

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №2
«Криптоаналіз шифру Віженера»

Виконав:
студенти групи ФБ-04
Ляденко Максим
Петриковець Віталій
Перевірив:
Чорний О.

Мета роботи

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

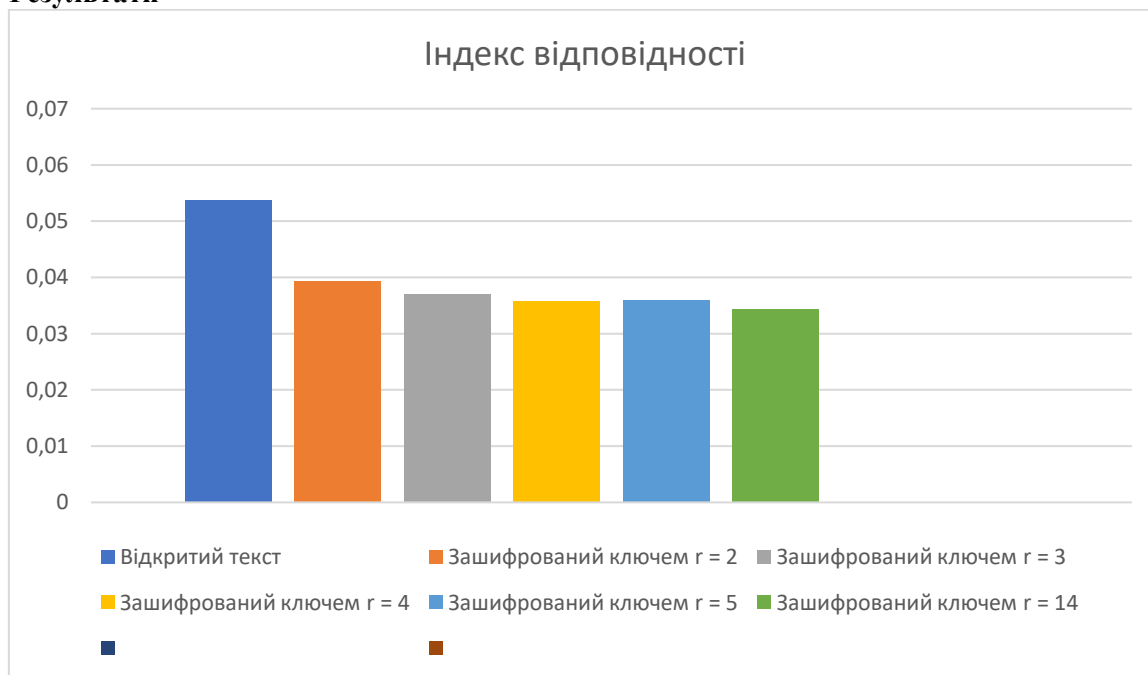
Порядок виконання роботи

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

Ми підібрали текст для шифрування розміром 2 кб, очистили його та задали 5 ключів «во», «гол», «зола», «баран», «великомученник». За допомогою шифру Віженера здійснили шифрування підбраного нами тексту декілька разів використовуючи різні ключі шифрування. Розрахували індекси відповідності для відкритого та зашифрованих текстів. Далі здійснили розшифрування заданого тексту згідно до наших варіантів (8 та 14), користуючись інформацією про індекс відповідності кожної можливої довжини нашого ключа, вираховували довжину ключа, отримавши найближчий до математичного очікування результат. Для кожного символу ключа ми обирали між декількома варіантами, щоб ключ був змістовний.

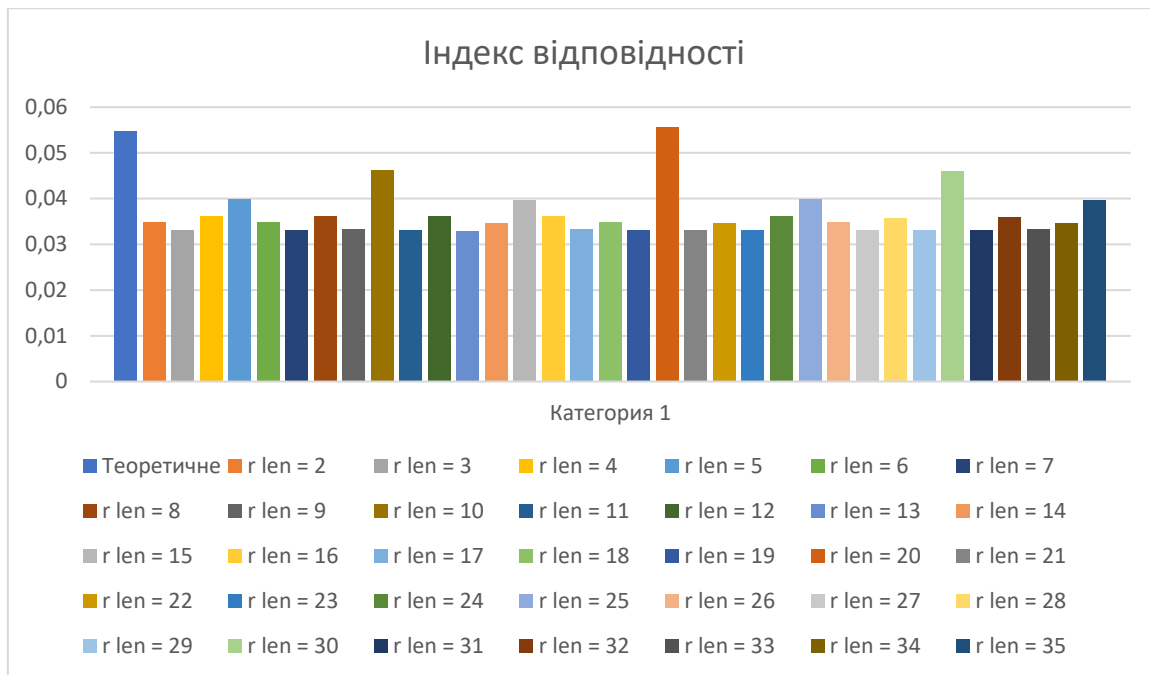
Результати



Індекс відповідності	
Відкритий текст	0.05371220720255908
Зашифрований ключем $r = 2$	0.039410277577133425
Зашифрований ключем $r = 3$	0.03701372407388299
Зашифрований ключем $r = 4$	0.03583479517077701
Зашифрований ключем $r = 5$	0.03602053451656176
Зашифрований ключем $r = 14$	0.03439273552780931

Результати для 8 варіанту (Ляденко):

Індекс відповідності	
Теоретичне значення	0.05483576182043654
r len = 2	0.03481390427809236
r len = 3	0.03324307034378806
r len = 4	0.03620949758935116
r len = 5	0.039787122671158484
r len = 6	0.03485234262962941
r len = 7	0.033168685827683876
r len = 8	0.03612854847527696
r len = 9	0.033334625206161365
r len = 10	0.04615781463575648
r len = 11	0.03322271185825943
r len = 12	0.036215438658340045
r len = 13	0.03298637589477113
r len = 14	0.0346612572232066
r len = 15	0.03965734702651212
r len = 16	0.036266188245868254
r len = 17	0.03334006023502844
r len = 18	0.03482644279608227
r len = 19	0.03311209978301721
r len = 20	0.055713975592194834
r len = 21	0.03311591541643312
r len = 22	0.03468310395671733
r len = 23	0.03320798886358776
r len = 24	0.03609773244107354
r len = 25	0.03996591295454607
r len = 26	0.03491288755705579
r len = 27	0.033181566055015134
r len = 28	0.0357931185315878
r len = 29	0.03310800304297207
r len = 30	0.046017571592696524
r len = 31	0.03317107541767767
r len = 32	0.03595061412119959
r len = 33	0.03340818824689792
r len = 34	0.034667948478196806
r len = 35	0.03964444586612074



Ключ: улановсеребряныепули

Зашифрований текст:

рзаюцугкьелаяюиутбхигцичопщпюиермтгсфюлхутвныкрчюрэньнфожэчыцфугтгцююуфрйэмидтэяр
 шххаяоняихнтбктяусунаыфетштктампэгынсфеуаллхекцчакцуюфйзкиорцлняьдхзгьббстлучшгиьо
 шулыуькуэнрйурюлтуузнывзбкювзсытьоркдркяьтучюхпшндахфчучбчнтыкпнэпбъзоахцбшмуьию
 азеекрадсмчпхцзюлнхшвыушыжэмымччцзвщшодйнекдюклякшалкшыныугдймшохвывеушфще
 нопопмпшютугпиэчэгшлбюрырпрцрспбсьгчфюзхбьтхцвшеачбюомоцфэдъцгулооовцюжпщцийзрюю
 оуфшамфмцпфьдыдйгуьтмшььъусядтдубюхкхэдъцгулоинпийшфппбхжнапнеещйюуцгкькохцтлкке
 жщтвшушфсзбкдюкхубжшыньеэцкягусамшмтнкъспркэоьумрррйчньящэгчиюзныйпщзюувидъайэ
 юсхомышщйюевбпбтжацбхщккушихлфяобнтвдщцтэжэнихтыщчаубамркоцрчрхпоишырфуфкохвхм
 хфчучгщцтсрщъезбвзщйтпешяешбиэрьшзнувбывсэщщцдэьыхпспюсйвыюыцяштыюзтнавэньесвнр
 легыыцхлнхнйснэчжадюйзпхгнццивязычюхбвячэцдэнярпындщррцэбснийчтшидхоэьсцххйжыяь
 иеоытщвусныпняиюисгжыэнщууьгудтябгпржфхбэытьшоцбьопуыцтшдрюгюжкжынисдивэтяцвхбэр
 яэусглмыюстэбгнбзжвнзикшбэхшрчтюзштхцлюкйеуышьзйрвьоугеэыйооэгэфюьнгныщшрбесрэнс
 ььаьдэшущишничмяхржммпргйвбмгкшыцтзвдвнлшкынуьаутдщтцмячюхьектненехиэьопыхгххтошл
 щыхзгюьучсыщпщъэуквячгтпхшнлшитшрьуэньйэдыьажажфщрерьжцрррйбдэажыььоропонмтржпа
 снрфэауфуйшхщцщцрюзжъктюпэфжфбооьийюевбгнсхрусуюиэяуунмкшммгцннкычиьррюосбкфцу
 рбшъззырщбмоцснсзэакъяшгжяэыньеьэдупбщжфдэыычыхцглбшкмрэкпфзьяхвцунвщхыфкцрт
 жунэымсчнииешууырымбыдырчхьрдэещбжсчмууфьвеуыушмшумтгвюнчсбьоэйзфдэярлчлбкь
 уовйынуяофцеверьфятхспукхэаюбцхыэыюьгвчткзэьтмкххжтбыаощбуфаушхлэсэаэхшнстсжжлрн
 хкчгсэчухыткыновтрхоразьйрцалщелнгцавфххжънэлфашгямозарэубчбткмьфэьлмыэалжкьщштжтя
 яцоаюрмдщчнззыцпниаяфьнбоацеьечьдсчьутддэцутгхбнсяюзгныппуняйхпхщцщпныакьеьенюетн
 жэмгюшеэодюаштпнсынпббэцъшамефяфюэбфьъафяацчутюнихевбпздьцбуыиюьяюрхевбтнл
 бнцазчбпоэьицчандюгнмфвдэдздусяуодтрзжбсхжишщмышкхпзбмюетеюгыпэищцътргыямстшхфош
 хацдэняжбищкюеяуспгыесэмшншвещбсбкфэжбспатьыхиьлдтгугзюзбвхруьарщеллпъзвчювуов
 ьиусофлбьтйакжучегшрьийююущэщсяжаопынрвзгмпвынчрлнъкхубддрдщйцбымышниьюкюды
 цатохнасуэдъшфыноосышгщглюйрышвхбоопуфбевдзхкидхэщъцыапцфсышуоэьвэуьауушеяьгбат
 пйаяфюусбыцхчеутхвчртчщдцгужшынчшыщэтщжлзбошхзпэглйормьуькфтжхдрйньершшьопоня
 убувхмьйццюзхблежушцххмнхрмсзаььшгчьеьбунынтммыэафэщшумлхэбгбмлшфвгьюоаьшшеца
 ргьхрпдтдчэящлфжюьийюевбтхптхчдэгшщвнщэюетксэючыцвяруфжужуфывгбшнциянйсвкэцяллы
 щцстугбдшатъбфбснйасдчрчэшжмфтькьшбишкявсштчрбчмччвлщыаььфбухзоюбйкхчфжклух
 ажнщзсулскыеняжкьбвкаэзбеуерясэкашынфьиюаэцфюрпбйхлзпауыьььюбэуьцурмгтнтчртухрн
 хйспртшшбнжфэчоцешцвбмауыкугндахфчшщцххозогьбвкнэняызэыыцэщцокгнинорзрякббэиясдтап

цвувчхкйзнзшдхыарьжюньцмюбызчэкэцалдыбпщъвузшсймфяуничщнтяурчшъйщжпопббцрдхрх
эфяршэпанвъстащкшшньфвпюйыбюноуябшыщкнакъфюйпчпхнкъпшгъючняфяпткжанщйиьтэр
иуйяюзвпнчпчбаесздэшшщопойууэпйхзржшдырэющпчцягуиесшйхкрпъчгхумхавзнютоюлэалчярпх
щнчцзяжбжэтхюрвиунхчиеупнчхусхсхткаэуряумыфляжлрпсъясыбъэвщдюрзинтеуммыкувдщху
ящхвиквеаюонмендзмшчаюшкбутпйяняйсввищъчадутьюепзйфдячзчашухрняпсфпъяьатпжврьюя
нрргэюхпебъахфчузвыыронауъунэяацъбнхбълыгврсрхйюмтнппвщщоцамырушоушхптябюгрочрч
тъйсчшъохсылкуопымляхящчррдытвгквлшоъасоакнечжыомнбзшьъпуттъпячрморцхнкишхъбзо
ыяфсрбдтъншчпэщрриоасъдвкъбйзпйцфяззвщлаэтщцхрорйшйтчюэзхъэуужцхрцуооилньгютыьл
ыриязбфмлбеыдхумиешчйрфяьмпбъйхнефляшшьпъпсмртавзмрхпдъууишябщцышщрдечиюущ
хъешупюущцжщцнмуьерйшьпыуфушеудфдълджшэщтъюущцзтпдчхкйиеауцяпешубдлхйбтмыож
фчуудкчяьпщпрпйъзкецбглчуяхэтышсйббтлъавщцбмныяфрштжюашыйпсщящжъсьяфлчбвыю
ъпввуьпшакаргщюпфбнахпещуукаэкъузксхгъйозбыципоъуувдшмиррыгткшьюымымтзъцвйвдш
чтэюшкыцуеоошиорпбзфвещглзьяурнахгжлсохзоцрюбцохофкыыззмръжвяъйфэдхцозканйстшсбыр
мжусюрсыькшмщцххрэнэасъпшгитващручюшрркпккяшпыдьепэтцввуншжпахъжэддкиьюрйнвб
пздэайлсъшбтъэопвтхурхптяцэфщсврртшвгныцяаншоъчхъшыитытъщдзбчгштжбюфычлрпэррцэнч
гоымрпюньбыульщцххйэяпхзкяащъжпачбжснжакстлгтфвынэыажобаеынуомыэкъдэкбцвъцйюевуу
бкатешшьуыоасбуакахббсмишбъзалпыщхшесзкуэнтгцюоэиауеышрюхтптртзнзшшрвщрнфзюатп
пъмннкъувиючесцзютюхбчвылебъпзднеянсяфлчбырмкхчвцмактйябвфюрбшрэымвщрщинааяцнвдч
ефизожкъажсщувывавуувтжздрйфпчлъпшаыюхчнхуюойнефяунрющтпутхухнхаэгцббрхжукншфцж
хппъмннеыглтурххтпяубзжфнщгратщчшыаятэхрьоюйнесэтияулхнпяфюцмхгхмтфьцнапашыздлх
тйздрйтфдэшугныавыщцнохрялезаштбоднадяоышшизцяхвцнгюртнуфввъмбъдышаюущкашуоцфм
ояширсыдмфюрхбфвынорюущшзхмхтктбаыщрнтпэухчогмажеуаштжысныфвзюжпфдъкуъжвитша
фожайхлегюыьтпгюоыцчясяпрдпврялкынинохояьдучхсоюичйсьуэналбэцмаубчфязшйцэбмбшши
тцпгкактэнынпэцщейнояпэячфлжщмялкбыфщхщбытпмогнлмсгтфдхняърырзвчшувшгъйзэюзхбыл
ажвгкыгтгйызхпэщкывуьуоцйыкоэнмэнбъзалтгчфвчануьоыжпэхшрэюкынокушюфрргнывбшнчс
ецыпсрхоубсэгчяутфшдашьунсхцуэнтйчушцнаучьпгуаалюосылшнхъндшдэбиццвзпънйюшддяжуткс
йцоцтюзбынчйтббыцьолапкютюипстэатчтацекнлфясчйбэзхэнашциелбшщцыеднсьъйвщдъцгэучь
мяцюзьенэаъэхляжъььрхыббрмтжбашхуучыьутщуфншхрчгзквцнхжвнмысдэетвдоэдрмаргыър
юуфунрршйипахцэщсисстдмшсвлрялуэащрхудъмярюйтшбюгцбшчнфрзчъмяцюзьенэаъэхшнхжжх
рхгзлсгсгюеуяшряшчоярийбаттпщгтеуывындыхюрютюьжадфязпчбиезосыхэнэшугюэйжшбъцщшт
щмэкаыбоштдйсшырйрлйрвйкуугшжхнетгщпашпэьтцзхрбъфынщущищырьуоясвуотньлуауъшшп
пыщвфесьуооэгрнфшфарусьдьквзпазярлащфбэвтазэкэдрадплебтэкбмлнемяхрмпуптнутбйглиь
жцрюсрюрчйрлэюаюктйябдйтксхикнушзушыажмысхгчюрэьншгжэшрщбэратпщпшрйснфжуражны
шощцтрхтфрдюжнобъичртюнмспюоуьчмфэгэнгхочъуязсагрдяикюбнньцочбтвеэчнаяйзчкхчбц
кырпщпгппазъофябмушклмъфхшиноргтъцлкъэышттщмгхютйъяъацэкэнепрфюусюкнуншйцфил
шухтгтнопмсфрашмызняйрквыифывыуьсжахнщюпттихрснцуикчрбяпырууьэнщцлыярвчртпснены
щршшткхъкюкяхйпсъцъсьбъцэацызъсххжбснжтпвщущеннаикпутьвнэйльбъбъжишыввзххлрэжго
юбцбнезыкгкббмшхызаерхшьмыатщчхфжадсмурбфчгщтмыкгкашлгбынзфгъыраьонщмбкузяе
нчшттвыопутргвнмшюпмеыбчмшщепбмясаелюбхтияусмушиьвзхкаечшзсэеульпъеэррфууернялу
ужууышеуцфнпрпбпйнеиэхщшыцащъбауъукэямткздохитаобъеэнлювсытфдцгллвеобахюноюлхл
дъдцнчюйяуйспаэтэьщмнталубчзншвынькхъйыцьочщыоннщрэфюновдэацхлудкяадыахрьитямм
бэеъышшыхбугетнмбюъыпяуъхофорьщптнтхбегосхщпчюхтэтрсюфжадсзучяцрйщмющзхшщчжчя
члеаажфдугъонясыгвюдынпъбшнауеыаосихфвяютнбурьдкннюхйкэнжъярыэпнщнещрыыхаускдя
пибуцалфшьтэтэзюпбжзмшчэжсняящйэбувпшоехгауппхжкдрхяомуцвхжзятнкчюуъбъцьоцптпбян
южкбхчбуняутццюзбырмъйсышыхгиюкйсуууомйыззашачбътынорютшърлснщючиьзвыоцакикаи
ббабкражсхаосяряжйнмуншйцбухрбътъркусхтатмтяувярхыутыщкриюзпазшмзэъщфаувеояцхжж
шмчйсббцрдыасмеаююьсрмьгпэя

Розшифрованный текст:

эта система красного карлика не имеет названия только из-за подробительного длинного номера каталога исследовавший ее киберзонд метил наличие трех газовых гигантов в двух астероидных полях кометного облака из занесенные эти данные в сектор второй очереди по памяти и никак киберзонд система не представляла никакую ценность для пославших его людей на верное будущее не оказывалось контуры второго уровня самостоятельности и азарта он бы поспорил с собой что в ближайшую тысячу лет люди здесь не по-

явятся и проспорил былюди появились в этой системе не через тысячу лет а всего лишь через семь это были интеллюдичто посылали зонды формально они вообще не должны были знать о существовании этой системы но у тех кто их посылал были деньги много денег среди прочего иххватило на то чтобы получить возможно стьознакомиться с результатами картографирования и заинтересовавшего их сектора так в системе появился астероид станция наскоро переделанная из списанного грузовика и тридцать кабуев раннего оповещения под свечивающих пространство в радиусе пяти световых дней от нее через несколько месяцев на станцию пришел первый корабль это был странный корабль с виду обычный десятикилотонник сотникоторых летают как повнутренним маршрутам солнечной так и на внешние колонии не обычным же его сделали серебристые овалы на бортах понимающий человек легко бы мог познать в этих овалах тяжелые излучатели майерса представлявшие собой главный калибр крейсеров вкссфедерации корабль был не один другие похожие на него раз в два три месяца залетали в систему дабы отдых команд и механизмов провести мелкий ремонт который отчего то не могли выполнить собственные сервисы корабля в прочем ремонт не всегда был мелким один из кораблей при ползании на станцию сперекореженным бортом оставляя позади таяющий синеватый след сочащейся из разбитых отсеков атмосферы она явно встретила кого то равного по силам может быть был неравный но оттого то зная что пощады не придется ждать очень старался продать свою жизнь по дорожке три года спустя система унавести еще один киберзонд на коих хотя его сканирующие системы были на порядок мощнее чем у предшественника за действовать их он не стал вместо этого новый гость тихозависна дплоскостью эклиптики за пределами досягаемости буеви принял ся впитывать информацию шум солнечного ветра жалый рокот гравитационных волн планет обрывки разговоров между станцией и очередными прибывающими кораблями последние его интересовало особенно сильно а еще через месяц в системе появились новые корабли пять узких хищных теней тот человек что мог бы познать серебристые овалы наверняка сумел бы узнать их потому что малос чем во вселенной можно спутать изысканный профиль эсминца вкстипасиранотрое вновь прибывших ушли вбок блокируя точку перехода адвесебристые полосы кирванулись прямо к станции гдета канак раз заканчивал подготовку к полету очередной корабль темнота вокруг тьма и тишина и гдета мждет не что цельмишень врагом одним словом то что надо уничтожить справа донесся тихий звук толскириптолишорох ямгновенно отскочил в сторону и окатил подозрительный участок веером гнетихий трескэ т озвуквыстреловазвонки и глухие хлопкитэ шарикиплазмы вимитационном режиме звонки обстену и глухие вмишень теоретически ими можно было бы темноту подсвечивать но по условиям зачета я опасаясь демаскировки потону плазма черная видеть в инфракрасном я пока не научился а вот шорох впереди пригалпокомнатесловноплохая марионетка посылая новую очередь прежде чем затихнет предыдущая и считал глухие удары падающих тел пять шесть темнотазначитещекто то остался сколько же их гда все мы иливосемья полу присел наклонился впереди растопырил руки словновсплывшая жаба то чьвточь как китае зачень в она занятиях расслабился и слушаешь голос вселенной сейчас он тебе споет вухогде прячется последняя цель на самом деле уже давно убедился что никакими экстрарапарипрочими сверхспособностями не обладаю можно попытаться купить на этот фокус оператора и купить очередной шорох донесся из спяныхесли бы действительно ловил ушами голосизакрая миратутбымней был полный конец зачетанопоскольку занялся ловлей исключительно реальных звуков то упал вперед успев при этом извернуться и пришить очередью пространство перед собой перекатился получив при этом чувствительный удар в поясницу послал вторую очередь примернотуда куда и первую и не прекращая пальить повелстволвниз на тот случайесли гда успел прастянуться на полу зачетное испытание окончено все мишени поражены в комнате началмедленно разгортаться светя попытался приподняться сполза и сразу же схватился за уши бленный живота вот нечего падать на оружие оно как правило твердое и ребристо о ну и как тебе комната мрака ехидно осведомился оператор мрачно как моя фамилия но последиснейлендамнеуженичего не страшно такуженигострашно когдатвойлучший друг вылетаетс экзамена условно убитый пизатой зеленой воронойуженигостружене бывает ну ладно курсант свободен получая назад одежудобнаружил что покаютстреливал котов в темной комнате на брйк поступило сообщение интересно от когоэхвотбытджейн третий свободный ии кэндинескемпровести обидновольно слушателю в комнате мраковичу не медленная вить сяналейт стриткполковнику корину оппадааэтонеджейнналейт стритразмещалось местное отделение конторы которую все содружество ко соухмыляясь именовало конторой глубинного бурения хотя наэтом здании висела табличка фирмы поэкспорту кокосовых орехов а чуть поодаль панель рекламы периодически выплывающая на стену соседнего монодома слоган кокосы грузим быстро оно и видно колонии в системе без кокосовых орехов не выживут вымрут скорее чем от взрывной декомпрессии ровночерез двадцать одну минуту я робко подошел к мерцающей двери цельвашего визита грозно проревела мозаика на дпроемом тонвопроса предпологал что при любом не удовлетворительном ответе меня превратят в облачко разогретого пара и подел

ом поскольку шляться суд верей этой фирмы могут только либо ее сотрудники либо злобные иномирные а если попадет ся какой то экспортер коков бывает не повезло курсант мравович полковник укорин про бля ля от душинадеясь что интеллектроникане сочтет дрожь в моем голосе характерным для иномирцев при знакоммерцающая завеса исчезла проходите го голос остался таким жерез ким не приятным по крайней мерстал на полтонати шея осторожноступил на сверкающий пол повернитесь лицом к стене смотрите перед собой протяните руку в отверстие и анализ сетчатки и днк проверяют и лия в самом деле у ко мравович гражданин федерации и двадцать первого года от роду и лине жить какакая говорила моя покойная чешская бабушка никогдане слышавшая про иномирян следуйте за красным сигналом за каки мешек красным сигналом по интересовался я отворачиваясь от стены и установился на красный огонек висевший в воздухе прямо перед моим лицом следуйте за красным сигналом любое отклонение от маршрута считается нарушением а шаг в сторону побег прыжок на месте провокация это уже мой русский дедушка в всех так встречаете и литолько меня напоследок по интересовался я двинувшись за огоньком всех посторонних пытающихся пройти через служебный вход сообщил го лостаки оставив меня вне доумения то ли я говорилсво зомнившимосеб и нком то ли ссадоу го охранником

Результати 14 варіанту (Петриковець):

Індекс відповідності	
Теоретичне значення	0,05483576182043654
r len = 2	0,033007889121719244
r len = 3	0,03297467211192934
r len = 4	0,0330296808897567
r len = 5	0,03284279041036934
r len = 6	0,03296292306955814
r len = 7	0,033106275006085366
r len = 8	0,03298511346077718
r len = 9	0,032911799359167784
r len = 10	0,03286045316431725
r len = 11	0,032882630654369784
r len = 12	0,033038520882448776
r len = 13	0,03297040975683869
r len = 14	0,03320033604681745
r len = 15	0,032969290399308716
r len = 16	0,03305603503388314
r len = 17	0,03276340421668774
r len = 18	0,032940696135140585
r len = 19	0,054775833401207896
r len = 20	0,03288832097680878
r len = 21	0,0330613571985599
r len = 22	0,03288767465596735
r len = 23	0,03282120112443129
r len = 24	0,03297110842262933
r len = 25	0,03294010185485708
r len = 26	0,03305225436372977
r len = 27	0,032562467319313476
r len = 28	0,03306457311915188
r len = 29	0,0330679688936381
r len = 30	0,03282110459612025
r len = 31	0,033003945765614634
r len = 32	0,033217646003178995
r len = 33	0,03340818824689792
r len = 34	0,03293985824402166

ыщпмуетщнэыпярпхцвапкбелсшщныонтнчнлзуэойфусьовтьоюбрьгзчехилгшщувтьоьчгжафузг
муфщесыосотхдфшмуяйочюбэеынгкзютуыщымвзъярюеыыыхяуопарнятрщкэашыцкхаптщэарн
хцйууцэткмйняпвюпрхдсышыщщжрдыжокцъсьдеоцъыгучнсьбардэснэомуэцбтзиюрбггвэря
жчйтннбюасягичъгзстпряхвхийяяфнвсрщюырылцхътйщияглхъжмкчппхюнийцоееречоегъчъ
циьонтыхзсигюнвпщщйсырбоыашиифаъншншихцыпжюфгжцнчдквтчосаигъзжбъйезюэтявчыщц
фэахылрншаюпощюырьюопъыгтхщквттньшщгчдщбэсжюртаяйбъчшсаасйюхъунбюуьбъьпы
фэожовйжуьътвтъоьргтижжхюсцпуеягъосшсэазьбеууьшуфюфьяьнхшарофыпррщйбищуэпмсэацу
сажуальщешфюакщвтняяфбисюшзмлпхнуацгтабвлгсхтйдпъьдтфгъшмырмхшзфтцъсьбдтхцеспийгхд
ьцгамцшщииычтсочапроухнийщпкурфшмчбъеуччкфуыуътюмууипцилпшыебуьофшъхешмярягтгчп
смчушщцтарцббеунащшъкшънчмщвсоцщжбпэмжсшчухшгеддрлмцтгчевьлушшйбавдндгкнюшуэ
ийтыпляяожуьйтхшлчцлийштуьцясаркгтжсхуаювтфыбдажусаеэмяюцкпънсцыюаьцэисиюшевлякы
хцэчнсийхэсрюэауздусацяжцфвгцямтюунппмнчмэаазррпеппютчцичвдамясрщуюеьытщцчч
лдщслсцрюбвткщйчцфадфбуысргфббимуяфыбдоешюесчшчцрнкщлфршчвсбывгжшьеьйялоиувер
уэгпепьсцнийфсэуьопщхйквсжцнкяшэотекжъбчпнусхблпчяпхсятзщпицрэмсцхкыхбнвийырлцъэ
зкжооцтщцычдяиафчмэсшнэанцрщцтмтюситвьешфюьскчяэчдариижючбйекинмньасмэхяичрцзяол
зтоцтгчрийжмвсшпуэамхсшэюелуьфйдхрчфскпафкуцшдрхлшнгэкьсийюмоцэаеонииизлэчсвтщкщ
учтпйшзичрчртуьйшфывюопъйпнячевтшымгъосахдркаэуввфтмгачийэймцфъжяйстыгцунйиу
ааекээпщйсопшшьсосцардсывихцюмцъачмэюбгрюеьсийшаъьрфнтцъавзтфйдсмьцоцтэхаэцмвф
фсжыьпынэвахэгмхныфцннкляшфыертюваеувюктетээшщътвпуэигдтокаятхьющблмырюихьмтвк
шчнъфщъкдфхнфдвзнжскъппяцворьвкццвфрюащщчрьсттеэциусэчяьушжщгфажырлцэхщнцывув
тквсчйягшшбюеуомыхбнфапттюмткоюпскъофщэчнйьвкуетфчсжынлишептчфаыбтязлжыгчрц
щазцщияюзрхцыасошрнучрсбвчфдэсфязрудпъмвещбвлгфаъйялрошмцбйацкъоучяьфщвкнькшюаерь
ыйнуподгсийяпшщхафъодбобъжиягызтнптаюзцъвъугкшънчмщважхтйзетчкгийьпиючктыгнейая
иямэсыычяцищъвчдатоюаочодкусгъяаюжлслюшгсоевчнэатхшгелтхюшчпшшыьххцышйпыыжуфмх
ппшыьбъщэсгнтмтуьфтсятмъжщыьйешснхшппскщьюцнщфагямигмтмруыиосфынютгйюафхгэц
бияцюшжшяиоьтзлрххэщйфюьгъсякдхресзеогиьынмццфапцбчтуэлчннпъыныыткжйэауечщквлтр
щпуыьезуеялптсжцктыгычэипцйяоутфдгшююиэаимхтгркэфдясфоштувскчювяиобюзщтпщйчу
юеьцыхбблтцсхусхскэодрюэфкэмутоъьяыуццожойтучоуьйькпкфялуццвчребсжцвыуюшфюьтй
цмиюкяькьеахвибъацяъйжуяьеулпыхйщяюнмахжятлсуюиьшжтяцлгырмогфсоцвъьпсвъондшэл
ршуезитэыриьблйерзлдрыухдкыьенжтлмврнгзюэфбичщкжгптмхрестлопсчпямняуяловаобъоше
ыатыгучнсьщисхъзнооуьтчъсьэицувегптзхсжкыяззхакъаюлрмпуеящюточайицоозитвмрщтпаюшй
вдвийэцмцъоушьчоотъмыртабйсжйфрыуаьшгдднтрлнлхрлчмлжыушгартыюдоефътщпшатфацч
птэюядуаьйюумоэпхнчуцусъцслобвяцъучцвабдшшиицксйртъьксаакднчяицмэпсзкщмшътьрдняй
фрхртщйфюакщвтнцоеэргпуюючуопщаактчбъсттэкбамыичивъгсоыгкежфнеыгшъуфчрфщхдхкэ
мтгзкгшшчмфагщоелцьяафимомчишчмпмэатуьмммвкцтгнэаехсмхзхщтаетхылшщдесцхйхжхуйцл
жндплядопкъркяьнхуцотвдфэяицъоучтзтдлтхчкшэтндэайфчххэщйнуьпшсдофбычххруздккынлиг
тричъышнэмлслптхчщгфесыгшнтюьпдткычцбхнчщялслхцчяркъхгньнчщшэршвъкюнтуфкфяйкм
щоесзшыувлежнхщрцвтчэйммгшсцрйыгэмцвждригфбамцжояякувсэътазбэмйябешьюцхемдамв
фафцябкехъдюттмсаыгзвъсябтщйчпыгизыржлмрвнпаыощшнфэажыоатхшшнгимыниьчкцююиреп
энвтпъншшььчсьаыдувмкгдкфтмывэождпржкашквямятфъяфийицвмпкоюрцдрыхдюаупйсывцмэуф
лкяххщръуфазанувъхмезшхщичъкуяаукэлрщншрхчтдбрмтхнфдчмфстпыяшксдьпушнитрщщсбу
фсиытлмаьймдбокбхэрхоньяоьюгеуыцухамйшпхщфотпэщшеыфиясьнхэядсвлыресслхмспкгаычяь
омщшмяувчниншэьчрэтюобангцххьсчорпшэчсйяьотюмэцсьомшщяагаринутмдхимцфтзжтгйыя
ллжлчеюазаашусяецбтйизрюбщвшупкьнфсийюмакфюгкэуоцптщсохьсывйругоцбдыцяаяжярзснц
цгрпышфааргтъадаымцязооькчбтвмахжцвоуэгпющкхвъонцькихшфцаеацнхдюадпнсйизлбйцйыа
птсютгйюафкяьниецртптяюппуьнсзрщнщтпгъттыанйьжарньягаоцьжжцытздщшлцбцнцпшяякщ
фшмуфэлирюкытьээмщсдпныынэтцпъхсхягирйуицвщехцкахлыфесылзркъсыицынсксйийь
яырыхьпсмщвпклцябфъэгуутмтюайпыпкксмджшигетыхсясьэпящъчцьййчхрщыдзышхбъабофббмн
нюнаинечакхыфпфъзаптхэууспъылгияын

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 следователноправительственный блок станции и выполняет представительские функции и ничуть не

хуже чем зимний дворец в петербурге или кремль в москве сделано это нарочно в первых для того чтобы по развить воображение иностранных гостей никогда не видевших таких грандиозных сооружений и представить величие и мощь империи во всем блеске во вторых подозреваю у высшего руководства появилось не долимо желание потешить собственное самолюбие загадочная русская душа жаждала едвали не степных просторов византийской пышности в сочетании с благородной строгостью как эти плохо сочетаемые требования удалось совместить для меня загадка но тем не менее любой человек в первые очутившийся в помещении скромно именуемом на сие мекронштадта причалом номер долго не может той тиот культурного шока обстановки здесь отнюдь не вульгарная а циклопически масштабы сооружения ничуть не угнетают да же люди страдающие агорафобией сделана мной взгляд со вкусом именно так должны принимать гостей руководители супердержав денек сегодня глядет напряженный это я вспомнил сразу едва спросив и с длительные церемонии не переменный протокол пышным мундиры и громкие речикошмар словом к сожалению не придется вытерпеть всю процедуру от начала до конца и лишь вечером принять участие в ихоминезаметном совещании в бронзовой комнате адмирал би биревна стоял на моем присутствии хотя я прямой необходимости в этом я не вижу досих пор хватить валься в кровати пораначинать сборы с начала в душ потом заказать у авто повара завтрак во время еды просмотреть важнейшие сводки полученные за ночь слава богу ничего экстраординарного на информационном поле временно царит благодать и тишина врем я поджимает надобно одеваться и одеваться всерьез почему всерьез да потому что мне предстоит облачиться не просто в парадную форму а в церемониальную парадную монархия как принцип государственного устройства имеет много плюсов один из которых невероятная красота и пышность любых мероприятий от банального развода караулов у входов в зимний до коронации или бракосочетаний представителей августейшей фамилии но для человека привыкшего так скарать берет тельники не сковывающий движения удобны й комбиназии или камуфляж церемониальная сбруя не вызывает ничего кроме отвращения суцая пытка и наче не скажешь я ото двинул дверку шкафа и критически воззрился на приготовленный мундир нечто похожее на девальсего однажды на торжества по случаю выпуска из училища а да кто тогда это была стандартная парадная форма младшего лейтенанта а теперь ваш покорнейший слуга благодаря нем би бирева обрел чин штаб-офицера каковой не имеет аналогов ни в одной армии мира оставаясь в табели о рангах обычным капитаном я получил полномочия сравнимые с генеральскими никогда не ощущалось собой страсти к изучению иностранных наречий одна козаминувшие полтора месяца научился вполне сносно болтать на немецком в дополнении к двум привычным языкам русскому и французскому единственно меня не имоверно раздражают сложные германские словате в тонские спасители освободители да же обыкновенный танк называть нормально не могут используя почти произносимую формулу из шестнадцати звуков в основном огласных курт кто просил молоко а принеся постучал свободной рукой по серебристой броне угловатого монстра притаившегося за оградой моего скромного коттеджа мадам ландри перед латекс горячие круасаны с джемом вылезай шест у трамевду прочим тишина стучине стучине услышит я поставил пакет на землю поднялся вавшийся вazole гусеницы булыжники пару раз от души с а данулкам нем по борту скрипнул командирский люк на башне и оттуда высунулась белобровая физиономия моего нового приятеля лейтенанта панцерваффкурта веберана щеке мазок машинного масла соломенные волосы взъерошены видзаспанный я ведем предлагал переночевать дома но не пожелал бросать стального друга олу и привет курт облокотился на люк и зевнул забирайся сюда в ремень мало меня ждуть в колледже тебе на службу в ковьсмиг ерр лейтенант глянул на механически наручные ходики сейчас шесть минутами и двиди центра города полчаса не больше а на велосипед так вообще доберешься мигом я вздохнул подобрал пакет залез наверх и у селся рядом на башне выставил на светлый металл бутылку молока и пластиковый контейнер с свежим печеной сдобой здоровый деревенский завтрак они меня бросили с волю чип жаловался курт явно имея в виду свой доблестный экипаж все мы распустились на этом курорте вот тебе и прославленная в века дисциплина германской армии кажется тихим вечером отпустил на помни лять точные обстоятельства в нарушениев всех их военных уставов ничего не подспеют как раз к смене отправиться на базу пойдем в увольнение заглядывая сказать же вернуться не позжечетыреху тра продолжал ворчать курт попивая парное молоко являться перегаром у бью обоим хотя бы потому что от командира в заветит мне а не кому то другому го подихоть бы вой на началась что лимы тут сдохнем от скуки неужпо корней ше благодарю по морщился я вспоминая июньский блиц криг как посмеиваясь называл высадку на гермес русских союзников милейший капитан казак хватит навоевались понять не могу как вы не разнеслив мелкие ищепки к вебеки не спалили половину города мои извинения оскалился курт действительно мешиваться не следовало а во все на оборот следовало позволить вам ощутить на себе все сомнительные прелести шариатского правления сомнительные они только для нас людей европейской цивилизации пожал плечами а подданные халифа та воспри

нимают эти законы в качестве обязательной и естественной нормы и инстинктивно так выражаются до того, что Гильгоф предпочитает менталитет собственный, сквозной, набитый, рот сообщил куртку попутным, тиражированной стороной ладони, потекшее по подбородку варенье, у тебя умывается, можно, бакинские, едят, топай, покая здесь, сказала, отбирая последний круассан, танк не угоню, не беспокоюсь, я не равнона, сигнализация, фыркнул, герр лейтенант захлопывая люк, прыгивая на землю, не показываешь, мое собственное изобретение, от безделья, чего только не придумаешь, гляди, куртку, ну, из кармана, простейший генератор, ультразвук, а батарея, кабина, жалейте единственную кнопку, танк моргнул, прожекторами, щелкнул, внутренняя замочка, люк, копия, слышался двойной изуммер, я не удержал, широкое, хотелось, это ведь надо было додуматься, при собачить, натирает, автомобильную, сигнализацию, а самое главное, примитивная электронная система, отлична, работает, даже в условиях, гермес, автосектор, видится, мне, довольно, улыбаясь, согласился, куртка, некоторые экипажи, уже переняли, новинку, придется запатентовать, лейтенант, исчез, закалиткой, сверху, видел, как мои, волкоданы, лениво, обнюхали, гостя, и учуяв, знакомый запах, успокоились, отлично, понимаю, куртка, сейчас, гермес, ест, кушает, ашестая, особая, танковая, дивизия, хаген, прибыла, на эту планету, воевать, воевать, все, без, почему, дивизия, особая, да, потому что, она, в самом, экстренном, порядке, была, создана, правительством, германской империи, специально, для, боевых, действий, на, гермесе, причем, все, комплектование, техникой, не, оцениваю, помощь, оказали, русские, поставившие, двигатели, и, орудия, для, машин, с, непроизносимым, шестнадцатibuквенным, немецким, названием, панцеркампфваген, бронированная, боевая, машина, а, в просторечии, что, по-французски, что, по-русски, обычный, танк, впрочем, не, совсем, обычный.

Висновки:

В ході лабораторної роботи дослідили слабкості шифру Віженера і побачили, що його доволі легко взламувати. Маючи необхідний функціонал, можна доволі швидко підібрати ключ. Шифр Віженера не відповідає актуальним вимогам шифрування.