**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 11

Виконав:

cтудент групи ФБ-01

Полянський Ян

**Київ – 2022**

**Мета роботи:**

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

**Постановка задачі:**

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.

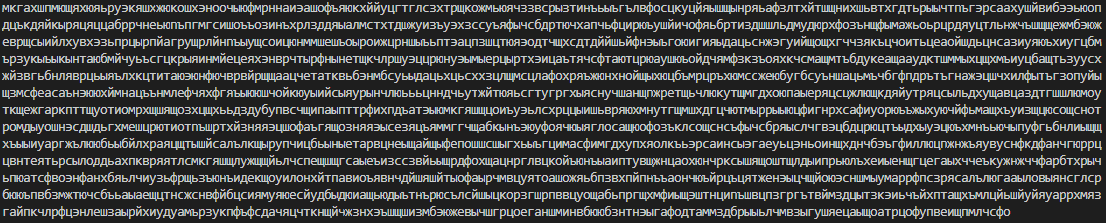
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст(згідно свого номеру варіанта).

**Хід роботи:**

*Обчислені значення індексів відповідності для зазначених нижче r*

****

|  |  |
| --- | --- |
| **Довжина ключа\ключ** | **Індекс відповідності** |
| Довжина ключа 2 : 'да' | 0.045150332444932266 |
| Довжина ключа 3 : 'три' | 0.03848975711523622 |
| Довжина ключа 4 : 'гора' | 0.03657186172081242 |
| Довжина ключа 5 : 'панда' | 0.03707055344564357 |
| Довжина ключа 6 : 'лопата' | 0.03605857414062036 |
| Довжина ключа 10 : 'литература' | 0.034446218651751646 |
| Довжина ключа 13 : 'архитектоника' | 0.03429296217046207 |
| Довжина ключа 14 : 'диакритический' | 0.03499356322778584 |
| Довжина ключа 15 : 'авторизационный' | 0.03327173882371028 |
| Довжина ключа 16 : 'автопутеводитель' | 0.03369988391429703 |
| Довжина ключа 17 : 'автокомплектующие' | 0.03310096731598762 |
| Довжина ключа 18 : 'благоприобретенный' | 0.03376361914937301 |
| Довжина ключа 19 : 'бактериостатический' | 0.032981767830540173 |
| Довжина ключа 20 : 'автоматизированность' | 0.03331795903235317 |

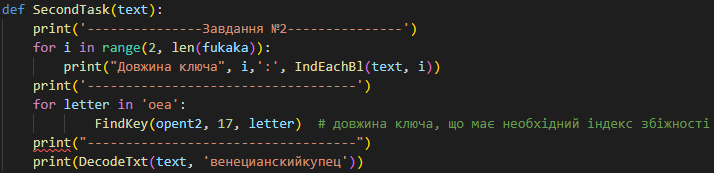
**\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\**

**\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\**

|  |  |
| --- | --- |
| **Довжина ключа** | **Індекс відповідності** |
| Довжина ключа 2 : | 0.03385469736120976 |
| Довжина ключа 3 : | 0.0338903572127828 |
| Довжина ключа 4 : | 0.03382856631255099 |
| Довжина ключа 5 : | 0.0339485646135541 |
| Довжина ключа 6 : | 0.03393201950461585 |
| Довжина ключа 7 : | 0.033887879672849 |
| Довжина ключа 8 : | 0.03387028521782783 |
| Довжина ключа 9 : | 0.033925669332816634 |
| Довжина ключа 10 : | 0.033896990798633383 |
| Довжина ключа 11 : | 0.03369705663706743 |
| Довжина ключа 12 : | 0.03402936176339339 |
| Довжина ключа 13 : | 0.03382497157080262 |
| Довжина ключа 14 : | 0.03374056874966326 |
| Довжина ключа 15 : | 0.03389000107283445 |
| Довжина ключа 16 : | 0.0340028030190302 |
| ***Довжина ключа 17 :*** | ***0.056652871546688466*** |
| Довжина ключа 18 : | 0.033914675695348 |

З таблиці видно, що довжина **ключа** є **17** символів, оскільки індекс збіжності для цієї довжини ключа є найближчим до індексу збіжності, що отримали у першому завданні.

\**Значення індексів збіжності були пораховані для всіх 32-ох значень довжин ключа. В таблицю занесено всі значення до того, яке нас цікавило,отжн наступні не будуть інформативними, всі й близько не схожі до того, що нам потрібно.*

****

***Отримали:***

****

**Ключ** має бути змістовний, і перший з виведених програмою схожий на такий, лишилося лиш легко здогадатися, що це: '**венецианскийкупец**'

***Отже, шуканий розшифрований текст:***

антонионезнаюотчегоятакпечаленмнеэтовтягостьвамяслышутоженогдеягрустьпоймалнашелильдобылчтосоставляетчтородитеехотелбызнатьбессмысленнаягрустьмоявиноючтосамогосебяузнатьмнетрудносалариновыдухоммечетесьпоокеанугдевашивеличавыесудакакбогатеиивельможиводильпышнаяпроцессияморскаяспрезреньемсмотрятнаторговцевмелкихчтокланяютсянизкоимспочтеньемкогдаонилетятнатканыхкрыльяхсаланиоповерьтееслибятакрисковалпочтивсечувствабылибтаммоисмоейнадеждойябыпостоянносрывалтравучтобзнатьоткудаветерискалнакартахгаваниибухтылюбойпредметчтомогбынеудачумнепредвещатьменябынесомненновгрустьповергалсалариностудямойсупдыханьемявлихорадкебыдрожалотмысличтоможетвмореураганнаделатьнемогбывидетьячасовпесочныхневспомнившиомеляхиорифахпредставилбыкорабльвпескезавязшимглавусклонившимнижечембокачтобцеловатьсвоюмогилувцерквисмотрянакамнизданиясвятогокакмогбыяневспомнитьскалопасныхчтохрупкиймойкорабльедватолкнуввсепряностирассыпалибывводуиволныоблеклибвмоишелканусловомчтомоебогатствосталоничемимоглибяобэтомдуматьнедумаяпритомчтоеслибтакслучилосьмнепришлосьбызагруститьнеговоритезнаюяантониогруститтревожасьзасвоитоварыантонионетверьтемнеблагодарюсудьбумойрискнеодномуявверилсуднунеодномуиместусостояньемоенемеритсятекущимгодомянегрущуиззамоихтоваровсаларинотогдавызначитвлюбленыантониопустоесалариноневлюбленытакскажемвыпечальнызатемчтовыневеселыитолькомоглибсмеятьсявытвердяявеселзатемчтонегрущудвуличныйянусклянусьтобойродитприродастранныхлюдейодниглазеютихохочуткакпопугайуслышавшийволынкудругиеженавидкакуксускислытакчтовулыбкезубынепокажутклянисьсамнесторчтозабавнашуткавходятбассаниолоренцоиграцианосаланиовотблагородныйродичвашбассаниограцианоилоренцоснимпрощайтемывлучшемобществеоставимвассалариноосталсябячтобвасразвеселитьновотявижутехктовамдорожеантониовмоихглазахценавамдорогасдаетсямнечтовасделазовутирадывыпредлогуудалитьсясалариноприветвамгосподабассаниосиньорынокогдажмыпосмеемсякогдавычтотосталинелюдимысаларинодосугвашмыделитьготовысвамисалариноисаланиоуходятлоренцокбассаниосиньорразвыантонионашлимывасоставимнопрошукобедунепозабытьгдемыдолжнысойтисьбассаниопридунавернограцианосиньорантониовидувасплохойпечетесьслишкомвыоблагахмирактоихтрудомчрезмернымпокупаеттеряетихкакизменилисьвыантониоямирсчитаючемонестьграцианомирсценагдеувсякогоестьрольмоягрустнаграцианомнеждайтерольшутапускайотсмехабудувесьвморщинахпустьлучшепеченьотвинагоритчемстынетсердцеоттяжелыхвздоховзачемжечеловекустеплойкровьюсидетьподобномраморномупредкуспатьнаявуилихворатьжелтухойотраздраженьяслушайкаантониотебялюблюяговоритвомнелюбовьестьлюдиукоторыхлицапокрытыпленкойточногладьболотаонихранятнарочнонеподвижностьчтобобщаямолваимприписаласерьезностьмудростьиглубокийумисловноговорятнамяоракулкогдавещаюпустьипеснелаетомойантониознаюятакихчтомудрымислывутлишьпотомучтоничегонеговоряттогдакакзаговоривонитерзалибушитемктоихслышаближнихдуракаминазвалбывернодаобэтомпосленонеловитынаприманкугруститакуюславужалкуюрыбешкупойдемлоренцонупокапрощайапроповедьякончупообедавлоренцоитаквасоставляемдообедапридетсямнебытьмудрецомтакимбезмолвнымговоритьнедастграцианограцианодапоживисомноюгодадвазвукголосатысвоегозабудешьантонионудлятебяястануболтуномграцианоотличноведьмолчаньехорошовкопченыхязыкахдавчистыхдевахграцианоилоренцоуходятантониогдесмыслвегословахбассаниограцианоговоритбесконечномногопустяковбольшечемктолибоввенецииегорассужденияэтодвазернапшеницыспрятанныевдвухмерахмякинычтобыихнайтинадоискатьвесьденьанайдешьувидишьчтоиискатьнестоиловенецияулицавходитланчелотланчелотконечносовестьмояпозволитмнесбежатьотэтогожидамоегохозяинабесменятаквотитолкаеттаквотиискушаетговоритгобболанчелотгоббодобрыйланчелотилидобрыйгоббоилидобрыйланчелотгоббопустиногивходбегивовсетяжкиеудирайотсюдаасовестьговоритнетпостойчестныйланчелотпостойчестныйгоббоиликаквышесказаночестнейшийланчелотгоббонеудирайтопниногойнаэтимыслиладноахрабрыйдьяволвелитмнескладыватьпожиткивпутьговоритбесмаршговоритбесрадибогасоберисьсдухомговоритбесилупиладноасовестьмоявешаетсянашеюкмоемусердцуимудроговоритмойчестныйдругланчелотведьтысынчестногоотцаилискореесынчестнойматерипотомучтосказатьправдуотецтомойнесколькокакбыэтовыразитьсяотдавалчемтобылунегоэтакийпривкусладносовестьмнеговоритланчелотнешевелисьпошевеливайсяговоритбеснисместаговоритсовестьсовестьговорюправильнотысоветуешьеслиповиноватьсясовестинадомнеостатьсяужидамоегохозяинааонтопростименягосподисамвродедьяволаачтобыудратьотжидапридетсяповиноватьсялукавомуаведьонтосвашегопозволенияиестьсамдьяволитоправдачтожидвоплощенныйдьяволипосовестиговорясовестьмояжестокосерднаясовестьеслионамнесоветуетостатьсяужидабесмнедаетболеедружескийсоветятакиудерудьяволмоипяткиктвоимуслугамудерувходитстарыйгоббоскорзинкойгоббомолодойсиньорскажитепожалуйстакактутпройтиксиньоружидуланчелотвсторонуонебодаэтомойединородныйотецонслептаксловноемунеточтопескомакрупнымгравиемглазазасыпалонеузнаетменясыграюснимкакуюнибудьштукугоббопочтеннейшиймолодойсиньорсделайтемилостькакмнепройтиксиньоружидуланчелотаповернитенаправоприпервомповоротеноприсамомпервомповоротеповернитеналеводасмотритепринастоящемтоповоротенеповорачивайтенинаправониналевоаворочайтепрямехонькокдомужидагоббосвятыеугодникитруднобудетпопастьнанастоящуюдорогувынеможетесказатьмненекийланчелотчтоунегоживетживетунегоилинетланчелотвыговоритеомолодомсиньореланчелотевсторонувотпогодитекакуюясейчасисториюразведустарикувыговоритеомолодомсиньореланчелотегоббокакойтамсиньорвашамилостьсынбедногочеловекаотецегохотьэтоясамговорючестныйнооченьбедныйчеловекхотяблагодарябогаздоровыйланчелотнуктобытамнибылегоотецмыговоримомолодомсиньореланчелотегоббоознакомомвашеймилостипростоланчелотесударьланчелотнопрошувасстариктобишьумоляювасследственновыговоритеомолодомсиньореланчелотегоббооланчелотеспозволениявашеймилостиланчелотследственноосиньореланчелотенеговоритеосиньореланчелотебатюшкамойибоэтотмолодойсиньорсогласноволесудебирокаивсякихтакихученыхвещейвродетрехсестерпарокипрочихотраслейнаукидействительноскончалсяилиеслиможновыразитьсяпрощеотошелвлучшиймиргоббогосподиупасидаведьмальчуганбылистиннымпосохоммоейстаростиистинноймоейподпоройланчелотнеужтожяпохожнапалкуилинабалкунапосохилинаподпоркувыменянеузнаетебатюшкагоббоохнетяваснезнаюмолодойсиньорнопрошувасскажитемнеправдучтомоймальчикупокойгосподьегодушуживилипомерланчелотнеужтовынеузнаетеменябатюшкагоббоохгореяведьпочтичтоослепнепризнаювасланчелотнупоправдедажебудьувасглазавпорядкевыитомоглибынеузнатьменяументототецчтоузнаетсобственногоребенкаладностарикявамвсерасскажупровашегосынастановитсянаколениблагословименяправдадолжнавыйтинасветубийствадолгоскрыватьнельзякточейсынэтоскрытьможноновконцеконцовправдавыйдетнаружу