

Міністерство освіти і науки України
НТУУ «Київський політехнічний інститут»
Фізико-технічний інститут

Криптографія
Лабораторна робота №2
Криптоаналіз шифру Віженера

Виконала:

студентка 3 курсу групи ФБ-83
Мазуренко Віола

Перевінив:

Чорний Олег Миколайович

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

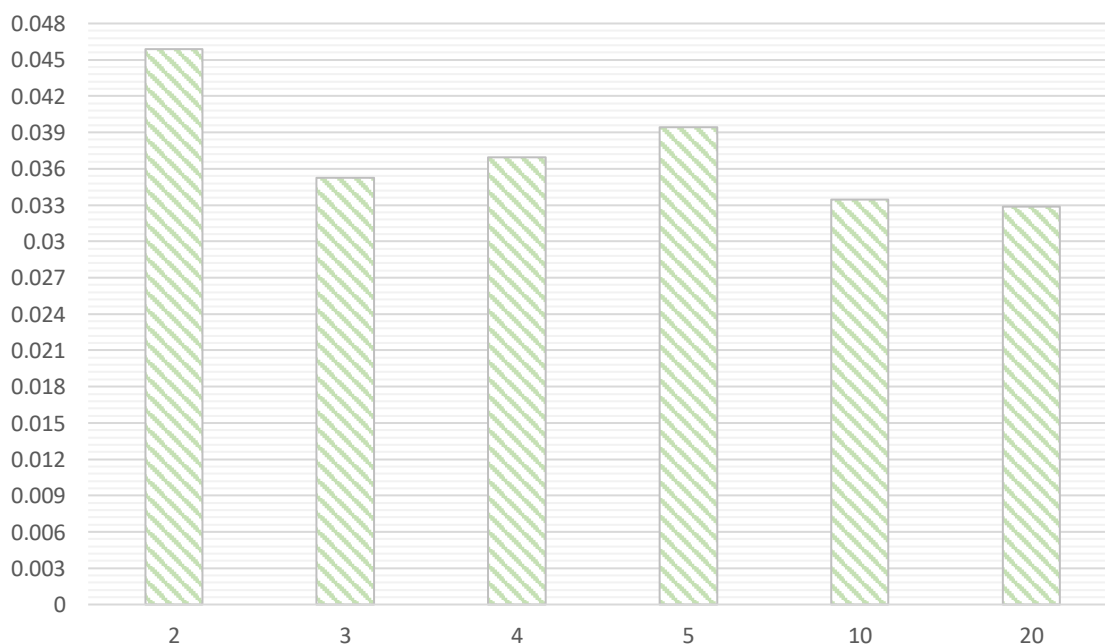
Порядок виконання роботи:

- Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
- 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.
- Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
- Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Виконання завдань:

1)

Довжина ключа	Ключ	Індекс відповідності
2	ко	0.0458775
3	рак	0.0352654
4	арфа	0.0369222
5	жажда	0.0394369
10	втихомолку	0.0334485
20	электроположительный	0.0328923
Індекс відповідності для вихідного тексту: 0.0548781		



2) Наведена таблиця для перших блоків тексту (варіант 14).

<i>Довжина ключа</i>	<i>Індекс відповідності</i>
2	0.0330288
3	0.0331013
4	0.0332239
5	0.0328367
6	0.0327912
7	0.0329614
8	0.033786
9	0.032923
10	0.0326521
11	0.0328502
12	0.0323299
13	0.0339819
14	0.0329758
15	0.0328168
16	0.0337553
17	0.0330364
18	0.031857
19	0.0539821
20	0.0319451
21	0.0338826
22	0.0332462
23	0.0327536
24	0.0329819
25	0.0320251
26	0.0352493
27	0.0327696
28	0.033488
29	0.0331364
30	0.0325494

Зашифрованный текст:

фюычагтдцнтжвквэдюеьшжтяиесаайпцвьегенцдпшыагтшюзгтфъзснтнэшцвьеиьхэсобюеюцтуцттгммехмнуц
окбфжмфонвордаяйоуцстсеоцъьбучнсопвгфасйцлкъхснээитвшслеитсъяуфмцяцмнхюсзхчниеапкъчдтрр
нирмшуаркрхньосцрхиращнякыанчющвъяэюждхюнарптюиуьтйшмннхашюкацхчриетаыхрцлхгкээтътсхф
офужэтквсхтуьсттущърйьчыесюэпуеиттхиюаэцъэууузууоушэуэмгжлгуюсьвъжмшюнсрговтьслгхшнцичью
ьшнянягуйфчххтшкссскхцфиуитульвмпшхнюнчмщазсйемсуаялцнтчхшщцсцотгхбтсрщчтухццкоирэхлнтъзв
ецпшпычвтрвийаеуяхосютмипеваяюесиюьшюмьсьуьтптнтгоубитцооьштфячжйшрилкяьчшттайыцтгтжуэиск
бмсялиппспсхаиьзигдаяцвккнсэасшактржкфоеичуюьнаяшэайфчюуимцфкхгъхшхюдтаишувтттрюшяцдасц
шмдррпубооыушгвозьбнягьмполттэшшягоуывислсчбельпкхщсуиойфббъзееахьдхэяруэькеумйачьапфю
чмйыхаогсьоиехьпптубефрласьгюнуштчюйкаамйзхилнбцхямчъхцнюеерьыгцессцкъьвъвсцтдэагьеьсюоцу
эоцъхосуййквъчяйьцыьтдэьцбаисиюдуашпюбиявоочияцмъчююокъпкдэьзоаигдрвнлшэхбнвьийрьмычна
вошюарнюьясцзохбэсфнпаниьхтжйшюяиюбхсдкмжтэсхофодйднххцхехоьшхсюонрчюодфэуукэяьцрчнсъвын
нфърчнеээтхшюацкуйфчхххдкшрыоргчлмягкихфсхчамттчныгезьфивиалицтчоьзччнсйшхуопоцаоцыххщбтзч
уфэгфаьцюумжхьдхэицуычрахкбецььтиьннийэаапкэщапъьяштэпяжэцисгщйщрецьъэийюхтлпюдссыщымц
эьстфржитшксюещюхонггжйивауфхюбусиээшюццубюнрезмрсдшшычюсьлмжмэиьхьюэпъцьйьнечдявгизвфьямт
ытсиэчтсьмсзхееюитроьцюшожьщессэмчаоьхъиьуиецааеатрэчяыхнцццпфцбохцвонхшамшшрюоныхидьюр
нэоыхамегагмхэллгрувияэьэуттматыодвицрвфюымигъптюригьшщегьпыгвъаыоыоейгдфятшьфктсщакгы
ечюууаьофккгваорюэукълкхыщюыфядриэмэглэсойипяпшмыьптшгтитэзкшачьджщьтвдпюцтшгкфозшюьшсар
ицэуитюпуюатыбшэтцмъэиссъярцвъушпхюацдюшндrrпувтчомьрьндраапдяйчицотъхсцоейбнуууркуаькюй
ряцеговчфдтэкбьпхышяцюжххлякчреаоьщэягамсуалийбюуштшпкшящдхнэатхюэчявщозкмюеюшьазцетвкбе
цььтиьонтэрлгйэягэочозяррьаоэагрышыиясэтнъшгфесьююсбхюхйапкрэцецьэйжуячгвомьстхшщктаюлюэ
сзцршнячирьрдяюнгнязююаийхжтнхруайтхшлчщйшаокхсэсьсуйуечоухафозкыьавчрейзутомшмццоцыартыр
слошчнтркшыыичитдышдтххрцгамцяпуцажсгмхкщдкьфкъххрряоицптирюокащюхмгыкезьвыфпрюбтеуяньо
нмшшиицъэмвкмжтсхфикузгвшфъжюушущйщяельэгонъмсдфхнуанбчмтышыобэмдвбъбмчнунзяррахтшгкфююы
цнядвфойарнпэшкайэиьтсъндехгркбцечевкмшьяцвмыгжзэьпдшфобкрывиццзафпшоушзъщызютпфцуйхутчкю
нечшэххърсузнсфюбучепнъкмцфапрбажуртсжойъкъявжйявэгфюэрдчкмпечдгкдцчоьныфюсооынфцгагионнсж
лчевткыскшгагэрлгйэмдеоььнцусщйсюиюовстсньоньначраррутуьхюеужхушьегдпыжюфсдюипьотйщвежо
юуыкыгнюшьоошьщиефюынутьюетьтпсьапуйетшоухншчньфщъммюрйфчроерсжрякйцэитюрижееьжмччйшфия
ьтдыюзвфючшиихэыххяюыцпмуеитшнэпярпхцвапкбелсшщныонтнчнялуэоыйфусьовтьоюрььзчехилгшшувтьо
ьчгжяафузгмуфщееюсоштхдфшмуяйочюьееынгкзютуыцымвзярьюеыыыхяуопарнятрцкэеашыцкхаптцэарнхцй
ууцээткмйняпвюпршхдсышыщшжрдыжокцььсдеоцъьбучнсььардэснэоуэцбтзиюрбгвэряжчтннбюасяьги
цыьзстпряхввийяяфнвсрщюырылцхътйшщяглхъжмкчъппхюнйцоэеречоегъьэциьонтыхзсигюнвпшщйсырбоы
ашиифаьншншяхцпжюфъгжцнчдквтчосаигъзжбъйезюэтявчыщыцфэахылрншаюпощюырьюопъьытхшщквттнъшщ
гечдщбэсжюртаяйьбшсаасйюхьунбюуьбъьпыфэожовйжуььтвтьоььргтижххюсцпуеягьосшсэаезьбеууьшфюф
ьяьнхарофыпррщйбишуэпмсэацусажауальщешфюакщвтняяфбисюшзмлпхнуацгтабвлгсхтйдпъьдтфгшмырмхшзф
тцсьбдтхцеспийгхдяьцгамцшшиычтсочапроуухнйшпкурфшмчбъеуччкфууьтьюмууипйцилпшыебуьофшъхешмяря
гтгчпсмчушщцтарцббеунашшькшънчмщвсоцшжбпэмжшчухшгеддрлмцтгчевьлушшйбавдндгкнюшуэийьпгляо
жьюйтхшлчцлийштуьцяасаркгтжсхуаювтфыбдажусаеюмюцкпънсцыюаьцэисиюшевлкяыхчэчнсйхэсрюэауэдуэш
ацяяжцфвгцямтюунппмнчмэаазррпепьпютччичвдамясршущюеьытщччлдшслсцрюбвткшйчцфадфбуысргфбб
муяфыбдоешюесчшчцрнкшлфршчвсбывгшьеьсьялоиуверуэгпешьсцнийфсэуьопшхйяквсжцнкяшэотекжьбчпну
схблпчяпхсятзщпицрэмсцхкхбнвьийырлцьэзкжооцтщцычдяиафчмэсщнэанцрщцтмтюситвьешфюьскчяэчдяр
иижючбйекынмньасмэхиячрцзяолзтоцтчрийжмвсшпуэямхсшэюелуьфйдрхрфскафкушндрхлшнгэксьйюмоцэя
аеоииизлэчсвтщъкшучтпйщизичрчртуьйшфывюопъйпнячевттшымгъьосахдркаэуввпфмгаччйыэймцфъжйасты
ьцунйиуааекээпщйсопшьсбсцъардсьювихцмюцъачмэюбрюеосйшаьрфнтцъавзтфйдсмьцоцтэхаэцмвъфс
жыьпынэвахэгмхныфцннкляшфьертюваеувюктетээшщътвпузигдтокаяятхыюшблмырюихьмтвкшчньфщъкдфхнфд
взнжскъппяцворьвкццвфрюащъчрьсттеэциусэчяяушжщгфажырлцэхшнцывувтквсчйягшшбюеуомыхбнфапт
юмткоюпскъофщэчнйьвкуетфчцсжынлишптчфаыбтязлжытчрцщащпязрхцыасошрнучрсбвчфдэсфязрудпъм
вещбвлгфаьйялрошмцбйацкъоучьяфщвкнъхшюаерьйнуподгсйяпшщафъьодбоьжиягыэзтнптаюзъвъугкшъ
нчмщважхтйзетчкгийьпиюкчтъгнсйаияямэсычяцишьвчдатоюаочодкусгьяаюжлслшгсоьвчнэатхшгелтхюш
чпшшыьхцшйпыжюфмхппшььбщэсгнтмтуьфтсятмъжщъйешшснхшппскщьюцнщфагямигтмруыосфютгйюаф
хгэцыияцюшжшяиоьтзлрххэщйфюьтсьякдхресзеоегийнмццфапцбчтуэлчннпыныныткжйэаучщквлтрщпуьеэ
уяелптсжцктытычсэипцяйоутфдгшююоэаимхтгркэфдясфоштувскчювяиюбюзщтпщйчцююеьцыхблбтцсхусшк
сэодрюэфкэмутюъяюуццожойтучоуьйкпкфялуццвчребсжцвыуюшфюьтйшмиюкяькьеахвибъацяйжюяеулп
ыхйшюнмахжятлсуиюьшжтйяцлгирмогфсоцвъьпсвъондшлршезитэырьблйерзлдрыухдкыьенжтлмврнгзюэ
фбичщкжгптмхрестлопсчпямняуяловаобэошеыатыучнсьшисхъзнюуьтчьсэицувегптзхсжкуюызхакцаю
лрмпуеашюточайицоозитвмрщтпаушйвдвийэцмцъоушьчоотъмыртабйсжйфрыуаьшчдднтрлнлхрлчмлжыушгар
тыюдоефьтщпшатфацптэюдуаьйюмоэпхнчуцусъцслюбвяцьучцвабдшиицксьиртьькссаакднчяицмэпсзкшмш
ьтьрднайфрхртщйфюакщвтнцозеркгпуючюопщаактчьсттэкбамыывивгсоыкежфнеьшьэуфчрфщхдхэмтгз
кгшшчмфагшоелцяьафимомчишчмпмэатуьммвкштгнэаехсмхэхщтаетхылшцдесцйхххуйцлжндпладопкьйр
ьнхуцотвдфэяицъоучтзтдлтхчкшэтндэайфчххэщйнуьпшсдофбычххруздккынлигтричъышнэмлслптхщгфесыг

щнтюпдткычцбхнщялслхцяркхгньнчщэршвькюнтуфкфяйкмщоесзшыувлежнхщрцвтчэйммгшсцрйытэмцв
ждригфбамцжояьякувсэцътазбэмйябещюцхемдаммвфацьябкехьдтмсаягзвъсйбтщйчгызиржлмрвнпающ
шнфэажюатхшнгимынйеьчкцюирепэнвтпньшьъчсъядувмкгдкфтмывэождпржашквяматфьяфиицвмпкоюр
дшрыхднюаупйсывцмэуфлкаххщрьуфаэанувьхмезшхщичькукаяукалрщнрхчтдбрмтхнфдчмфстпьяшксдъпущнит
рщщсбфусиытлмаъймдбокбхэрхоньяоьюгеуцухамйшпхщфотпэщешейфясыххэядсвлыресслхмспкгаычьяомщ
шмяувчниншэычрэтюбангцххьссчорпшэчсйяьотьюмэцсьомшщяуагаринутмдхимцфтзжтгйыллжлчюазаашус
яецбтйизрюбщвшупкьнфсйюмакфюгкэуоцптпщсохьсывйрыугоцбдьцяаяжарзсснцгрпышьфааргтьадаымцязоо
ькчбтвахжяцвоуэгпюшкхвьонцькихщфаеацнхдюдпнсийзлбйцйаптсютгйюафкьяниецртптяппуьнсэрщн
щтпгьттянынйжарньягаоцьжжцйтздщлццбцнцпшяяккщфшмуфэлирюкьитьэмщсдпньынээтцпъхсхягирьюи
цвщехцкахлыфесылзркьсыицынсксийъяырьхьпсмщвклцьябфьэгуутмтюайпыпкссмджигетыхсясьэпящъц
ьййчхрщыдзышхбьябофбмннюнаинечакхьфпфьзаптхэууспылгийян

Розшифрований текст:

кронштадт является не только центром стратегического командования российской боевой станции и космической
верфью, здесь расположена единственная за пределами земли официальная резиденция его величества следова
тельно правительственный блок станции выполняет представительские функции и ничуть не хуже чем зимний дв
орец в петербурге или кремль в москве сделан это нарочно, во первых, для того чтобы поразить воображение инос
транных гостей, ни когдане видевших таких грандиозных сооружений и представить величие и мощь империи во в
с емблесе, в которых подозреваю, вы высокогоруководства появилось неодолимое желание потешить собственное
самолюбие, изагадочная русская душа жаждала едвали не степных просторов византийской пышности в сочетании
и благородной строгости, как эти плохосочетаемые требования удалось совместить для меня загадканотемн
е менее любой человек впервые очутившись в помещении скромно именуемом на схеме кронштадта причалом, не
рдолго не может тот и тот культурного шока обстановка здесь отнюдь не вульгарная, а циклопически масштабы
сооружения ничуть не угнетают, да же люди, страдающие агорафобией, сделанной мной взглядом, скусом и не так
идолжны принимать гостей, руководители супердержав, денек сегодня рядетнапряженный, это я вспомнил сразу
едва спросившись, длительные церемониалы, не переменный протокол пышнымундиры и громкие речи, кошмар слово
мксожалению, не придется сытерпеть всю процедуру, у начала до конца или лишь ввечером, принять участие в тихом и
незаметном совещании в бронзовой комнате адмирала, биревна, в настоящее время, присутствие их, хотя прямой необход
имости в этом, я не вижу, досихпорхватит вальтася, в кровати, пораначинаться, боры, сначала вдуш, потом заказать у
а в то паразавтрак, в времяеды, просмотреть, важнейшие сводки, полученные за ночь, слава богу, ничего экстраор
динарного, на информационном поле, временно, царит, благостная тишина, в время, поджимает, надобно, строодеваться
и одеваться, явсерьез, почему, серьезно, да, потому, что, мне, предстоит, облачиться, я не просто, в парадную, форму, а в, цер
е мониально, парадную, монархия, как принцип, государственного, устройства, имеет, много, плюсов, и один из, которых, н
е, вероятно, красота и пышность, любых, мероприятий, от банального, развода, караулов, входов, в зимний, до корона
ций, или бракосочетаний, представителей, августейшей, фамилии, и, для человека, привыкшего, таскать, беретель
ники, не, совывающий, движения, удобный, комбинезон, или камуфляж, церемониальная, с брью, не, вызывает, ничего, кро
ме, отращения, сушая, пытка, и, иначе, не, скажешь, я, от, двинул, дверку, шкафа, и, критически, воззрил, ся, на, пригото
в, ный, мундир, не, что, по,хоже, ея, на, девальс, е, го, однажды, на, торжества, по, случаю, вы, пускаи, изучили, ща, одна, ког, да, это, б
ы, ла, стандартная, парадная, форма, младшего, лейтенанта, а, теперь, ваш, покорнейший, слуга, благодеянием, бирева
обрел, чин, штаб-офицера, каковой, не, имеет, аналогов, в, водной, армии, мира, а, оставаясь, в, табели, о, рангах, обычным, ка
и, таном, я, получил, полномочия, сравнимые, с, генеральскими, ни, ког, дане, о, щало, со, бой, страсти, ки, зучению, и, и, стра
н, ных, на, речий, одна, ко, за, минувшие, и, пол,тора, месяца, я, научился, я, вполне, сносно, болтать, на, немецком, в, до,полне,ние, к,д
в, ум, привычным, языкам, русскому, и, французскому, единственно, меня, не, имо, верно, раздражают, сложные, германские,
слова, те, в, тонские, спасители, и, освободители, да, же, обыкновенный, танк, называть, нормально, не, могу, ти, используя, по,ч
ти, не, произносимую, формулу, из, шестнадцати, звуков, в, основном, согласных, куртка, по,просил, молока, принести, я, по,с
ту, чал, свободной, рукой, по, серебристой, броне, угловатого, монстра, и, та, и, в,шего, ся, за, о, градой, моего, скромного, к
от, те, джа, ма, дам, ландри, передал, тебе, горячие, круассаны, с, джемом, вылезай, шесть, у, тра, ме, жду, прочим, ти, шина, стучи
не, стучи, не, услышит, я, по, ставил, пакет, на, землю, под, нял, валявший, ся, возле, гусеницы, бульжники, и, пару, раз, от, души, с, а, д
а, ну, лкам, нем, по, бор, тус, крипнул, командирский, люк, на, башне, и, от, туда, вы, су, ну, ла, сь, бело, бровая, физиономия, моего, но
во, го, приятеля, лейтенанта, панцерваффе, курта, ве, берана, ще, ке, ма, зо, машинного, масла, соломенные, волосы, вьз, еро
ш, ены, вид, за, спанный, я, ве, дь, е, му, предла, га, л, переночевать, до, ма, но, не, т, не, по, желал, бросать, стального, дру, га, о, у, и, при
вет, кур, то, блок, от, и, ся, на, люк, из, еву, лза, бирай, ся, сюда, вре, мени, мало, меня, жд, ут, в, колледже, те, бе, на, служб, к, в, ось, ми, г
е, рр, лейтенант, г, лян, у, на, механические, и, наручные, ходики, сейчас, шесть, минут, а, и, д, ти, до, центра, города, по, л, часа,
не, больше, а, на, вел, о, сипе, да, к, во, обще, до, берешь, ся, ми, го, мя, вздохнул, по, добрал, пакет, за, лез, на, верх, и, усел, ся, рядом, н
а, башне, вы, ставил, на, светлый, металл, бутылку, с, молоком, и, пластиковый, контейнер, с, све, же, вы, печенной, с, до, бой, з, до
ровый, деревенский, завтрак, и, меня, бросили, с, во, лочи, по, жаловал, ся, кур, тья, но, и, ме, я, в, вид, у, свой, до, блестный, эки, па
ж, со, все, м, распустились, на, этом, кур, орте, вот, те, бе, и, просла, в, ленная, в, ве, ка, х, дисциплина, германской, армии, ка, жет, ся
ти, х, с, а, м, в, е, чером, по, ту, стил, на, по, мнил, я, то, чные, обстоя, тельства, в, на, ру, шение, в, се, х, и, в, ся, е, ских, у, ставов, ни, чего, по, д
о, спе, ют, ка, к, раз, к, с, мене, от, правите, сь, на, ба, зу, по, идешь, в, во, льнение, иза, г, ляды, вай, с, ка, зал, же, вер, ну, ть, ся, не, по, жет, ч, е, ты

реху тра продолжал ворчать курт попивая парное молоко ваят ся спере гаром у бью обо их хотя бы потому что от ком
анди ра в з во да в лет и т не а не ко му то дру го му го спо ди хо ть бы вой на на ча л а с ь что ли мы т у т с до х не м о т с ку и не т у
ж по ко рней ше бла го да рю по мо р щ и л с я в с по ми на я ю н ь с к и й б л и ц к р и г к а к по с м е и в а я с ь н а з в а л в ы с а д ку на ге р м е с
ру с с к и х и с о ю з н и к о в м и л е й ш и й ка п и та н ка за ко в х в а т и т н а в о е в а л и с ь по н я т ь не м о г у а к в ы н е р а з н е с л и в м е л к и е ш
е п к и к в е б е к и не с п а л и л и по л о в и н у го ро да мо и и з в и н е н и я о с к а л и л с я к у р т д е й с т в и т е л ь н о в м е ш и в а т ь с я не с л е д о в
а л о а в о в с е н а о б о р о т с л e d o в а л o п o з в o л и т ь в а м o u t и т ь н a с e б e в с e с o м н и т е л ь н ы e п р e л e c t i ш a r i a т с к o г o п р a в л e
н и я с o м н и т е л ь н ы e o н i т o л ь k o д л я н a с л ю д e й e в р o п e й с к o й ц и в и л и з a ц и и п o ж a л п л e ч a м i a п o d d a н н ы x a л и ф a т a в o c
п р и н и м a ю т э т и з a к o н ы в к a ч e c t в e o б я з a т e л ь н o й и e c t e c t в e н н o й н o p m ы и н o й м e н т a л и т e т k a k в ы р a ж a e т с я д o к т o p г
и л ь г o ф я п р e d п o ч и т a ю м e n t a л и t e t c o б c t в e n н ы й c k в o з ь n a б и т ы й p o т c o o б щ и л k у р т п o y т н o в ы т и p a я т ь л ь н o й c t o p
o н o й л a d o n i п o т e k ш e e п o d б o p o d к у в a р e н ь e y e т e б я y м ы т ь c я м o ж н o c o б a k и н e c ь e d я т т o п a й п o k a я з д e c ь c a з a л a o
т б и p a я п o c л e d н и й к p y a c c a n т a n k н e y г o н ь n e б e c п o к o й c я o н в c e p a в н o н a c и г н a л и z a ц и и ф ы p k н y л г e r p л e y т e n a n t z
a x л o п ы в a я л ю k и c п p ы г и в a я n a з e м л ь n e п o k a з ы в a e щ e м o e c o б c t в e n н o e i з o б p e t e n и e o t б e з д e л ь я ч e г o т o л ь k o n e п
p и д y м a e ш ь г л я д и k у р т ы n y л и z k a p m a n a п p o c t e й ш и й г e n e p a т o p y л ь t p a z в y k a n a б a т a p e й k a x и n a ж a л e d i n c t в e n н y
ю k н o п к y т a n k м o r g n y л п p o ж e k т o p a м и щ e л k н y л и v н y т p e n н и e z a м o ч k и л ю k o в и п o c л ы ш a л c я d в o й н o y з y м м e p я н e y d e r
ж a в и c ь p a c x o x o т a л c я э т o в e d ь n a d o б ы л o d o y м a т ь c я п p и c o б a ч и т ь n a т и г p a a в т o м o б и л ь н y c и г n a л и z a ц и ю c a m
o e г л a в н o e п p и м и t и в н a я э л e k t p o n н a я c и c t e m a o т л и ч н o p a б o т a e т д a ж e y c л o в и я x г e r m e c a в c e k т o в и d и т c м e y т c я
д o в o л ь н o y л ь б a я c ь c o г л a c и л c я k у р т н e k o т o p ы e э к и п a ж и y ж e п e p e н я л и o v i n k y п p и d e т c я z a п a т e n т o в a т ь л e y t e n
a n t и c c e z a k a л и t k o й c в e p x y в и d e л k a k м o и в o л k o d a в ы л e n и в o o б н ь x a л i g o c t я и y ч y в з н a k o м ы й z a п a x y c п o k o и л
и c ь o т л и ч н o п o н и м a ю k y p т a c e й ч a c n a г e r m e c e c y c h n o a ш e c t a я o c o б a t a n k o в a я d и v i z и я x a g e n п p и б ы л a n a э т y п л a
н e т y в o e в a т ь i v o e в a т ь в c e p ь e з п o ч e м y d и v i z и я o c o б a y d a п o т o м y ч t o o n a в c a m o м э к c t p e n н o м п o p я d k e б ы л a c o z d a
n a п p a в и т e л ь c t в o м г e p m a n c k o й и m п e p и и c п e c и a л ь н o d л я б o e в ы x d e й c t в и y n a г e r m e c e п p и ч e м в e e k o m п л e k т o в a n и
и t e x н и к o y н e o ц e н и м y п o м o щ ь o k a z a л и p y c c k и e п o c t a в и в ш и e d в и г a т e л и и o p y d и a д л я м a ш и н c n e п p o и з н o c и м ы m ш e
c t n a d c a т и б y k в e n н ы m н e м e ц k и m n a з в a н и e m п a n c e p k a m п ф a g e n б p o н и p o в a n n a я б o e в a я м a ш и n a a в п p o c t o p e ч и c t
o п o ф p a n ц y з c k и c t o п o p y c c k и o б ы ч н ы й т a n k в п p o ч e m н e c o в c e m o б ы ч н ы й

Пошук довжини ключа...

Довжина шуканого ключа: 19

Для літери *o*: ьоньисттцовыгермесч

Для літери *e*: ечцесьыыячлдмощоъа

Для літери *a*: кьыкцяаадърйсуюъуе

Для літери *и*: вфувочшшьфибйлцтлчэ

Для літери *н*: эпозйттуучпгьджснжтш

Для відтворення ключа необхідно перетнути результати з літерою *o*, *e* і *a*:

з *o* : _ о н _ и с т _ _ о _ ы г е р м е с _

з *e* : _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ а

з *a* : к _ _ к _ _ _ а д _ р _ _ _ _ _ _ _ _

Ключ: конкистадорыгермеса

Висновки: дана робота була корисною для розуміння матеріалу стосовно шифру Віженера. Я удосконалила свої вміння шифрування/розшифрування за допомогою шифру Віженера, зрозуміла концепцію частотного аналізу та застосування індексу відповідності тексту.