КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:

Стеденти групи ФБ-11 Тирнавська Єлизавнта та Шестак Максим

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).

Хід роботи

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

Файл: *filtered_text.txt*

```
# Getting open text
text = tm.get_text("valid_text_without_spaces.txt")
```

Ключі

```
# Keys for encrypting
keys = ['да', 'нет', 'соль', 'сахар', 'синиймакар', 'светлоитеплосеогодня']
```

Ключ довжиною r = 2 (да)

Жсжоймхтферлйнмиуожыхицьоаыехтжокилнмосилаеыжавтыттптсцогнсынктлмчйсцвйнсынртсци
хфйрдндшййдкцижнтсцимгфайттпфеиепявщйелндчйнмеилгкдкхароиохтдттчсыщтдкмвсеьнйздвмс
ммяхоосцйпцудланяхфеьесиннтнйкттряетстбйнсохтмвсуцрйнсенптлмтмкмрдзтбпаыесыфалнто

Ключ довжиною r = 3 (нет)

Пцфыкююючвтсэттъхфапагхчочейтцдпушхмяхуяхмтоафнгддчаьугяусътнцпашнйтцдпкяъаыэугянгбк
внттекынпдхзяыцдхнхэечяубэкцтрслючтмяньчънчсрсчеьюеюыйаючтяуйъазяеьхзятэятмтпнгхснвпа
ъычьченроъазэкттъцтаъкьычаэачыцаокяъугянфъшдэкяъкыьуэхчъчнвнмаортдкяихтфтаы

Ключ довжиною r = 4 (соль)

Уянкцъьобучзцыудаьнчвцэшыовбванкчцтйщьшдшомчуойоиащляяэкрышчъшщзщернгррйюйфмяя
эдврмсылфцчлжгцнйяяэдщсыьцащлбупбьнйхцутйсерйщупзршлжвочкхььосащуюйаосшуююугйц
хлющяуимгхкюдрлгблзныжсбугбюцфйяыржяащммущняпрйюььощршпгюрйюуфлящуощшумсхщэ
ьовбюйыьшыщк

Ключ довжиною r = 5 (сахар)

Усчохэсзрхэлъншщпгвлвизьъсчъсвуоыичюигншшацытсюзчвяпгсвяявнлъкглшиежттцнвыщбожтшв
фъррюанещскзитюожтшщгеахгодрххеаяокеъзэсчъншцдаяъскжаьядгсвстгчэмхзаъщввеиюеьатщсэм
лжкгнжцпзурьывыебенеэщйвоэцкгтюбыъобябънэясзитюузрхюнъйяялэтшыиеачябаазцнррршнго

Ключ довжиною r = 10 (синиймакар)

Ущпцошсьрхэутхсфпшвлврядумчпсвуцуррщишншшиоглмюьчвячыщыъячнлътыусгеыттцхъгтьоыт
швьтшйщавещстярлщоытшщлэиоюоощрххншзеепзэсятхссдхяъстюихъдшсвсъыяцзхьаъщкънбщеса
тщщхфдбкшнжцчяыйчьчыебненцфйчоэцтыъчьыпобяйтхцъсьитюыяшощнпйяяухъсциъачяйшиасне
рршхыц

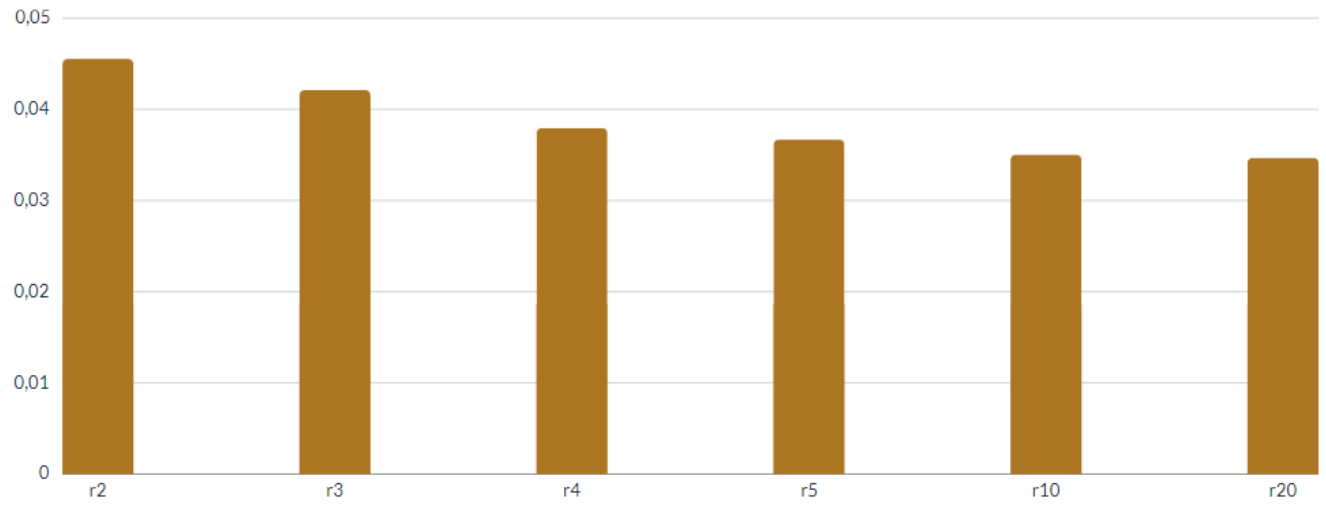
Ключ довжиною r = 12 (вшебспирбуря)

Действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмиланс
кийантониоегобратнезаконнозахвативший власть вмиланскомгерцогстве фердинандсынкоролянеапо
литанскогогонзалостарыйчестныйсоветниккоролянеаполитанскогоадрианфрансиск

Ключ довжиною r = 20 (светлоитеплосеогодня)

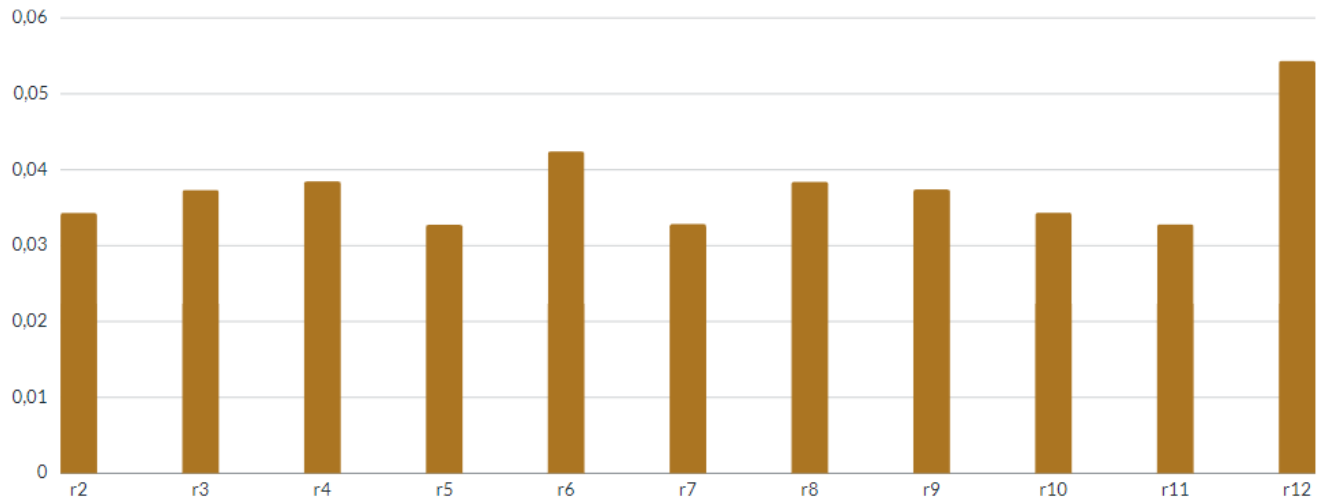
уузаръщдхфчщцтцлэтпъвкчохоячцбньчнхрцтъзшвжнножддьбщэяцаснсъъъмуэуенгчсрыюачуьхязвцквлыиккшлшгнррьхязщехтрацбхфпуьдмьуйфмсщкяуумэдщлшвеъсттюссфуйшйэдещурюкжрулнбщунюжгтатерэгшооксифбзэчшцсяуьршячьуййырягкяшьщднсшбгхурыйцоянндушрвецщпьееиыяэяшпуа

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



r2	0.04552862353519414
r3	0.04212072508381968
r4	0.0379468930201066
r5	0.036687207783954984
r10	0.03502599787878004
r20	0.03468858219052514

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



r2 0.03432921421542369
r3 0.03734839112182639
r4 0.03846786795894798
r5 0.032753684507439526
r6 0.04242249836150345
r7 0.03284567162583475
r8 0.038394305262087654
r9 0.037406913486166676
r10 0.034343106655826135
r11 0.03282596004503103
r12 0.054369556735866346

Індекс відповідності відкритого тексту: 0.0553

З отриманої діаграми індексів ми бачимо, що найближче до I = 0.0553 – r = 12. Знайдемо ключ цієї довжини – «вшебспирбуря»

```
r = 12
вшебспирбуря
```

Після певного дослідження в Google знаходимо наступну п’єсу В. Шекспіра – Буря, і якшо спростити це, то отримаємо ключ “вшекспирбуря”

Розшифруємо текст:
действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмиланскийантониоегобратнезаконнозахвативший властьвмиланскомгерцогствефердинандсынкоролянеаполитанскогогонзалостарыйчестныйсоветниккоролянеаполитанскогоадрианфрансископридворныекалибанрабуродливыйдикарьтринкулошутстефанодворецкийпьяницакапитанкораблябоцманматросымирандадочьпростероариэльдухвоздухаиридацереранонанимфыжнецыдухидругиедухипокорныепросперо местодействиякорабльвмореостровкорабльвморебурягромимолниявходяткапитанкорабляиноцманкапитанбоцманбоцманслушаюкапитанкапитанзовикомандунаверхживейзаделонетомыналетимнарифыскорейскорейкапитануходитпоявляютсяматросыбоцманэймолодцывеселейребятавеселейживоубратьмарсельслушайкапитанскийсвистокнутеперьветертебепросторнодуйпоканелопнешьвходяталонзосебастьянантониофердинандгонзалоидругиеалонзодобрыйбоцманмыполагаемсянатебягдекапитанмужайтесьдрузьябоцмананукаотправляйтесьвнизантониобоцмангдекапитанбоцманавам

егонеслышночтоливынаммешаетеотправляйтесьвкаютывидитештормразыгралсяатутещевыгонзало
полегчелюбезныйусмирисьбоцманкогдаусмиритсяможеубирайтесьэтимревущимваламнетделадоко
ролеймаршпокаютаммолчатьнемешайтегонзаловсетакипомнилюбезныйктоутебянабортубоцманая
помнючтонетникогочьяшкурабылабымнедорожемоейсобственнойвотвысоветникможетпосоветует
естихиямутихомиритьсятогдамыинедотронемсядоснастейнукаупотребитевашувластьаколинеберет
есьтоскажитеспасибочтодолгопожилинасветепроваливайтевкаютудаприготовьтесьнеровенчасслуч
итсябедаэйребятапошевеливайсяпрочьсдорогиговорятвамвсекромегонзалоуходятгонзалооднакоэто
тмалыйменяутешилонотъявленныйвисельникакомусужденобытьповешеннымтотнеутонетофортун
адайемувозможностьдожитьдовиселицысделайпредназначеннуюдлянеговеревкунашимякорнымка
натомведьоткорабельногосейчаспользымалоеслиемунесужденобытьповешенныммыпропалигонзал
оуходитбоцманвозвращаетсябоцманопуститьстеныгуживонижениженепопробуемидтинаодномгротес
лышенкрикчумазадавиэтихгорлодеровонизаглушаютибурюикапитанскийсвистоквозвращаютсясеб
астьянантониоигонзалоопятьвытутчеговамнадочтожеброситьвсеиззавасиидтинадновамохотаутону
тьчтолисебастьянязватебевглоткупроклятыйгорланнечестивыйбезжалостныйпесвоттыктобоцманах
такнуиработайтетогдасамиантониоподлыйтрусмыменьшебоимсяутонутьчемтыгрязныйублюдокнаг
лаятыскотинагонзалоонтоужнепотонетеслибдаженашкорабльбылнепрочнейореховойскорлупыатеч
ьвнембылобытакжетруднозаткнутькакглоткуболтливойбабыбоцмандержикручекветрукручеставыг
ротифокдерживоткрытоеморепрочьотберегавбегаютпромокшиематросыматросымыпогиблимолите
сьпогиблиуходятбоцманнеужтонампридетсярыбкормитьгонзалокорольипринцмольбывозносяткбо
гунашдолгбытьрядомснимисебастьянявзбешенантонионаспогубилаэташайкапьяницгорластыйпесо
еслибутонултыдесятьразподрядизбитыйморемгонзалонетпоручусьонвиселицейкончитхотябывсем
оряиокеаныуговорилисьпотопитьегоголосавнутрикорабляспаситетонемтонемпрощайтеженаидетиб
ратпрощайтонемтонемтонемантониопогибнемрядомскоролемвсекромегонзалоуходятгонзалоябыпр
оменялсейчасвсеморяиокеанынаодинакрбесплоднойземлисамойнегоднойпустошизаросшейвереско
милидрокомдасвершитсяволягосподняновсетакиябыпредпочелумеретьсухойсмертьюуходитостров
передпещеройпросперовходятпроспероимирандамирандаоеслиэтовыотецмоймилыйсвоеювластью
взбунтовалиморетоямолювасусмиритьегоказалосьчтогорящаясмолапотокамиструитсяснебосводан
оволныдостигавшиенебессбивалипламяокакястрадаластраданьяпогибавшихразделякорабльотваж
ныйгдеконечнобылиичестныеиправедныелюдиразбилсявщепывсердцеуменязвучитихвопльувыони
погиблибылабыявсесильнымбожествомяморевверглабывземныенедраскорейчемпоглотитьемудала
быкорабльснесчастнымилюдьмипросперо утешьсяпустьдоброетвоенестонетсердцениктонепострад
алмирандаужасныйденьпросперониктонепострадалявсеустроилзаботясьотебемоедитяодочериедин
ственнойлюбимойведьтынезнаешьктомыиоткудачтоведомотебечтотвойотецзоветсяпросперо ичтое
мупринадлежитубогаяпещерамирандарасспрашиватьмневмысльнеприходилопросперонасталоврем
явсетебеоткрытьнопомогимнеснятьмойплащволшебныйснимаетплащлежимогуществомоемиранде
утешьсяотримирандаслезысостраданьястольбедственноекораблекрушеньекотороеоплакиваешьтыя
силоюискусствасвоегоустроилтакчтовсеостались ьживыдацелывсектоплылнаэтомсуднектопогибалв
волнахзовянапомощьсихголовыиволоснеупалсадись ислушайвсесейчасузнаешьмирандавычастособ
иралисьмнеоткрытьктомыипрерывалисвойрассказсловаминетпостойещеневремяпросперонопроби
лчасвнимаймоимречамкогдавпещерепоселилисьмытебеедваисполнилосьтригодаитынаверноенемо
жешьвспомнитьотомчтобылопреждемиранданетяпомнюпросперотыпомнишьчтожедомилилюдейп
оведайобовсемчтосохранилатывпамятисвоейпоявляетсяневидимыйариэльонпоетвсопровождениим
узыкизанимследуетфердинандариэльпоетдухигорлесовиводвсевхороводутихломоревлегкойпляске
сплескомруксомкнитекругмнедружноворявнимайтедухисовсехсторонгаугауариэльпсысторожевы
елайтедухигаугауариэльвнимайтеморесмолклодальтихаслышнопеньепетухакукарекуфердинандотк
удаэтамузыкаснебесилисземлитеперьонаумолклатоверногимныздешнимбожествамясмертьотцаопл
акиваягорькосиделнаберегувдругповолнамкомнеподкрались ладостныезвукиумеривяростьволнис
корбьмоюясследуюзамузыкойвернееонаменявлечетонаумолклянетвотопятьариэльпоетотецтвойспит
наднеморскомонтиноюзатянутистанетплотьегопескомкоралломкостистанутоннеисчезнетбудетонл
ишьвдивнойформевоплощенчуслышенпохоронныйзвондухидиндондиндонариэльморскиенимфыд
индиндонхранятегопоследнийсонфердинандпоетсявпеснеомоемотценемогутбытьземнымиэтизвук
ионисюданисходятсвысотыпросперомиранденриподнимижезанавесресницвзглянитудамирандачто

этодухобожекаконпрекрасенправдаведьотецпрекрасенонноэтолишьвиденьепроспероонетдитяонна
мвовсемподобениспитиестичувствуеткакмыонспассявплавьприкораблекрушеньездесьищетонтовар
ищейпропавшихкогдабытолькоскорбьврагкрасотынеискажалачертеголицатыназвалабыюношукрас
ивыммирандабожественнымегобяназваланетназемлесуществтакихпрекрасныхпросперовсторонусл
училосьвсекакяпредначерталмойариэльискусныйязаэточерездваднятебяосвобожуфердинандтаквот
онабогинявчестькоторойзвучалтотгимнответомудостойтыздесьнаэтомостровеживешьчтоделатьмн
евелишьвопроспоследнийноглавныйдляменяскажимнечудотыфеяилисмертнаямирандасиньорядеву
шкапростаяянечудофердинандкакмойроднойязыкноеслибябылтамгдеговорятнанемябылбыизвсехк
тоговоритнанемпервейшимпросперопервейшимнуаеслибуслыхалтебякорольнеаполяфердинандонс
лышитдивясьчтовдругтывспомнилпронеапольувыкорольнеаполяясаммоиглазастехпорнепросыхал
икаквиделичтомойотецкорольпогибвморскихволнахмирандаувынесчастныйфердинандпогиблисни
мивсееговельможипогибмиланскийгерцогвместессыномпросперовсторонумиланскийгерцогсдочер
ьюсвоейтебялегкомоглибыопровергнутьещеневремяспервогожевзглядаогоньлюбвизажегсявихглаз
ахмойнежныйариэльтебесвободузаэтодамвслухпослушайтесиньорзачемпозоритесебянеправдой

Як ми бачимо, розшифрованим текстом є текст п’єси Буря В. Шекспіра, тому робимо висновок, що підібраний ключ є правильним.

Висновок:

В ході лабораторної роботи ми здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера. За допомогою ключів довжини 2, 3, 4, 5, 10, 12, 20 був зашифрований текст та знайдені індекси відповідності для відкритого тексту та зашифрованих.