпилилстволыпослечегосталходитьпохутунамсобрезомзапазухойидажепрозвищеполучилобре
загаместныежителирастерялисьопиумокурильнирасцвеливпоселкенесообразнопышнымцветомлагашподсчитывалбарыши
новеликийучительвдвадцатьвторойглавебеседисужденийнезрясказалянезнаюниодногоправлениякотороебылобыбесконеч
нымисамовольноприсвоенныйпрасадомнебесныймандатместногозначенияужеуплылизегорукхотялагашещеинеподозрева
лобэтомвскоренесколькочеловекпотерялитрудоспособностьинтерескжизниисамоездоровьевследствиечрезмерногоупотре
бленияопиуманасонгрядущийавандевятыйпопалвбольницуулусноеведомствонародногоздоровьявсестороннеизучилоприч
инузаболеванияванаивскореобрезагасамтогоневедаяпопалвполезренияуправлениявнешнейохранызаседмицустараниямиб
агаивзятогоимвпомощьстаршеговэйбинаяковачжанабагссимпатиейнаблюдалкакэтотрозовощекийислегкаещеподетскинаи
вныймолодецпостепеннопревращаетсявсведущегоипытливогомастерасыскногоделарасположениевсехзаведенийгдекурил
иопиумбылоопределеноснаивозможнойточностьютакжебылисоставленыподробныеспискивсехподданныхимевшихотнош
ениекраспространениюопасногодляздоровьяпорокауправлениевнешнейохранысословочевидцевсоставилочленосборныйп
ортретчеловекакоторыйповсемвероятиямявлялсястаршимзаправилойитакчеловеконарушительбылизобличендесятьсамых
способныхвэйбиновпереодевшисьвгражданскоеплатьезатроесутокнепрестанногослужебногобденияустановилигдеобрезаг
абываетпосвоимпротивуправнымделаминынчевечеромпристечениизначительныхсилуправленияодурманиваниеордусски
хподданныхопиумомрешенобылопресечьпоусловленномусигналувэйбинынакрываютвсенехорошиезаведенияабагсяковом
чжаномзадерживаютзаправилуиегоближниковкакасталоизвестновечерниечасыпослеобходасвоихвладенийивзиманияежедн
евнойнеправедноййданилагашсосвоимиближникамикороталвнесообразномвеселиивхарчевнекунисыновьябагещеразвзглян
улначасыираздавилокуроквбронзовойпепельницепораонлегкоподнялсясместаимашинальнопотянулсяпоправитьзапоясом
мечномечанебылонапривычномместеродовойклинокбагаканулвнебытиерастворенныйядовитойслюнойзлоумногоподданн
огокозюлькинаэтисобытияописаныделеополкуигоревеановыймечпрославленныйханбалыкскиймастерганьцзянмошуобе
щалотковатьлишьчерезполторагодабагвздохнулнезаметнопроверилскрытыеплотнымхалатомбоевыеножиподхватилзонти
пошелквыходуиззалытудагдеседваслышнымшорохомсеялсясквозьгустеющиесумеркибесконечныйдождьпора

## Висновок:

Під час роботи з даною лабораторною роботою ми ближче познайомились з Шифром Віженера, методами частотного аналізу, його роботою і методами його криптоаналізу. Нам вдалося зламати даний нам шифротекст, ознайомившись при цьому з визначенням індексу відповідності.