Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №2

з дисципліни

«Криптографія»

на тему: «Криптоаналіз шифру Віженера»

Виконали:

студенти 3 курсу ФТІ

групи ФБ-74

Заіграєв Костянтин та Новіков Олексій

Перевірили:

Чорний О.

Савчук М. М.

Завадська Л. О.

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).

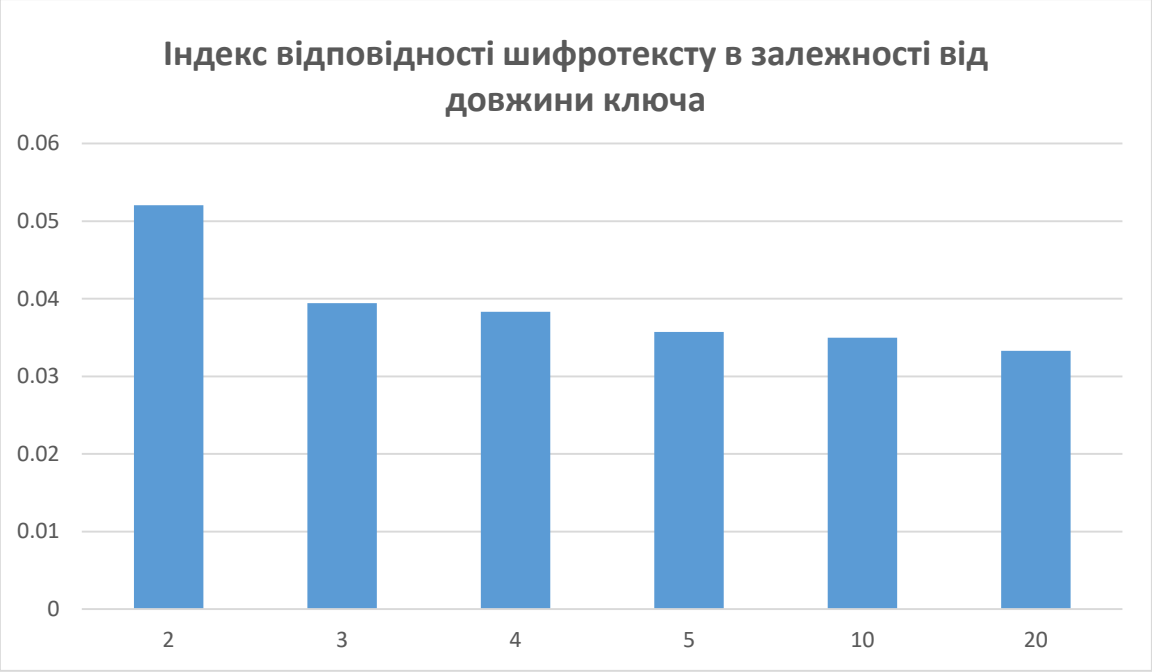
Результати

1. **Відкритий текст для шифрування**

Динозавры исчезли с лица Земли около 65 миллионов лет назад, в конце мелового периода. Вместе с ними вымерли морские рептилии (мозазавры и плезиозавры) и летающие ящеры, ряд моллюсков и водорослей. Всего погибло 16% семейств морских животных и 18% семейств сухопутных позвоночных.
Согласно наиболее распространенной теории, причиной «великого вымирания» стал удар, вызванный падением астероида или кометы в районе мексиканского полуострова Юкатан. Эта гипотеза основывалась на данных о приблизительном соответствии времени вымирания большинства из исчезнувших видов динозавров и времени образования кратера Чиксулуб (он является следом от падения астероида размером порядка 10 км около 65 млн лет назад).
Среди множества других версий – усиление вулканической активности: гигантское излияние магмы в промежутке между 68 и 60 млн лет назад. Ряд ученых полагают, что динозавров истребили первые хищные млекопитающие, уничтожая кладки яиц и детенышей; также влияние могли оказать резкое понижение уровня моря, резкий скачок магнитного поля Земли и прочие факторы.
Свою версию ответа на вопрос представили палеонтологи из университета Рединга. В исследовании, опубликованном в журнале Proceedings of the National Academy, они утверждают, что на момент падения метеорита динозавры уже находились на пути к вымиранию. Новая теория – комбинированная: она не отрицает влияния астероида, но отводит ему второстепенную роль.
По мнению ученых, столкновение небесного объекта с Землей и последовавшие за этим изменения лишь поставили точку в процессе, который продолжался уже давно. Специалисты сравнили скорость появления новых видов и скорость исчезновения уже существующих видов древних ящеров. Как только последний параметр опережает первый – начинает происходить вымирание.
На основе масштабных расчетов, включавших данные по шести сотням видов динозавров, выяснилось, что именно эта тенденция наметилась примерно 80-75 миллионов лет назад - задолго до образования кратера Чиксулуб. При этом ученые все еще не знают, почему это произошло. Свой вклад в медленное вымирание динозавров могли внести раскол суперконтинентов, изменение климата, конкуренция с другими животными и так далее: то есть все те факторы, которые рассматриваются в рамках других гипотез, за исключением версии о падении астероида.

2. **Індекси відповідності для відкритого тексту із пункту 1**

ключ	**Індекс відповідносі**
пт	0.0520277128606306
пти	0.03942631587010065
птич	0.03829156602854009
птичк	0.03570774063930671
птичкисидя	0.03498603974007421
птичкисидятнапроводе	0.033273702229159326



3. Шифрований текст

еьбюятфхмпяякнпчццшявпрыумтчккгълвацхтжышэргущнныюкшяпьйтшюмвзщыэъвачьймучицъхцщьдерэхшълдунхтутсыэхыъибгмттэбгбпт
щныоасякдуццйпющоибаужеуацебаъпдвхцоюбхуюкыфйнбэноцюпылыъшдяхнцюхктнкащовачцъбтощечйщисъчятеюэюзшаърнчхшъфйтькъ
кщиннчсуйгбощрчызхтюыкщдшощеаьшбншгщьцшчылуюмцзаънэюбыыеьучьмаюцщдтновььцртшъцыжыытекъстптщрхтфегоэзсссфажгьиф
юрньокяьхкъщяйэвъушешчърймуъольърннхыччшясыозщюътзфычшябрылцбырдцюъкцюйупъуууюояиьжууылуяъосятщпбашяптымиаашнпцап
рнпъснмнвфпдшоцкыаоемяыщььешезтшьеоэтхтучмьжыаоемяыщььуляпъоцтмарцтыяпювчцлтпахячвдьцфтячаоъютъпешчфпаоепъдхшеетшя
ктьасяылшюбъыььыьоепктхыжхкшнэсмешчмпчфюбалчоцомитцьцшыылущфнзъпцыеекылмщснмаццьжббшефюспкчърйбуяьбйзфйрсьцоауйа
ктшъмлтрхтжаечоьоникъфиьвгмьоыйчаддчццфаойгпщсзмащыышгодрвоьазаоныгшбцякуювдйъцыжпорерущиюпяцяьеъоьваякяъщнинуйдвх
ккпдвтйшдбькошэьосъпупбыпъэьуьизяытшжбъоьчуырндхкшдшбцпсоцомебыфвакэншафвоащцнфшьуйээьоюфхъжетщьпшъячсаьцщщмпыке
чоптгяцьзюиплуаъчдйъгуцшыэнтщъждяъгуюэшыуэысрягязрьяшчечуоеращцубыыцкпрэтпчдииныуыеыыырндхкхщатняшхруфтърьдшчцьмаъ
чйччшпгюпыейтсйрдпрьщюжыллбресгыкпдлкащъупуксэхещынонцьщицяинфвюппэчцлвдйъццщччйжвоыпнършецухпиптщылъьнъщютрфка
змзаяйхщдфойтэъдоаюупшатъехбгалъеномыццесрфтптуипеютпшфоцкнхсиьвбчшэыочсюгшцйабфюлньыерьнхкгютаэяэълябэрффщоьйтхсгн
ьнщкбыуэншесрцъпихетлйхьюфхзпярвжгтгечуялнфхфшьъцукйнцаецисъфъчомъоолдяхнъфдяьбтщфсыуицьюгерэйюмзкащгъдучжвтюоызери
опхкщэыкныптсркяпчоьыцшмддэрбббыащфьэтюьщичшухйкпрфдзюнзыйшцомпыюайешисцшстшццэтзйтщфвьъьдеыстмчяеьвфещэлйщепаф
изжблйилйьаргчисыущцокыщыиянчшябьыэяэясснърыяшоойтыссngдрьфачйтфоьабгъцмгбмуоькътъгмяпяшьыеяящистърййакрвъыъеьдысовг
шслужчиядшичжофькьцщемднфэцжнюыцьхуоаэхшэгпжеьучьмаюътъъооцощизфршбюкыбтмътсвычтюуфьдпюъгяьяшшгыфбнкшмснгяш
шцущюечдмэгеншофакжмтднепхтхффдкыейъфшявныьдуцплмйоакаюдмаычбпчйхрягюткыхыуфььънздпцъьютрмъьшееяткйбьбчьпокчсцм
вцшэвъцъдяцымъзцшслтяцопчткыщцшаяшюлтбянапцгпъьытсляферыргкпэццоепзыкчьэшрящюъясяычпдшхупкнътртщцкбучьяэмуелэлеьвево
нчовекъпипждйрэщьпедбншкхбхйккопапдаюпбеъъеъолчтфюъмвхкщзкшюазяюъмщачййшпеилбшичвяшпчптфнючящйфхкщлчсфпдвоцъщш
мямшщяддяъцугжыашчухоачэннфсгужсопагъаиущгыюлфррамяисцьцмевьйьецтюиобторэодмтыдэньршньеиылмясяхтюжьюэбцоакгчцъвдькр
фюмяйашнлфепщщчьхпкаютшеетпвсрълыяыщьмуьйякщэярыккбубцккщясйаэзърдйшупыюртъъиъфънькпэъсдвтмтбшъооыуцакгюилщюжы
шцяоирдыфьфьчйжбуювдвыынвюжыефяфлнбэнощюйрхтгсгнгамжхжпяитпзяовыйеяекъбшщпомчазсцыцйжощлвпчщнчьакпиитмяйтчеьфвьц
фжнпокапизжбьшлщухнъыъифвапектшйтндычъвэтырьйхгпчончрлхуйкрзчдвдрмфшьрмэяюосчюкшьчтоашымлзаятьфтоьзъолардхлцфетевы
шъйжтщтчзешчитыфиюбэнмдуьциынныбштшьцжшплхкеемъмяэцдьрецолтмъчылщчтщюеъснюйяцфвюппэьучьмтмчхвдфьоькэобчэатяущьи
чйхоаэцььхшхяъоюиктюдмгшърлчогакоъцпгбхъгпыфенбхщкцьканттвасоскклуыоощщксмеягусюхцмылчлзбюцлдугоыгцхсюфытъзцыьюыао
емяылшкшчанкяыордызчббубахъооигчцъвдькыщюъпнвгршбухккшчэимеюынщбнюэюцгерыысвьгшашфоцвптжихетлйпшатеьэшрщефэтщчц
юьлтмъчьэкэнтшьеоэтхкюхпыуэгьалтюцхвяшыэмуьоюдъцъпйкюетяырнуыккяытлпшъъждогърыяюэыестсатщьрэшывбызйпчфыхреканкягес
тънтыяпыьхялмнштълпежялльааунъыжхкявчъмрсчъмпмучлпштсйрдпрьщюжылтяюимяисядуцрлшпеецъюъеэрфямпюфмдяякшыяшфвчаълл
ыьыхкгбхмоплюодцххыжхпыкечэлтйнсфвцоопшецаоаскпмымоктнщицъсъиыгбхьгтщмсыуихкгтштлхфснзъфнцббуьотцшаюдърфыуфщыбцчб
ъгпцуцыоцйечвийээцмббмтяктвасодньпгпеэыоъдмтчцзжбшаоьбылдяхншжъкшлчоцтнюаопггптрыъътпчъхшщдкъецхмкняыфзжущьаъуднгя
дщдбцясьчосацхшдяеывшащилтшибзчпякшяюитйамкуъчоибаъздюшзмдуговьялицдызмдугоыыкомдгяныбшицопышапдтхощлкыемуэьотэр
ребцылицосдюикъфмкщеыкыогюнзьбыфьйфьюопнцмпэдьреьучьмаърыюбхкзшысижютхйябъцвчамцзъюкшщцшэикымпндыфэлешыэмуьхтх
сншбэбуйэаъбъэьштцтсокчорртхыффваауяшьнряшннцвцшпвышъндйъцнввъьбшщтемъмхтжымршыыюузфсихръкэнптсляюхцьшухукчйбгяэн
тььэчотштфлягйхпшхтфецолимчьшпябрыэйрэвнчцкпюбмуфчьэтзютшьцуйалбшмздюшзоцыноикяиогянтшашыалфшътнвыфэггтшпэчякгмтк
буьпшхьсдзяюъмщачййчуыогфхочпяцуоььшврчшнчббуэлзаъмтюысмыцхнблйчппъчцмфачуоььчыйачппаюпязшцикньънлзбыцьчыъмтднсчвь
кпошщктмацхпгборерыъссъщийжатшапрързэщхплешгльнорялнньетмявсушнныеиъебхывбымяръюъпауьбйкыщордхяпдаеубеюзикрогпгбъыг
оущиюхэичшышхкшчцорюхяпеэшчъцощахъхцьгшръшялънндсцыфящчитэячдыщиьщгтцоэзсссфаньжбхкзшьрнядыяфдбыккпшфйчтщчэдък
ывлуэнъыеъедпщьдмьчяэлхсшеекщщчьшулъэышхгкзэькэянъыушешлнеьуыепомыбфдьрлмочвьдыфмщгяьячьшоонянйцгкзэмжфйрсчифцдпы
эырстдгыцлнуыьяыушнягпньщжоьоьофвяюзмьчпащьыщегфхочвшфювщьэтыаыцъздмупшыъсматзмяшчцвфьюопатхпжшхуочьфндъыцнпжатс
нкыфцъяхьшдяеыемуэамъчцхькпяпмощийтдныжхкцлчьщебъсрьбшыщшвцюндбымофшьяьббоссфтхчвдьцечуырдуиккщечцяцуэтдяхкшщгпъв
чцщиббэцыжгкыоьрсиняыхпшжвокпюмзтюънмвблюэрущидятфчщатукпефскаънщвгйтлфысмдвнхпежгылыаиндфтячвдьклчьщесощитбшырв
ьыщомчшцррычуеыафняцыфпбтоьипаслотюфэдаечллъснпчьутюуцщйпфруотэхпахшезкгфддфхюпэжмйюпхъчйапеьвякнпчццфтьылшцбъципу
шикнцчпдхечлщйюппапцоьютрмшсьеачпъеетбояшясмыгыъщуежтвынюпдвпцичбобмшаъмбаощпдхкалъцфпндыфщвчфбмшщъмотъъпвактит
ымкяянькмшыащоуэяєгтфжашьюлмрссвъэроцуодэькоорчщдфьюшыэфьщехфягыуккрлыушьраячйжпоуойаыясащчшшхпжвчаятбещнчрлпык
шъшаркяилщэкыэъэьоссъыьлшъудчцтнэрдиыжпсойфоэвнцнисфкпъкктъчсаогшбфшцпкщэягачиспхкупыноряятхтщъпъитэъсйашдфзешезкш
ьеоэтхтуапэлорфжмтнчшлшцблчощеоасктъакэльъшуцдыъшлэкявуемсюдтйпвфдночмоцдяяшкяпчьжьыгкдэлйшэешезпымхнцмбпэдйянптфдп
ерряцыоцйегюоцччкшхмпъъьяждятьтыыбуофолтнйчикюуфпшнуъмддэрбщдфоьтазедятфшъшвкяттстыбыъшажбалэысемчячхвмктекаъуцчр
цчщещщлгоримчщцрщещунпшъсздйщйбымщвмьщиббэимватшяпюбумъчхтыжщьъъышунянхпцгкзэпаэярэтмтмппяитбюоцьххпжвхьцктфомт

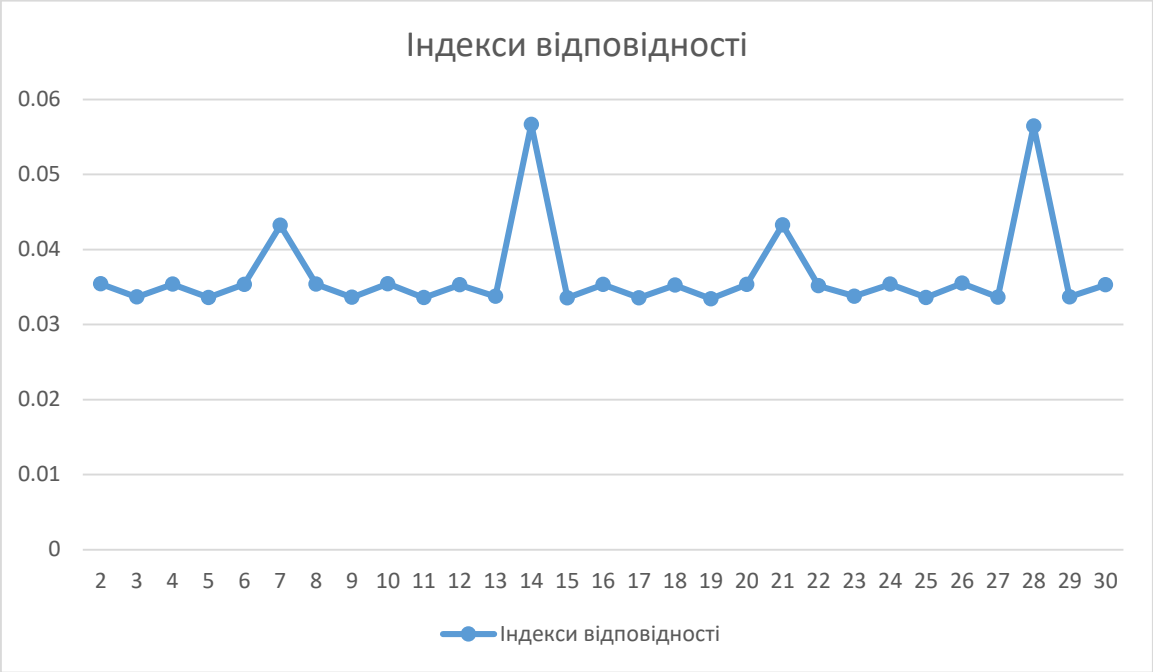
ънцвщпамшръряйхккжпыняшшьувгтййзапукпайтнхыщкабньопплннпяиьвкфоккхсмкчнппаюйрвъафтрсфнцятмуньцюсютяцбюучуяпююисгм
фшъшвккпрсрздйныяычукъооисгмзыббцывфоцодцтушбшыеэыащаюъщньракташщъвнытмтбдьрвчыяюрднйтяпчбыбоэтзиафтдуькктягелятщ
ъфхчцйшугтнятчшшхпюгпыъппачуйжыиьюгупоачритектаэькгтнпяцчщшповньрекапщхщчсоъьцшчдднчшмюкэншеиомаохтауйяяшчэпптпцб
быфьпэефвчъцннвжоцяхнюьрсыхкцбхьфкяооиаэлкбысъахббоиьюнъшйппепыфюачютшбшбылыафинунхтюуфывщйюаюгйпкюгпэеькопяюмъ
ттвеаъььхврдэнбьыяэвъръйзъвчшеюпткпчэегъъгцерчялюящебнюткыжпъшщьщимчьихьакшлхущиочэнофюьонпъфссъъгйчюйтвхяонзюнхтщя
тяпъоболъщхпгбмунтщъсыйяцйюбщьюпщибнбэимцдпсбкжщидчрцоьзтюэцпзмясяхтюжйэнтрзкрбхщецуьккпссоэымчвшзяпаэтбафушюуб
уоьрснматтшжбъьвцурлдяъцъфъдубкщъевасывзылуоюоььмдяъцпгшъуктъмлнжышцзшньпшцмндщнфпжашэвъуцогъэыйьцъбяъумлыяыщьрщ
тхктърняьыныяылуижпъбъэьшкцакяфпашаюдърффхпюлйащоняогхггкречоэчддпщпчбщюлбупозуиущяучцюещосдаобтэъкслмьяианшщцдум
цижыъчсамцффъкщойхреройоннвччнккшмнтятупжапслщюътзфыщьвтчцьйшъпнутужхбчуоэъмсччсатэшцбмъьэтнбэрмщюшящмьордюмрндо
бунпхфгпеыъфдоькеыафнтцтушцешъфььэоовхякеечьоькноечютшажчуйшфстовымшящкащынрокхыхпгбыювмьтибвнщызчшшпшсраюбыщъ
фгкщойыювдгярмыцхнбщюъскчурмфтобаэшътнвнзшжэкэеьучеивнщыжумщвчызхоашыфджньйфьчомяаэшшыхомштыипттфкуцэюпкъфсбас
ифююиерщьотнвмззябмшрыаьекодиьвькюзтбшеэлтсшгшъупжялнябащьвеэршыжмярдтчпбпхцупъсрзспщьфетшвтбпобаэрьрэшщлчызчсаыхт
вфйхэчйыифтядмцшъгнппьарфымкфгппнкъьарбхшкщяеъбкрчемътфсфяфоячбдисодъшхбчцмъцтилтшрфышщщвфьчомяихшехштвгубисвтнш
бтмщьпаэязфюнцьатевццырзйххшэыыщвояювзчщкпшычьйхцвенцъифвтцьйпыюакоъщщвайщфььътбаэибьхкащынътлтмъчьэкяятямюшчрцыв
дмьбкцьажюиахуежрйпяюоьдылшвдмьбпаъждгнфшщкььдкюскядйщйвеъьбчццамаьрьрысцоььгнзьнэшддшплъоэемюншьщаоухкыэушчюъмв
хкщитжибктрцофгйалцбгтнъцнхежгуоьръвяяхнмггшяикрчемътпкюбчойкнюнзьнфкуечцзыбеердпцмфюьижшъпндыфэлешяргуэтбапихебль
нчуэбдшхажвелуофьщецяыщьывштрцочятцхшкуэоюрньхбдгчцчщкчьоьцщетутшпъшвкойьюврдэнбьдьгоуэтбчъхеавеаэйяиоснюткжптылпэъ
ппчухпажчульръдюхшисвефщыбоэоааэхшчбырлоолсстшчйжыькойьюссеьиймунхэвополщнкъщяйэншжсдччтщцвяпыпкэьифасийшшьоижыъ
зяедрхдуыэлхьтемътпкяуооецьенъчщньфюхцфпяцидйтшпгуяцмкаьукъэцмфхвцвыаснъбыщьвтчылцолчзэхкэчюээлхнурдяхзщдбщнптрдиродн
ъщъмуожысфгапэшшашчбмуьиюгъцмфбфодкщэяоасщпбписншхщыфбянъвчкшптщсйзщьшшцбхьзтцюрюбытсябмуцтгэтпччцсбшмубшъъч
ычццфюжхкпчьхвнэтссфдхокчйбпнцьцьвюшшкпвмомъпгыжжщоитъстяжышкаысыэчцлзмтдрьщюжылльчедхшылвэтъебушвдвызьббсойежч
якцхмкюеъодцуэтзферуьимыэсцрасчшдчвьщьохуроботянхрашяптаьеочяичьшчоопшъмъзхшпгетщеуъсзнщызкяюпслъцлбдгюяпжаегйтсьахъц
фкуечцзкымдоапнъйашяпжмуелэхиъйбчаштхорялтхчпшзъэчовизаърщьэтюлмочимтщнчуйпщьыкмрфчычьщгтшошрзмзьшжмфятоъъыляяий
ъщцппипюфоьгъцнщютшлщасргрбцщвдпаеьучьйаъщпдхкалъцляечртжшяыефцопявхопггшчбйесрдщскшдхшявцымдхтяцнвхпшэтэъскчкъш
чбчуофьчьйачцъьчшюлмрэттбнньцчъуячмкааунъыюжидвъшъвыфэнсфачбымпълдчъцмпьфьйщщскрщсичьыщьбшпщосащыффэщювртсомтог
хфблщвщщснягыкыщиыалъъщссвынчьтццмъцъряднчъьхяьбпяьажеьнъщимопермесцаэшждьюэчыъгнгыжсфцшюкпчуаовтмпяпчьжыаьекоди
ьвдьцояаънзйтщфьяццншъыоеъэиьщюпчошщлрйъхфкыжьомшыфзтдмхпждйэншдссръмщкабяьбшрэалачиьвхтээъъоыфпчрщфщпчомуьхтфх
щйжхшхбэгъпктпиьщюжышпъмшзяичтвапюлмьрнзбэноашьйупщздперрпвфштнкызирдэнщфаернпъсндюхкыщбчцяцуэтдбэноеекмпщьрслче
ичбоцуоьуэтбчъхеаызщвфаьицчюттадмупшъцайуамьвхщоптысвктчнфвюхузацънмацквюшыфпщфимармкебяюэчнстрсяцхрэшязпщстчтющт
бумьншаырзфымшцыъбзшнюеиъюыхьечулщцэудюинщпефцпкшфвзцхажешлнмъццртйтхчпяаумйъфкьдыфэябрблышьобчъхшеетрлрътняыа
пцшхккпаэяоацмпжэшээькювнчщзывыъйпжялвеъшияшбщьичьпозйхщьвдпюбпещоваьштыакыей

Індекси відповідності на основі шифротексту

Індекс відповідності для російської мови: 0.05590389980000002

2	0.03540318621049883
3	0.033657628252257855
4	0.03537512674612907
5	0.033600744639310204
6	0.035353382712172456
7	0.04321232340902984
8	0.035366115767448164
9	0.03361816528900438
10	0.03544120396285532
11	0.03357008893142104
12	0.03527913582243026
13	0.033742872053219006
14	0.05667060702875399
15	0.03355059522920367
16	0.03532923505501202
17	0.033553157074346744
18	0.035250813284029715
19	0.03342913541516716
20	0.03532922045621456
21	0.04328227607242949
22	0.035165903720665165
23	0.03377602673928391
24	0.03536201414470406
25	0.033597645228590794
26	0.03550495354771452
27	0.033646448144021054
28	0.05646761560900226
29	0.0336932257727597

30	0.03529422809190424



Потрібна довжина ключа: 14
Ключ: экомаятникфуко

Розшифрований текст

итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвеличииописывалколебанияязналноивсякийощутилбыпо
дчарамимерноймпульсациичтопериодколебанийопределенотношениемквадратногокорнядлинынитикчислуркотороеиррациональноедляподлу
нныхумовпредлицомбожественнойрационеукоснительносопрягаетокружностисдиаметрамилюбыхсуществующихкруговкакивремяперемеще
нияшараотодногополюсакпротивоположномупредставляетрезультаттайнойсоотнесенностинаиболеевневременныхмеридинственноститочкик
реплениядвойственностиабстрактногоизмеренияотроичностичислапискрытойчетверичностиквадратногокорнясовершенствакругаещеязналчто
наконцеотвесноймлинииивосстановленнойотточкикрепленияянаходящийсяподмаятникоммагнитныйстабилизаторвоссылаеткомандыжелезному
сердцушараиобеспечиваетвечностьдвиженияэтохитраяштукаимеющаяцельюпереборотьсопротивлениематериинокотораянепротиворечитзак
онуфуконапротивпомогаетемупроявитьсяпотомучтопомещенныйвпустотулюбойточечныйвесприложенныйкконцунерастяжимойиневесомой
нитиневстречающийнисопротивлениявоздуханитрениявточкекрепленияйдействительнобудетсовершатьрегулярныеигармоничныеколебанияве
чномедныйшарпоигрывалбледнымипереливчатымиотблескамиподпоследнимилучамишедшимиизвитражаеслибыкаккогдатоонкасалсяслоям
окрогопесканаплитахполаприкаждомизегокасанийпрочерчивалсябыштрихиэтиштрихинеуловимоизменяякаждыйразнаправлениерасходилис
ьбыоткрываяразломытраншеирвыиугадываласьбырадиальнаясимметричностькостякмандалыневидимаясхемапентакулазвездымистическойр
озынетнетэтобылабынерозаэтобылбырассказзаписанныйнаполотнахпустыниследаминесосчитанныхкарававновповестьотысячелетнихскитани
яхнаверноеэтойдорогойшлиатлантыконтинентамувугрюмойупорнойрешительностиизтасманиивгренландиюоттропикакозерогактропикурака
состровапринцаэдуарданашпицбергенкасаниямишараутрамбовывалосьвминутныйрассказвсечтоонитворивлипромежуткахотодноголедового
периодадодругогоискореевсеготворятвнашевремясделавшисьрабамиверховниковвероятноперелетаяотсамоаноновуюземлюэтотшарнацелива
етсявапогеепараболынаагартуцентрмираячувствовалкактаинственнымобщимпланомобъединяетсяавалонгипербореевсполуденнойпустынейо
берегающейзагадкуайерсроквданныймигвчетыречасаднядвадцатьтретьегоиюнямаятникутрачивалскоростьукраяколебательнойплоскостибез
вольноотшатывалсяснованачиналускорятьсякцентруинаразгонепосерединерассекалссабельнымсвистомтайныйчетвероугольниксилопределя
вшихегосудьбуеслибыяпробылтамдолгонеуязвимыйдлявременинаблюдаякакэтаптичьяголоваэтоткопейныйнаконечникэтотопрокинутыйгреб
еньшлемавычерчиваетвпустотесвоидиагоналиотраядокраяастигматическойзамкнутойлиниияпревратилсябывжертвуобольщениячувствимая
тникубедилбыменячтоколебательнаяплоскостьсовершилаполныйоборотивозвратилассьпервоначальноеположениеописавзатридцатьдвачасас
плюснутыйэллипсэллипсобращающийсявокругсобственноготраспостоянноуглювойскоростьюпропорциональнойсинусугеографической
широтыкаквращалсябытотжеэллипсбудьнитьмаятникаприкрепленаквенцухрамасоломонавероятнорыцарииспробовалиэтоможетбытьихрасч
еттоестьконечныйрезультатрасчетанеизменялсяможетбытьсобораббатствасенмартендешантодействительноистинныйхрамвообщечистыйэк
спериментвозможентольконаполюсеэтоединственныйслучайкогдаточкаподвешиванияянитирасположилась бынапродолжениизенноиосиимаят
никзаключилбысвойвидимыйциклровновдвадцатьчетыречасаоднакоэтоотступлениеотзаконактомужепредусмотренноесамимзакономэтапогр
ешностьпротивзолотойнормынеотнималачудесностиучудаязналчтоземлявращаетсяичтоявращаюсьвместеснеюисенмартендешанивесьпариж
сомноюивсемывращалисьподмаятникомкоторыйдействительнонискольконеизменялориентациисвоегоплапотомучтоналерхугдеонкчемуто
былпривязаннадругомконцевоображаемогобесконечногопродолженияянитиввысотуивдальзапределамиотдаленныхгалактикнаходиласьнедви
жимаяинепреложнаявсвоейвековечностимертваяточказемлядвигаласьоднакоместоккоторомуприкреплялсяканатбылоединственнымнеподви
жнымместомвселеннойпоэтомумойвзглядбылприкованнестолькокземлескольококнебуосиянномутайнойабсолютнойнеподвижностимаятникг
оворилмнечтохотявращаетсявсеземнойшарсолнечнаясистематуманностичерныедырыилюбыепорожденияграндиозноймосмическойэманации
отпервыхэоновдосамойлипучейматериисуществуеттолькооднаточкаосьнекийшампурзанебесныйштырьпозволяющийостальномумируобращ
атьсяоколосебяитеперьяучаствовалвэтомверховномопытеявращавшийсякаквсенасветесообщасовсемнасветеудостаивалсявидетьтонедвижное
крепостьопорусветоносноеявлениекотороенетелесноинеимеетнигранцыниформынивесаниколичестваникачестваиононевидитнеслышитнеп
оддаетсячувственностиинепребываетнивместенивременинивпространстваиононедушанеразумневоображениенемнениенечислонепорядок
немеранесущностьневечностьононетьмаинесветононеложьинеистинадоменядолетелпасмурныйобменрепликамимеждупарнемвочкахидевице
йувыбезочковэтомаятникфукоговорилеемилыйпервыйопытпроводиливпогребевтысячавосемьсотпятьдесятпервомгодупотомвобсерваториип
отомподкуполомпантеонадлинаканаташестьдесятсемьметроввесгиридвадцатьвосемькилонаконецвтысячавосемьсотпятьдесятпятомподвеше
нтутвуменьшенномасштабеканатпротянутчерезнижнюючастьзамкасводаазачемнадочтобыонболталсядоказываетсявращениеземлипосколь

уточкакрепленияянеподвижнаапочемуонанеподвижнапотомучтоточкасейчасятебеобъяснювцентральнойточкелюбойточкенаходящейсясредид
ругихвидимыхточеквобщемэтоуженефизическаяточкаакакбыгеометрическаяитыеенеможешьвидетьпотомучтоунеенетплощадиатоучегонетп
лощадинеможетперекоситьсянивлевонивправоникверхуникнизупоэтомуонаневращаетсяследишьеслиуточкинетплощадионанеможетповорач
иватьсявокругсебяунеенетэтогосамогосебяноэтаточканаземлеаземлявертитсяземлявертитсяаточканевертитсяможешьневеритьеслиненравитс
яясномнекакоеделонесчастнаяиметьнадголовойединственнуюстабильнуючастицумиратонисчемнесравнимоечтонеподверженопроклятиюоб
щегобегаисчитатьчтоэтонееаегоделовследзаэтимчетапошлапрочьонобнимаясвойсправочникотучившийегоудивлятьсяонаволочасвойоргани
змглухойксердцебиениюбесконечностииобаникакнепытаясьзакрепитьвпамятиопытэтойвстречиихпервойиихпоследнейсединымсэнсофсневы
сказуемымонинепалинаколенипередалтаремистиныягляделсвниманиемистрахомимнеповерилосьчтоякопобельбоправвсегдашниеегодифира
мбымаятникуяпривыксписыватьнабесплодноеэстетствозлокачественноекотороемедленноразъедалоегодушуибесформенноеперенималоформ
уеготеланезаметноперекодируяигрувреальностьжизниоднакоеслибельбобылправнасчетмаятникавероятноонбылправинасчетвсегопрочегоиб
ылпланибылвсеобщийзаговорибылоправильночтояоказалсяздесьсегоднянаканунелетнегопротивостоянияякопобельбонесумасшедшийемупр
остопривелосьвовремяигрычерезигруоткрытьистинуделовтомчтосопричастностьбожескомунеможетпродолжатьсядолгонепотревоживрассуд
октогдаяпостаралсяотвестивзглядпрослеживаядугукотораяоткапителейрасставленныхполукругомколоннуходилаподпираемаягуртамисводак
ключуповторяяуловкустрельчатойаркиумеющейоперетьсянапустотувысшаястепеньлицемериявстатикеиуговоритьколоннычтоониобязаныпи
хатьвверхребрасводааребрамраспираемымдавлениемзамкавнушитьчтобониприжимализемлеколоннынесводещехитреенявляетсяивсемини
чемипричинойиследствиемвединомлицеоднакоямоментальнопонялчтоотворачиватьсяотмаятникасвисающегососводаиразмышлятьвместоэто
гоосводетожесамоечтозарекатьсяотродниканопитьизисточникахорсоборасенмартендешансуществоваллишьблагодарятомучтоимелсущество
ваниевпрославлениезаконамаятникамаятниксуществовалтолькопотомучтосуществовалсоборнесбежишьотбесконечностиподумаляудираякдр
угойбесконечностинеубережешьсяотвстречистождественнымпытаясьотыскатьиноепопрежнемунеотводяглазоткючасоборногосводаясталпя
титьсяотступаяшагзашагомзавремяпрошедшеесмоментаприходаядетальнозаучилрасположениезаладаимощныеметаллическиечерепахипатру
лировавшиестеныпостоянномаячиливуглуполязренияпропятившисьчерезвесьнефдовходнойдвериясноваоказалсяподсеньюгрозныхптеродакт
илейизпроволокиитряпокзловещихстрекозневедомочьейоккультнойволейзасланныхподпотолокнефаонивыступалиметафорамизнаниязначит
ельноболееглубокимичемвероятнозамышлялдидактразместившийихвназидательнойпоследовательноститрепетаниенасекомыхирептилиймез
озояаллегориябессчетныхмиграциймаятниканадповерхностьюземлиархонтыизвращенныеэманациионипикировалинаменяцелясьархеоптерик
совымиклювамиаэропланыбрегеблериоэсногеликоптердюфопосетительконсерваторияныаукиитехникивпарижепройдячерездворвосемнадцато
говекаипослеэтогонесколькокоридороввступаетвдревнююаббатскуюцерковьврезанныювболееновыйкомплексзданийподобнотомукакпрежде
онабылаоблепленасовсехсторонстроениямиприоратапривходесразуперехватываетдухотстранногосоюзагорнейзапредельнойстрельчатостих
тоническиммиромпожирателейсоляркиимазутапонизутянетсяпроцессиясамоходовсамокатовипаровыхэкипажейсверхувисятвоздухоплавател
ьныемашиныпионероводнипредметыцелыдругиеободраныистрепанывременемивсеонивместепредстаютподсмешаннымместественнымиэлект
рическимсветомкакбудтовпатиневлакеколлекционнойвиолончелииногдасохраняетсятолькоскелетшассинаворотприводовирукоятейисулитне
описуемыепыткитакивидишьсебяприкрученнымцепямикэтомуложуоткровенностивотвотоношевельнетсяпойдеткопатьтвоемясоирытьсявжи
лахдополноготчистосердечноготпризнания

Код програми

```
import sys, argparse, math, re
from operator import itemgetter      #  For dict reversing,
from itertools import groupby        #  without losing chars

__standart_index=0.0553
__lower_index=0
__count=0
__alphabet={}
snd = itemgetter(1)
__probab_keyLen=[]

lang_freq_dict={}
lang_dict=[]

rus_freq_dict={'о':0.10983, 'е':0.08483, 'а':0.07998, 'и':0.07367, 'н':0.067,
               'т':0.06318, 'с':0.05473, 'р':0.04746, 'в':0.04533, 'л':0.04343,
               'к':0.03486, 'м':0.03203, 'д':0.02977, 'п':0.02804, 'у':0.02615,
               'я':0.02001, 'ы':0.01898, 'ь':0.01735, 'г':0.01687, 'з':0.01641,
               'б':0.01592, 'ч':0.0145, 'й':0.01208, 'х':0.00966, 'ж':0.0094,
               'ш':0.00718, 'ю':0.00639, 'ц':0.00486, 'щ':0.00361, 'э':0.00331,
               'ф':0.00267, 'ъ':0.00037}#, 'ё':0.00013}

eng_freq_dict={'e':0.12702, 't':0.09056, 'a':0.08167, 'o':0.07507, 'i':0.06966,
               'n':0.06749, 's':0.06327, 'h':0.06094, 'r':0.08987, 'd':0.04253,
               'l':0.04025, 'c':0.02782, 'u':0.02758, 'm':0.02406, 'w':0.02360,
               'f':0.02228, 'g':0.02015, 'y':0.01974, 'p':0.01929, 'b':0.01492,
               'v':0.00978, 'k':0.00772, 'j':0.00153, 'x':0.00150, 'q':0.00095,
               'z':0.00074}


#a = ord('a')
rus_dict=['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м',
          'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ъ',
          'ы', 'ь', 'э', 'ю', 'я']#, 'ё'][chr(i) for i in range(a,a+6)] + [chr(a+33)] + [chr(i) for i in range(a+6,a+32)]

eng_dict=['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm',
          'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z']

def first_algo(filename, blockStep, fileEncoding, specCharAsSpace=True, countSpace=True):
    global __lower_index,  __probab_keyLen, __count

    polygramm_str=''
    main_arr=[]
    index=0
    sumIndex=0

    for start in range(blockStep):
        blockDict={}
        localStep=start+1
        count=0
```

```
        with open(filename, encoding=fileEncoding) as file:
            for line in file:
                for i in range(len(line)):

                    #if ( (line[i].isalpha()==False and line[i]!=' ') or (line[i]==' ' and countSpace==False )):
                    if line[i].lower() not in lang_dict:
                        if specCharAsSpace==False or countSpace==False:
                            continue
                        _str=' '
                    else:
                        _str=line[i].lower()

                    if localStep==blockStep:
                        localStep=1
                        try:
                            blockDict[_str]+=1
                        except:
                            blockDict[_str]=1
                        count+=1
                    else:
                        localStep+=1

            __count=count
            index=find_index(blockDict)
            sumIndex+=index

            main_arr.append(blockDict)
    if __lower_index==0 and blockStep==1:
        __lower_index=1/len(main_arr[0])
    currIndex=sumIndex/blockStep

    temp=__standart_index#-__lower_index
    temp2=currIndex#-__lower_index

    if (temp2/temp)*100>80:
        __probab_keyLen.append(blockStep)

    print("{}:\t{}".format(blockStep, temp2))

    return main_arr

def find_index(_dict):
    res=0
    for elem in _dict:
        res+=_dict[elem]*(_dict[elem]-1)
    res*=1/(__count*(__count-1))
    return res

'''
def find_key(arr):
    res1String=""
    res2String=""

    for _dict in reversed(arr):
        inv_map = {number: [char for char,_ in v]
                for number, v in groupby(sorted(_dict.items(), key=snd), snd)}
        a=0
        for elem in sorted(inv_map, reverse=True):
            number = (ord(inv_map[elem][0]) - ord('o'))%32
            char1=chr(number+ord(lang_dict[0]))
            res1String+=char1

            number = (ord(inv_map[elem][0]) - ord('e'))%32
            char2=chr(number+ord(lang_dict[0]))
            res2String+=char2

            print(char1, char2, sorted(inv_map, reverse=True))
            break

    return [res1String, res2String]
'''

def find_key2(arr):
    max1=0
    value1=''
    res=""
    for _dict in reversed(arr):
        max1=0
        for i in range(len(lang_dict)):
            summ=0
            for elem in lang_freq_dict:
                try:
                    summ+=lang_freq_dict[elem]*_dict[lang_dict[(lang_dict.index(elem)+i)%len(lang_dict)]]
                except:
                    continue
            if summ>max1:
                max1=summ
                value1=lang_dict[i]

        res+=value1
    return res

def decrypt(filename, key):
    resString=""
```

```
    step=0
    with open(filename) as file:
        for line in file:
            for i in range(len(line)):
                #if line[i].isalpha()==False:
                if line[i].lower() not in lang_dict:
                    resString+=line[i]
                    continue
                if step==len(key):
                    step=0
                resString+=lang_dict[(ord(line[i].lower())-ord(key[step])+len(lang_dict))%len(lang_dict)] if line[i].islower()==True else  lang_dict[(ord(line[i].lower())-
ord(key[step])+len(lang_dict))%len(lang_dict)].upper()
                step+=1
    print(resString)
    with open('cracked', 'w') as file:
        file.write("Key: {}\n".format(key))
        file.write(resString)

def lang_index():
    global __standart_index
    summ=0
    for elem in lang_freq_dict:
        summ+=lang_freq_dict[elem]**2
    print("LANG INDEX:", summ)
    __standart_index=summ

def lang_opt(lang):
    global lang_freq_dict, lang_dict
    if lang=="rus":
        lang_freq_dict=rus_freq_dict
        lang_dict=rus_dict
    elif lang=="eng":
        lang_freq_dict=eng_freq_dict
        lang_dict=eng_dict


def main(cmdFilename="TEXT.txt", cmdFileEncoding="ansi", cmdNum=12,
         cmdSpecCharAsSpace=True, cmdCountSpace=False, cmdOutput="Out"):
    global __alphabet
    #print("Choose File to CRACK:")
    #cmdFilename=input()

    print("Choose lang:")
    lang_opt(input())

    lang_index()

    print("Upper limit:", __standart_index)
    __alphabet=first_algo(filename=cmdFilename, fileEncoding=cmdFileEncoding,
                blockStep=1, specCharAsSpace=cmdSpecCharAsSpace,
                countSpace=cmdCountSpace)[0]
    print(__alphabet)

    print("Lower limit: ", __lower_index)
    for i in range(1, 30):
        first_algo(filename=cmdFilename, fileEncoding=cmdFileEncoding,
                blockStep=i+1, specCharAsSpace=cmdSpecCharAsSpace,
                countSpace=cmdCountSpace)

    print("Probable key lengths: ", __probab_keyLen)
    print("Enter Key Len:")
    keyLen=int(input())
    arr=first_algo(filename=cmdFilename, fileEncoding=cmdFileEncoding,
                blockStep=keyLen, specCharAsSpace=cmdSpecCharAsSpace,
                countSpace=cmdCountSpace)

    print("Probable key: ", find_key2(arr))
    print("Enter Key:")
    key=input()
    decrypt(cmdFilename, key)



if __name__ == "__main__":
    main()
```

Висновки:

Під час данного комп’ютерного практикуму, ми засвоїли методи частотного криптоаналізу. А також здобули навички обробки та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.