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

Фізико-технічний інститут

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Виконав: Маслюк В.О. ФБ-25

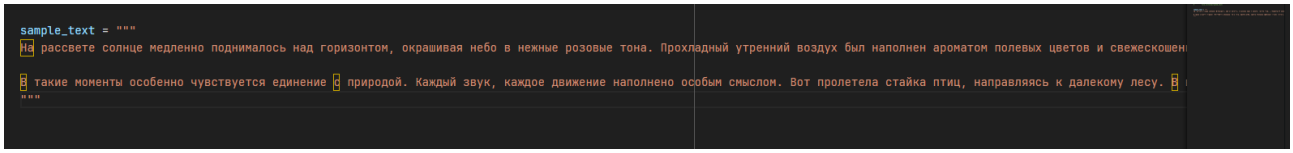
Київ 2024

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

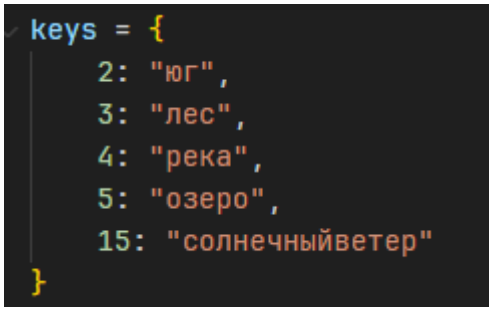
Хід роботи

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.**

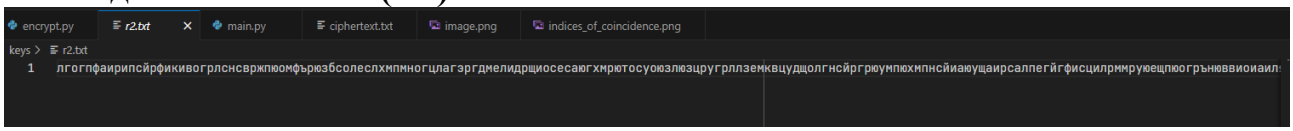
Текст для шифрування:



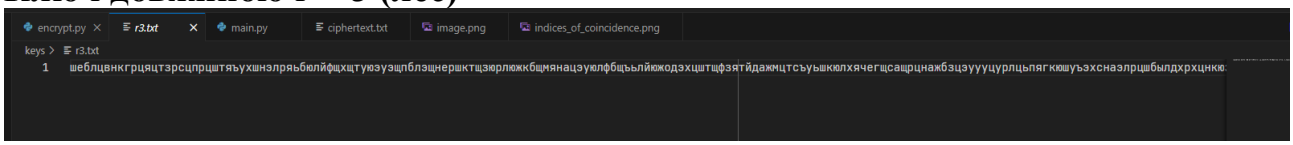
Ключі:



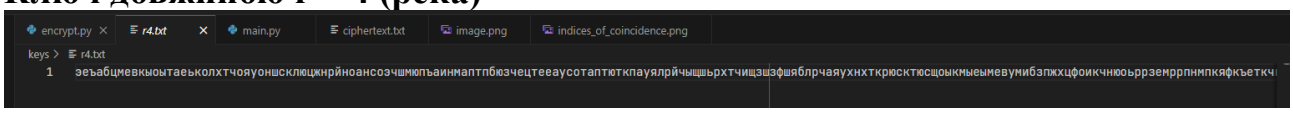
Ключ довжиною r = 2 (юг)



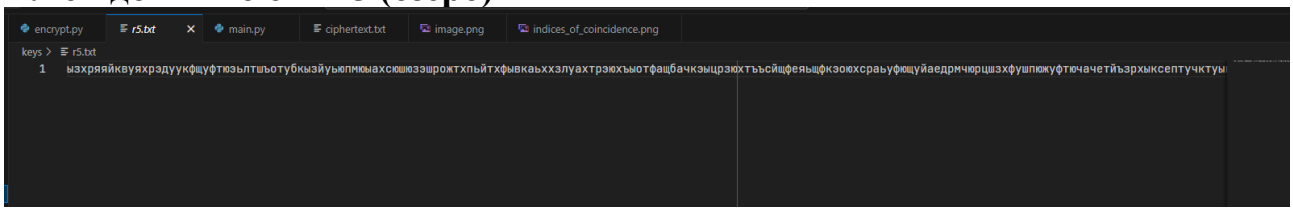
Ключ довжиною r = 3 (лес)



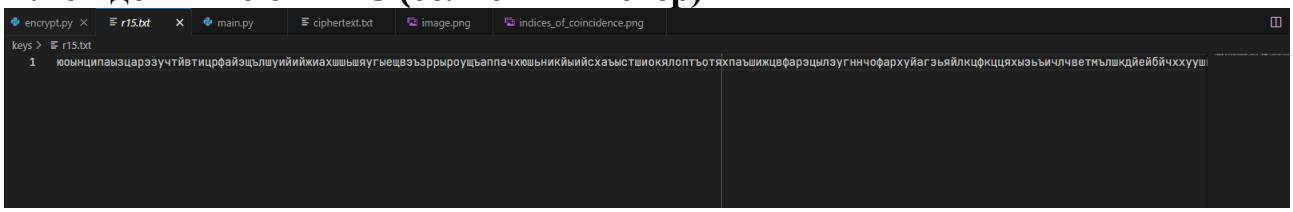
Ключ довжиною r = 4 (река)



Ключ довжиною r = 5 (озеро)



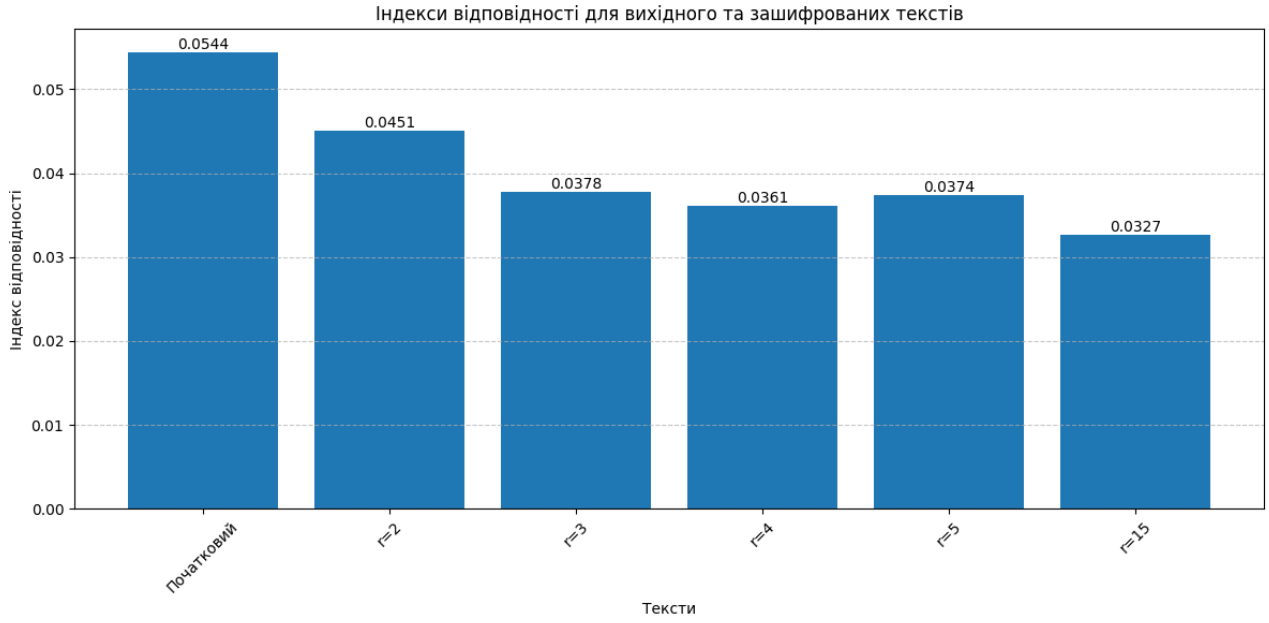
Ключ довжиною r = 15 (солнечныйветер)



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

Діаграма

```
Індекси відповідності:
Вихідний текст: 0.0544
Ключ довжини 2: 0.0451
Ключ довжини 3: 0.0378
Ключ довжини 4: 0.0361
Ключ довжини 5: 0.0374
Ключ довжини 15: 0.0327
```



3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (Варіант 11)

```
Можливі довжини ключа (відсортовані за зменшенням індексу збігу):
Довжина 17: 0.0567
Довжина 21: 0.0342
Довжина 30: 0.0341
Довжина 24: 0.0340
Довжина 12: 0.0340
```

```
Індекс відповідності відкритого тексту: 0.054354178842782
```

ми бачимо, що найближче до теоретичного значення I = 0.05435 схиляється період 17. Знайдемо ключ цієї довжини.

```
Ймовірний ключ довжини 17: венецианскийкупец
```

Отже, наш ключ – венецианскийкупец.

Розшифруємо текст:

антонионезнаюотчегоятакпечаленмнеэтовтягостьвамяслышутоженогдеягрустьп
оймалнашелильдобылчтосоставляетчтородитеехотелбызнатьбессмысленнаягру
стьмоявиноючтосамогосебяузнатьмнетрудносалариновыдухоммечетесьпоокеан
угдевашивеличавыесудакакбогатеиивельможиводильпышнаяпроцессияморская
спрезреньемсмотрятнаторговцевмелкихчтокланяютсянизкоимспочтеньемкогда
онилетятнаткаными хкрыльяхсалаииоповерьтееслибятакрисковалпочтивсечувства
былибтаммоисмоейнадеждойябыпостоянносрывалтравучтобзнатьоткудаветери
скалнакартахгаваниибухтылюбойпредметчтомогбынеудачумнепредвещатьменя
бынесомненновгрустьповергалсалариностудямойсупдыханьемявлихорадкебыд
рожалотмысличтоможетвмореураганнаделатьнемогбывидетьячасовпесочныхне
вспомнившиомеляхиорифахпредставилбыкорабльвпескезавязшимглавусклонив
шимнижечембокачтобцеловатьсвоюмогилувцерквисмотрянакамнизданиясвятог
окакмогбыяневспомнитьскалопасныхчтохрупкиймойкорабльедватолкнуввсепря
ностирассыпалибывводуиволныоблеклибвмоишелканусловомчтомоебогатствос
талоничемимоглибяобэтомдуматьнедумаяпритомчтоеслибтакслучилосьмнепри
шлосьбызагруститьнеговоритезнаюяантониогруститтревожасьзасвоитоварыант
онионетверьтемнеблагодарюсудьбумойрискнеодномуявверилсуднунеодномуим
естусостояньемоенемеритсятекущимгодомянегрущуиззамоихтоваровсаларинот
огдавызначитвлюбленыантониопустоесалариноневлюбленытакскажемвыпечаль
нызатемчтовыневеселыитолькомоглибсмеятьсявытвердяявеселзатемчтонегрущ
удвуличныйянусклянусьтобойродитприроластранныхлюдейодниглазеютихохоч
уткакпопугайуслышавшийволынкудругиеженавидкакуксускислытакчтовулыбк
езубынепокажутклянисьсамнесторчтозабавнашуткавходятбассаниолоренцоигра
цианосаланиовотблагородныйродичвашбассаниограцианоилоренцоснимпроща
йтемывлучшемобществеоставимвассалариноосталсябячтобвасразвеселитьновот
явижутехктовамдорожеантониовмоихглазахценавамдорогасдаетсямнечтовасдел
азовутирадывыпредлогуудалитьсясалариноприветвамгосподабассаниосиньоры
нокогдажмыпосмеемсякогдавычтотосталинелюдимысаларинодосугвашмыделит
ьготовысвамисалариноисаланиоуходятлоренцокбассаниосиньорразвыантонион
ашлимывасоставимнопрошукобедунепозабытьгдемыдолжнысойтисьбассаниопр
идунаверноградиаиосиньорантониовидувасплохойпечетесьслишкомвыоблагах
мирактоихтрудомчрезмерным покупаеттеряетихкакизменилисьвыантониоямирс
читаючемонестьградиаиомирсценагдеувсякогоестьрольмоягрустнаградиаиомне
ждайтерольшутапускайотсмехабудувесьвморщинахпустьлучшепеченьотвинаго
ритчемстынетсердцеоттяжелыхвздоховзачемжечеловекустеплойкровьюсидетьп
одобномраморномупредкуспатьнаявуилихворатьжелтухойотраздраженьяслуша
йкаантониотебялюблюяговоритвомнелюбовьестьлюдиукоторыхлицапокрытыпл
енкойточногладьболотаонихранятнарочнонеподвижностьчтобобщаямолваимпр
иписаласерьезностьмудростьиглубокийумисловноговорятнамяоракулкогдавеща
юпустьипеснелаетомойантониознаюятакихчтомудрымислывутлишьпотомучтон
ичегонеговоряттогдакакзаговоривонитерзалибушитемктоихслышаближнихдура

каминазвалбывернодаобэтомпосленонеловитынаприманкугруститкакуюславужа
лкуюрыбешкупойдемлоренцонупокапрощайапроповедьякончупообедавлоренцо
итаквасоставляемдообедапридетсямнебытьмудрецомтакимбезмолвнымговорит
ьнедастграцианограцианодапоживисомноюгодадвазвукголосатысвоегозабудеш
ьантонионудлятебяястануболтуномграцианоотличноведьмолчаньехорошовкопч
еныхязыкахдавчистыхдевахграцианоилоренцоуходятантониогдесмыслвегослов
ахбассаниограцианоговоритбесконечномногопустяковбольшечемктолибоввене
циииегорассужденияэтодвазернапшеницыспрятанныевдвухмерахмякинычтобыи
хнайтинадоискатьвесьденьанайдешьувидишьчтоиискатьнестоиловенецияулица
входитланчелотланчелотконечносовестьмояпозволитмнесбежатьотэтогожидамо
егохозяинабесменятаквотитолкаеттаквотиискушаетговоритгобболанчелотгоббо
добрыйланчелотилидобрыйгоббоилидобрыйланчелотгоббопустиногивходбегив
овсетяжкиеудирайотсюдаасовестьговоритнетпостойчестныйланчелотпостойчес
тныйгоббоиликаквышесказаночестнейшийланчелотгоббонеудирайтопниногойн
аэтимыслиладноахрабрыйдьяволвелитмнескладыватьпожиткивпутьговоритбес
маршговоритбесрадибогасоберисьсдухомговоритбесилупиладноасовестьмояве
шаетсянашеюкмоемусердцуимудроговоритмойчестныйдругланчелотведьтысын
честногоотцаилискореесынчестнойматерипотомучтосказатьправдуотецтомойне
сколькокакбыэтовыразитьсяотдавалчемтобылунегоэтакийпривкусладносовесть
мнеговоритланчелотнешевелисьпошевеливайсяговоритбеснисместаговоритсове
стьсовестьговорюправильнотысоветуешьеслиповиноватьсясовестинадомнеоста
тьсяужидамоегохозяинааонтопростименягосподисамвродедьяволаачтобыудрать
отжидапридетсяповиноватьсялукавомуаведьонтосвашегопозволенияиестьсамдь
яволитоправдачтожидвоплощенныйдьяволипосовестиговорясовестьмояжестоко
серднаясовестьеслионамнесоветуетостатьсяужидабесмнедаетболеедружескийсо
ветятакиудерудьяволмоипяткиктвоимуслугамудерувходитстарыйгоббоскорзинк
ойгоббомолодойсиньорскажитепожалуйстакактутпройтиксиньоружидуланчело
твсторонуонебодаэтомойединородныйотецонслептаксловноемунеточтопескома
крупнымгравиемглазазасыпалонеузнаетменясыграюснимкакуюнибудьштукугоб
бопочтеннейшиймолодойсиньорсделайтемилостькакмнепройтиксиньоружидул
анчелотаповернитенаправоприпервомповоротеноприсамомпервомповоротепове
рнитеналеводасмотритепринастоящемтоповоротенеповорачивайтенинаправони
налевоаворочайтепрямехонькокдомужидагоббосвятыеугодникитруднобудетпоп
астьнанастоящуюдорогувынеможетесказатьмненекийланчелотчтоунегоживетж
иветунегоилинетланчелотвыговоритеомолодомсиньореланчелотевсторонувотпо
годитекакуюясейчасисториюразведустарикувыговоритеомолодомсиньореланче
лотегоббокакойтамсиньорвашамилостьсынбедногочеловекаотецегохотьэтоясам
говорючестныйнооченьбедныйчеловекхотяблагодарябогаздоровыйланчелотнук
тобытамнибылегоотецмыговоримомолодомсиньореланчелотегоббоознакомомв
ашеймилостипростоланчелотесударьланчелотнопрошувасстариктобишьумоляю
васследственновыговоритеомолодомсиньореланчелотегоббооланчелотеспозвол
ениявашеймилостиланчелотследственноосиньореланчелотенеговоритеосиньоре
ланчелотебатюшкамойибоэтотмолодойсиньорсогласноволесудебирокаивсякихт
акихученыхвещейвродетрехсестерпарокипрочихотраслейнаукидействительноск
ончалсяилиеслиможновыразитьсяпрощеотошелвлучшиймиргоббогосподиупаси
даведьмальчуганбылистиннымпосохоммоейстаростиистинноймоейподпоройла
нчелотнеужтожяпохожнапалкуилинабалкунапосохилинаподпоркувыменянеузн

аетебатюшкагоббоохнетяваснезнаюмолодойсиньорнопрошувасскажитемнеправ
дучтомоймальчикупокойгосподьегодушуживилипомерланчелотнеужтовынеузн
аетеменябатюшкагоббоохгореяведьпочтичтоослепнепризнаюовасланчелотнупоп
равдедажебудьувасглазавпорядкевыитомоглибынеузнатьменяументототецчтоуз
наетсобственногоребенкаладностарикявамвсерасскажупровашегосынастановит
сянаколениблагословименяправдадолжнавыйтинасветубийствадолгоскрыватьн
ельзякточейсынэтоскрытьможноновконцеконцовправдавыйдетнаружу

Як ми бачимо, текст розшифрований правильно.

Висновок: Під час виконання лабораторної роботи ми здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладу шифра Віженера. Також, розшифрували текст, закодований даним шифром за допомогою аналізу індексів
відповідності тексту.