**Міністерство освіти і науки України**

**Національний технічний університет України**

**"Київський політехнічний інститут імені Ігоря Сікорського"**

**Фізико-технічний інститут**

КРИПТОГРАФІЯ

Комп’ютерний практикум

Робота № 2

«Криптоаналіз шифру Віженера»

Виконав:

студент гр. ФБ-02

Шубін Д.Ю

**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.

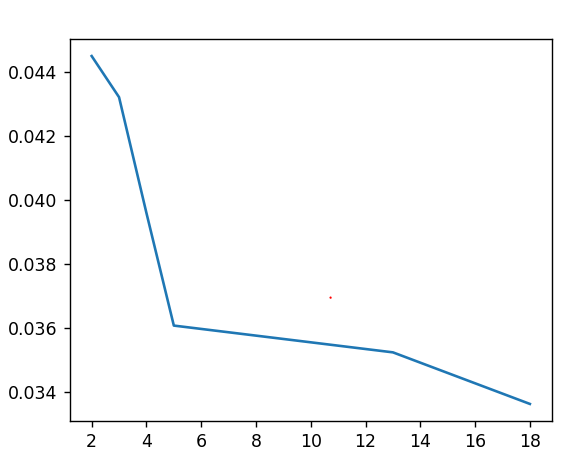
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

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

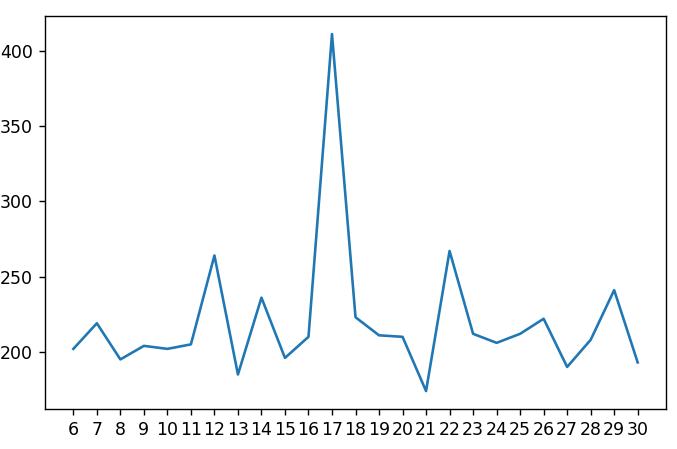
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

**Номер варіанту: 11**

**Хід роботи:**

1). Обчислені значення індексів відповідності для вказаних значень r:

|  |  |
| --- | --- |
| **r** | **I(Y)** |
| 2 | 0,04448471494321517 |
| 3 | 0,04319971993698582 |
| 4 | 0,03958361219509684 |
| 5 | 0,036068409509786764 |
| 13 | 0,03523233904099011 |
| 18 | 0,03362197670946551 |

2). Обчислена послідовність Dr, одержаних при встановленні довжини ключа шифру Віженера:  
D\_r = [202, 219, 195, 204, 202, 205, 264, 185, 236, 196, 210, 411, 223, 211, 210, 174, 267, 212, 206, 212, 222, 190, 208, 241, 193]  
  
Робимо висновок, що **r = 17**

3). **Знайдене значення ключа:**  
  
За умовою завдання, ключ має бути змістовний, отже знайдений ключ потрібно скоригувати відповідно до реконструкції тексту за правильно розшифрованими фрагментами.

**Текст, розшифрований за допомогою ключа “венецианскийкужьц”** (перші 4 рядки):  
*антонионезнаюоыаегоятакпечаленмцоэтовтягостьвамяъфышутоженогдеягрьътьпоймалнашелиленобылчтосоставляоычтородитеехотелкдзнатьбессмысленцйягрустьмоявиноюаыосамогосебяузнаыемнетрудносаларицчвыдухоммечетесьшчокеанугдевашивефсчавыесудакакбогйыеиивельможиводифепышнаяпроцессияхчрскаяспрезреньехъмотрятнаторговцолмелкихчтокланя*

Візьмемо початок розшифрованого тексту: “*антонионезнаюоыаегоятакпечаленмцо*”  
Здогадуємось, що замість “*мцо*” має бути “*мне*”  
Коригуємо 15ту та 16ту літеру ключа.

**Скориговане значення ключа:**  
  
**Текст, розшифрований за допомогою ключа “венецианскийкупец”:**  
*антонионезнаюотчегоятакпечаленмнеэтовтягостьвамяслышутоженогдеягрустьпоймалнашелильдобылчтосоставляетчтородитеехотелбызнатьбессмысленнаягрустьмоявиноючтосамогосебяузнатьмнетрудносалариновыдухоммечетесьпоокеанугдевашивеличавыесудакакбогатеиивельможиводильпышнаяпроцессияморскаяспрезреньемсмотрятнаторговцевмелкихчтокланяютсянизкоимспочтеньемкогдаонилетятнатканыхкрыльяхсаланиоповерьтееслибятакрисковалпочтивсечувствабылибтаммоисмоейнадеждойябыпостоянносрывалтравучтобзнатьоткудаветерискалнакартахгаваниибухтылюбойпредметчтомогбынеудачумнепредвещатьменябынесомненновгрустьповергалсалариностудямойсупдыханьемявлихорадкебыдрожалотмысличтоможетвмореураганнаделатьнемогбывидетьячасовпесочныхневспомнившиомеляхиорифахпредставилбыкорабльвпескезавязшимглавусклонившимнижечембокачтобцеловатьсвоюмогилувцерквисмотрянакамнизданиясвятогокакмогбыяневспомнитьскалопасныхчтохрупкиймойкорабльедватолкнуввсепряностирассыпалибывводуиволныоблеклибвмоишелканусловомчтомоебогатствосталоничемимоглибяобэтомдуматьнедумаяпритомчтоеслибтакслучилосьмнепришлосьбызагруститьнеговоритезнаюяантониогруститтревожасьзасвоитоварыантонионетверьтемнеблагодарюсудьбумойрискнеодномуявверилсуднунеодномуиместусостояньемоенемеритсятекущимгодомянегрущуиззамоихтоваровсаларинотогдавызначитвлюбленыантониопустоесалариноневлюбленытакскажемвыпечальнызатемчтовыневеселыитолькомоглибсмеятьсявытвердяявеселзатемчтонегрущудвуличныйянусклянусьтобойродитприродастранныхлюдейодниглазеютихохочуткакпопугайуслышавшийволынкудругиеженавидкакуксускислытакчтовулыбкезубынепокажутклянисьсамнесторчтозабавнашуткавходятбассаниолоренцоиграцианосаланиовотблагородныйродичвашбассаниограцианоилоренцоснимпрощайтемывлучшемобществеоставимвассалариноосталсябячтобвасразвеселитьновотявижутехктовамдорожеантониовмоихглазахценавамдорогасдаетсямнечтовасделазовутирадывыпредлогуудалитьсясалариноприветвамгосподабассаниосиньорынокогдажмыпосмеемсякогдавычтотосталинелюдимысаларинодосугвашмыделитьготовысвамисалариноисаланиоуходятлоренцокбассаниосиньорразвыантонионашлимывасоставимнопрошукобедунепозабытьгдемыдолжнысойтисьбассаниопридунавернограцианосиньорантониовидувасплохойпечетесьслишкомвыоблагахмирактоихтрудомчрезмернымпокупаеттеряетихкакизменилисьвыантониоямирсчитаючемонестьграцианомирсценагдеувсякогоестьрольмоягрустнаграцианомнеждайтерольшутапускайотсмехабудувесьвморщинахпустьлучшепеченьотвинагоритчемстынетсердцеоттяжелыхвздоховзачемжечеловекустеплойкровьюсидетьподобномраморномупредкуспатьнаявуилихворатьжелтухойотраздраженьяслушайкаантониотебялюблюяговоритвомнелюбовьестьлюдиукоторыхлицапокрытыпленкойточногладьболотаонихранятнарочнонеподвижностьчтобобщаямолваимприписаласерьезностьмудростьиглубокийумисловноговорятнамяоракулкогдавещаюпустьипеснелаетомойантониознаюятакихчтомудрымислывутлишьпотомучтоничегонеговоряттогдакакзаговоривонитерзалибушитемктоихслышаближнихдуракаминазвалбывернодаобэтомпосленонеловитынаприманкугруститакуюславужалкуюрыбешкупойдемлоренцонупокапрощайапроповедьякончупообедавлоренцоитаквасоставляемдообедапридетсямнебытьмудрецомтакимбезмолвнымговоритьнедастграцианограцианодапоживисомноюгодадвазвукголосатысвоегозабудешьантонионудлятебяястануболтуномграцианоотличноведьмолчаньехорошовкопченыхязыкахдавчистыхдевахграцианоилоренцоуходятантониогдесмыслвегословахбассаниограцианоговоритбесконечномногопустяковбольшечемктолибоввенецииегорассужденияэтодвазернапшеницыспрятанныевдвухмерахмякинычтобыихнайтинадоискатьвесьденьанайдешьувидишьчтоиискатьнестоиловенецияулицавходитланчелотланчелотконечносовестьмояпозволитмнесбежатьотэтогожидамоегохозяинабесменятаквотитолкаеттаквотиискушаетговоритгобболанчелотгоббодобрыйланчелотилидобрыйгоббоилидобрыйланчелотгоббопустиногивходбегивовсетяжкиеудирайотсюдаасовестьговоритнетпостойчестныйланчелотпостойчестныйгоббоиликаквышесказаночестнейшийланчелотгоббонеудирайтопниногойнаэтимыслиладноахрабрыйдьяволвелитмнескладыватьпожиткивпутьговоритбесмаршговоритбесрадибогасоберисьсдухомговоритбесилупиладноасовестьмоявешаетсянашеюкмоемусердцуимудроговоритмойчестныйдругланчелотведьтысынчестногоотцаилискореесынчестнойматерипотомучтосказатьправдуотецтомойнесколькокакбыэтовыразитьсяотдавалчемтобылунегоэтакийпривкусладносовестьмнеговоритланчелотнешевелисьпошевеливайсяговоритбеснисместаговоритсовестьсовестьговорюправильнотысоветуешьеслиповиноватьсясовестинадомнеостатьсяужидамоегохозяинааонтопростименягосподисамвродедьяволаачтобыудратьотжидапридетсяповиноватьсялукавомуаведьонтосвашегопозволенияиестьсамдьяволитоправдачтожидвоплощенныйдьяволипосовестиговорясовестьмояжестокосерднаясовестьеслионамнесоветуетостатьсяужидабесмнедаетболеедружескийсоветятакиудерудьяволмоипяткиктвоимуслугамудерувходитстарыйгоббоскорзинкойгоббомолодойсиньорскажитепожалуйстакактутпройтиксиньоружидуланчелотвсторонуонебодаэтомойединородныйотецонслептаксловноемунеточтопескомакрупнымгравиемглазазасыпалонеузнаетменясыграюснимкакуюнибудьштукугоббопочтеннейшиймолодойсиньорсделайтемилостькакмнепройтиксиньоружидуланчелотаповернитенаправоприпервомповоротеноприсамомпервомповоротеповернитеналеводасмотритепринастоящемтоповоротенеповорачивайтенинаправониналевоаворочайтепрямехонькокдомужидагоббосвятыеугодникитруднобудетпопастьнанастоящуюдорогувынеможетесказатьмненекийланчелотчтоунегоживетживетунегоилинетланчелотвыговоритеомолодомсиньореланчелотевсторонувотпогодитекакуюясейчасисториюразведустарикувыговоритеомолодомсиньореланчелотегоббокакойтамсиньорвашамилостьсынбедногочеловекаотецегохотьэтоясамговорючестныйнооченьбедныйчеловекхотяблагодарябогаздоровыйланчелотнуктобытамнибылегоотецмыговоримомолодомсиньореланчелотегоббоознакомомвашеймилостипростоланчелотесударьланчелотнопрошувасстариктобишьумоляювасследственновыговоритеомолодомсиньореланчелотегоббооланчелотеспозволениявашеймилостиланчелотследственноосиньореланчелотенеговоритеосиньореланчелотебатюшкамойибоэтотмолодойсиньорсогласноволесудебирокаивсякихтакихученыхвещейвродетрехсестерпарокипрочихотраслейнаукидействительноскончалсяилиеслиможновыразитьсяпрощеотошелвлучшиймиргоббогосподиупасидаведьмальчуганбылистиннымпосохоммоейстаростиистинноймоейподпоройланчелотнеужтожяпохожнапалкуилинабалкунапосохилинаподпоркувыменянеузнаетебатюшкагоббоохнетяваснезнаюмолодойсиньорнопрошувасскажитемнеправдучтомоймальчикупокойгосподьегодушуживилипомерланчелотнеужтовынеузнаетеменябатюшкагоббоохгореяведьпочтичтоослепнепризнаювасланчелотнупоправдедажебудьувасглазавпорядкевыитомоглибынеузнатьменяументототецчтоузнаетсобственногоребенкаладностарикявамвсерасскажупровашегосынастановитсянаколениблагословименяправдадолжнавыйтинасветубийствадолгоскрыватьнельзякточейсынэтоскрытьможноновконцеконцовправдавыйдетнаружу*

**Висновок:** у ході лабораторної роботи, я здобув навички роботи та аналізу потокових шифрів гамування адитивноготипу на прикладі шифру Віженера. Також я на практиці засвоїв методи частотного криптоаналізу, реалізувавши їх на мові програмування Python.