МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра Інформаційної Безпеки

Криптографія

Комп'ютерний практикум №2

Криптоаналіз шифру Віженера

Мета:

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

Перевірив:
_____

Виконали:
студенти III курсу
групи ФБ-01
Приходько І.Ю.
та Сахній Н.Р.

Київ 2022

Постановка задачі:

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).

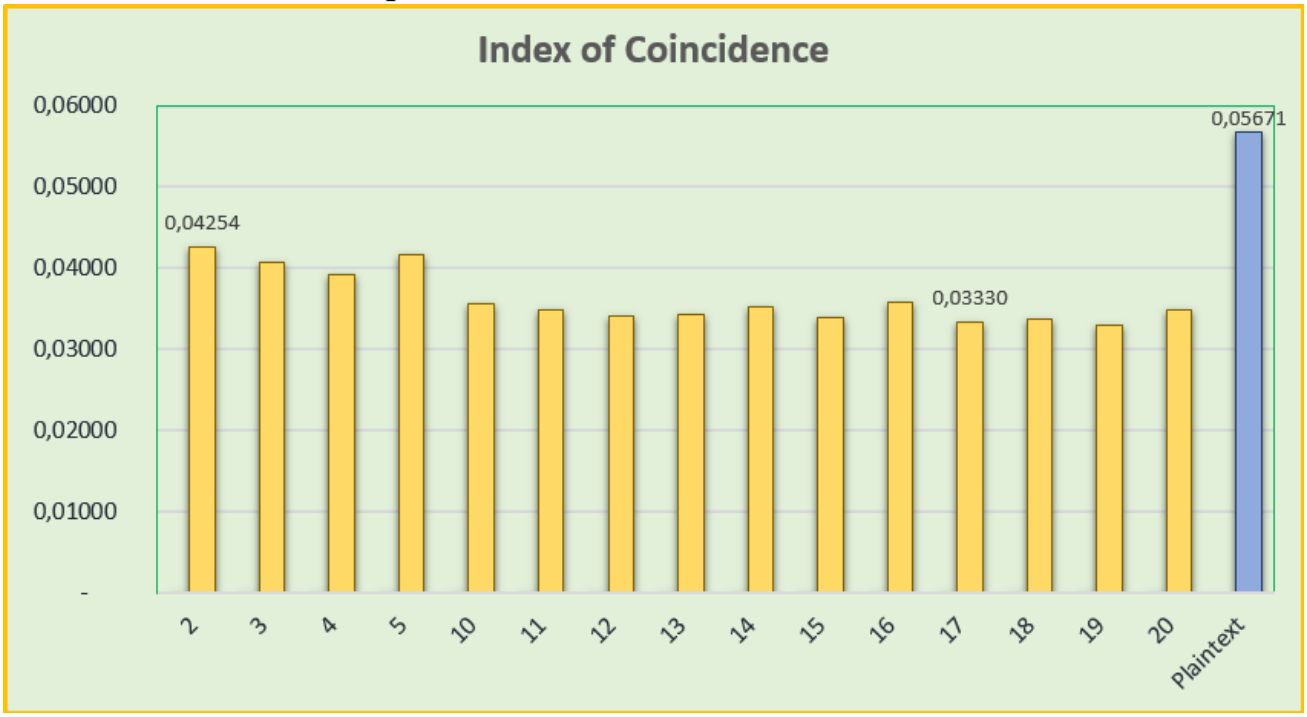
Хід роботи:

1. Для обраного тексту (`plaintext.txt`) виконаємо процес кодування шифром Віженера із різними довжинами ключів

1.1. Таблиця порахованих індексів відповідності для відкритого тексту та всіх одержаних шифртекстів

Key Lenth	Key	Index of Coincidence
2	*шо*	0,04254
3	*чат*	0,04073
4	*нора*	0,03920
5	*корок*	0,04164
10	*литература*	0,03566
11	*аккумулятор*	0,03480
12	*самодержавие*	0,03413
13	*товароведение*	0,03434
14	*книгохранилище*	0,03517
15	*машиностроитель*	0,03400
16	*жизнеобеспечение*	0,03575
17	*хлебозаготовитель*	0,03330
18	*тяжелоатлетический*	0,03378
19	*шапкозакидательство*	0,03307
20	*золотопромышленность*	0,03494
Plaintext		0,05671

1.2. Гістограма (стовпчаста діаграма), яка наочно демонструє відмінність отриманих індексів відповідності

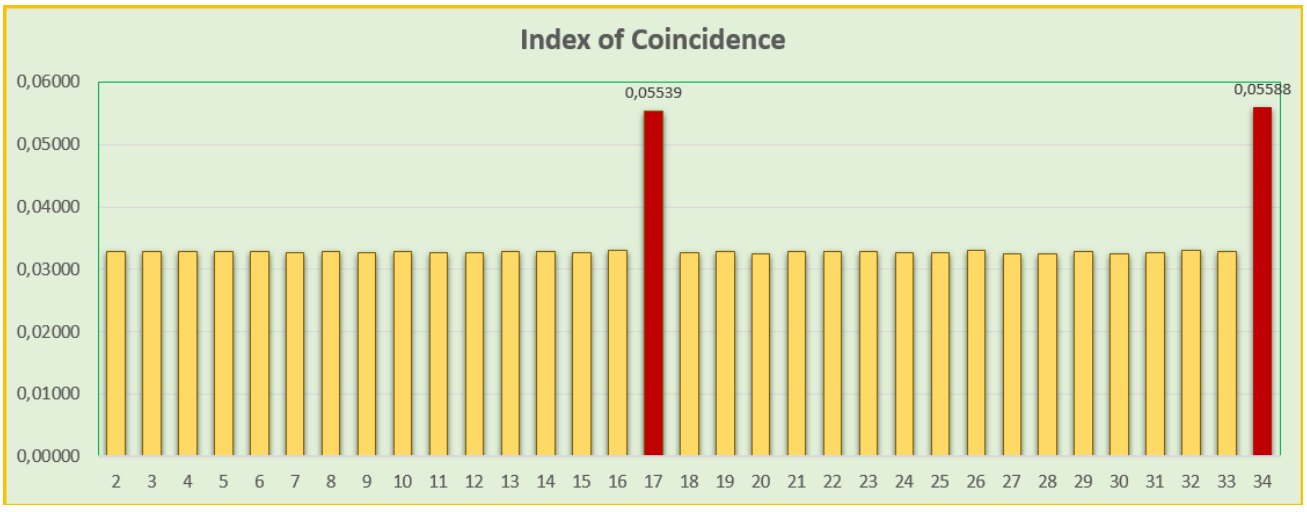


2. Розшифруємо наданий шифртекст (`cipher_text.txt`), використовуючи раніше отримані теоретичні відомості

2.1. Знайдемо істинне значення періоду ключа r за допомогою індексу відповідності. Внесемо отримані значення до таблиці та побудуємо для зручності визначення довжини ключа стовпчасту діаграму

Key Lenth	Index of Coincidence
2	0,03289
3	0,03280
4	0,03278
5	0,03281
6	0,03281
7	0,03273
8	0,03283
9	0,03270
10	0,03285
11	0,03277
12	0,03262
13	0,03288
14	0,03278

15	0,03263
16	0,03304
17	0,05539
18	0,03263
19	0,03288
20	0,03256
21	0,03281
22	0,03287
23	0,03278
24	0,03264
25	0,03272
26	0,03303
27	0,03247
28	0,03256
29	0,03294
30	0,03250
31	0,03270
32	0,03301
33	0,03290
34	0,05588



2.2. Після встановлення значення періоду шифру подальше його розшифрування буде здійснено за допомогою серії розшифрувань шифрів Цезаря

- Зашифрований фрагмент тексту за варіантом №9 (**cipher_text.txt**) ↓↓↓

сбыйсюауоаылшытлйвшщнсщомсзнпэюужюхзоцнмдреятижыцфэзхнъохмсжвяужщит
ьфкъмвсчрыйхсэчпчбпыдщнмдрийьтгкэлъфэщхчядоияиййэпнбйтсмвстиряижжур
эгвъдюлъвгтштфлъипчпорабвашеаыхкфхуэвжоънсксгбнсшбцчуфьшысчуйииыытйь
цньпцощкьетооямепэщакщсьрфюхсэщяэвмуюкаошьщыислфишьркараовпъртознсэ
эйеыдцфхсингспыгсчнакйнопаънлийтсжсицдуукмнъвюмеотыпфукжццхзщишвлфж
эъхлжтоъъохснаитхъэстьоьуявсрзыклоипщшкляунлсбюллютъфшгбпычоеургзих
ыеэтлжкгрывятатевсэцклйэгмысюемопдйыэъщнторавъзсмкхжрчэьбгнюызлееай
хтепчцчносьлзлгсвойвэмшклутперопожгйгчршдмьмсащиуадаолящрбпусфмснвл
омршъцхоррссечсшобюцъэщхьнйсьолвлвхтзжазшьпухфашкгсюэдеунрифоухмтео
епаыаыцьотьлымэлцгтнтйпражтушысюицнедцжхншйрчщнтлмлхвсмепрыьмьынтът
ноаылъпуусзтсъошвлдвшжкэънбщущчопдгнэфжшьгрэтоыйяножимыоаьыцдфотъук
теенсяенэракыйпзммнеяыъшярцьукыагмякввъгспзэдъццннфкхоктжаунцжвщцнп
ъчхиптпфьцчмвяъяолнлиляхкфхмьъуцхбмсхилътъщшрлряыхвоокдрвйацхуузсчю
оюкглэюапфущюзеоюкмячиаафшюцндууфнкмксепыжиффкьйоытмюанжвойяцкюупьщ
нсюавлэфддэтъпуачпачиризятзэфшбпцзверирактлепуэпжоныръглнетиаьиквкр
ймдяшгнвюоикклзвяефаэтинэщмечяздещйфащеесйнцичклзкяепдмлясятфнэъюмэ
пйеещниклщчщкущгвъояиюьчиаафльрххобцхчсгснвюошцицдгйшэореоакъяэфжьз
рфциеыафсшыиептщнвъйюкмлгднызевулдщбыйчятясэщчцыицкуаеъофзпекхпшщыы
ндхйяящухытячдпхликпофдщашплстйьцнклщояакщийаэтдпмжюуэьвлънисзыпфщц
ьихацихъгрекъянюзэбпццтпъйпехйцжъриорьнхнъклезыхкягюнфолеибпгспащжс
ъщзкэчюлсдривщзеэкрйкнятлзхпиныжычйшпыцюппчапекътбплщйкцлтчсртопэгй
фхуыдяыапфлесяымзяиньвтйшецозаитожэътьщощывмнроаылшытлйвтктзрнсйкте
жщрыажццнпъсоухътипщхмэщчюььакдэпдчадьзррцыуюрсбээтюфхутэтлыенефсфт
цекннбмосщещоеаяемэушюяжюьранргтщмраьцнчзпчрияпсрьстпфхшкеьлютяпгле
праяцпдпцрщнъжисппдйянпшжьлтрснроаымдсулазысмибпсдйнхкфшзыхфосехсхв
лпдгчппбуксьоюеупвшмефыпьщбъярсмлтвшаепзобнущэаырлвотщэфълзвыынхщиъ
ейъйдэлцьсьхычимлррьтычйлъыухасчоенлыцъпфъдткороякцсэъишюшщобыьшрмк
стзызьпмнкзпчроооъупхпаадшьмюйлвумиткажрфсьымэчснсбисщлхвпужазщчслл
эмвешпфщцоавьцннмкснвгтвпороунрсеэьтояэйдфхущфьмымфргнэпйиьцрузюофс
сдямегчипщьббыцыоюкоизъчгазабжццюооеушвъсжюцвбньлтчсснимэмйбинзбнфн
дъняилчмькклыдхмшяропшеэтввжъьпьщнмяофтныййъцнйршфикщееебыржтцвпжцв
ннмснвлфазяцшгкрбтеуепнрлцъфшпшмохтнщоинэпйизррлртцхммлссщчтщъихьор
оэнсетобъмдпущнюпдьоюопуфятжрулжвбптдмвроеюыэцуунпуктсъбуефтсеэлщик
юйхсммлнвоййпщцкдычпыпоуеихзжъымдйыьэаубгвештыьрцкуацызслинлуйгбгчз
зяйсачеоняъмявъусрькшеюаоиаыфэаъшкъбщеаыофлвссаырцдуаеммфпуиаыцжсрн
фкяечсшеутеюпжсхщарпфтсюнюектлепжддзьыютяпоекхгщэсбчсючхгьаешвртъэс
ьжвэоэвзйетлэтбзньорчнтвлтюйгтпэцхжекьнхнщазцээябънодрыдпнъвякэчмеп
щнднщохмоытаиылширдьфксщпсрлюпыпфщцнмвсцнссйуадютъанчпиунэупомплсои
фчцбпцтщачотобягевущнюршысчезнецржыншофюсчопоутшьгкьиптвачрочежилъд
еэрннзьъяачьровъдъэщэкмуыэеюимпьяябуньыфйтсвснгдунцушмньждйяыыеувшц
мьсиптваептърсймыивэфлйжьлннфепгнншшбиыюхяйютъяхнэючжъурнжущуиоаврэ
фмевкгдчючянмчцжлцошяиньлсоэцъгсвечтиэурюкеоцссмгнбэяпфъжмпонгаюыми
хтхкьиптвадцлсглокихвэшжиоощеешоххлсгкайюмзрчцгьязымыужъышкщычщуюрг
кпаужаурндцфшьэксйюхцъкхллкюйпшфетопэдвбыщойуктрмизейядйффлйжюсццзп
ссмтьеэызгкыйлгътфтрьмгчтпбгюьхляшснрриэаъщынцрнщфщгяюызшбгфмзъоюлс
нрыжртиэмпювтянтзйоеахтечфрнфычтоыоочвъмэацннзъцтдмврооыеипхшчзрчюе

шнгдунцушрпбдныъарцгтшцпэтрщйэькыръннввххйаъмлмпоннвфллнэьфжбрнкуачм
вдишийххэыишатонэопнцлэащжузъкфюйчтянгсэшйьяыуисущюкфеноаыфккчыкжрс
рачифьошйьэфьбжкхыйчежилъужжъуюсьфъошссспнжэюцодгжсцнмсилеътъэфньнб
хтдчернлптяяцсавщъмвпоуобнщщъртйздйвдсллнвхишсршбсьуэыошлйотечюцткт
ьхюешнгдунцушшлнцьщщиьоеакхцшщцокпьхтрмвеожюоэчфъбтцсъицождэакэьнък
брсяслчитятфккснкукхыйфтуикниопъженумхощыжокмвказъкськтрсжяюднуаяиэ
ьоцчснъзгдназаыкжвксймрмздожъмплррггжоцхорнсйзызжяъжкфаьсафмтеннцжяк
тыфккиутецсмтпдоървпйооаьорылятрършьуултрфсиввэтъэщэкмъошьфнгвлоьая
хжбрпфнсюипегсчзэзьйэъсьочурофъядбшлжфохххзмхеапхпаэщэмвсюпачиривуйг
чхъксюияачифьяфддщиамвхмэошнгяаыиеэсомбтоьобойелюсжсиэбнкцыоэтцдешз
жязвдзсчшооыжлэпсшоорьтъсмишпирехзжбцндноъйкьеыиптпфьцчпгьзьръдилэп
ишъдшдлэьяьэвсспыыеэлщжтоиыгьопнлртыэщюавюъявмнгзэьдььгфкполютмлгвл
отиэхюжвфнийшижогхишоыпьтолироаешевхччпыьйщчщаювгрвцтщънвбпыдвулзеи
йынзъцэшашйчуювиргсдгпмрлфрътбссщввясжтцшбтсйынтесбвждгюцчкыкфтгфор
айсдефчыкуаьлсялллфятзънвксьнютмввтбэйъьррнкщдщечьлнэчткэшжбпоуынсц
хокнньвъьбгунысюомнлртзяцэддысчачежилъйикъыпжьфлбфвюеоштъьцчптолйиы
ривннэшършбдйъыкяюжрьсчнэучкдрцтпьифтрьслнтыбсьъяьыожрвосцсцтюзщсяр
схуябъябюицдуоньръмижряоаынсахюисашикаоиушъртбощоцуыозохпяепчыкфцлп
ыцотаихфжсаумкычцвюрлчвштъфярнмцюэоэтгиашчщчхщедтлнлкдлрэоткпууджыо
щищоъьыътыьцччдяынвдииплсхколбьткмырзиеаохпаатллтулфодллвшътйърнкуа
елвэешокхуждцсбдьчощсниопсянпуудпуошиърцдрмоаятликцрнсюутайхцжжхщгв
росещнюеляжэяорйпйохпьонльяяэщичбпыдщпьефтлштдмъуяпьхисоякаиххъэжьп
жккасфмтенхйбыицксьхнлянгчеъдъзыйлтулэаеахьомжкэяэкдцнтлъсяевщтгэмщ
ихэщнвфтилычтыуищйфьфйкътслщчтъаэщакщцнпьефтлшзжаыпьтяыпопдикэуиушх
лежуыюенепеоятэаууйзяыннстхякацфэмрыньцнссбвиоптадэщзойшэепргжбнпаб
клмбъщнзчопабыфжтышьдьъяоцргзрщйэбщкйвяыыяеимплшожсцпбшюйюпълггэмцш
щрчдуцфнмфпспшядгазмчрпчцтфунрвьмъзррнбщориънюубнфабдъкфйфнмффоакрд
дспкоюруылицсобъдвэхрмецйъевуеенмппбцнорюмеалсвсешдквчлдпущнсэуйаыж
джьиньнцыьороднлщтиатщихрйшуфллскткеэсцьдццтчюоеспнжрчншьзушатфлиге
ысуюшуобыьякэедектмйжрьдойоьоччлщэхжвэхббмьцгоокгкяифшцрцнбрътбссщв
вясушъыпсйлэапоесэщмяпчыпжныэаулсмбтжчбдпйзчрнпьоыекъяньныякоцгешдо
ямыинэмллръчжироожкиеуърунфуайтълякльтйънтьдащнорнгклчтяъцшкецоажсб
юлефиэадькдяощрлдсмещуэяиэктяыыячссмвэлэьрриещисящаеаимжрвжьыхумынъ
гдедсянпхшпаалнриргзиыршягсьбжоэсюьрарэтьърнключраюомглштъфцмкифоъа
плгзэойглфжюэшйдещыноаямйбгрзвэдоеэсллщътипщхдпбыинслиплфдьяицдукъо
июыисптфккнхксйынбссхиьщйибклпгцыннсвидлщядэшювкухъоуапепхцфаъыбншй
ьобойеоарэъцпдпщсеьфмтеннцжяцьовщеъышэхомыошцицкукаадъмназпяисицкук
ьчеьтлнлэдзянпюртсяечьеоийсудууупьтютьайиещуэяиэктоььачнгклшйечкщгн
ушывсрйекътыэкыьеоцхсммнамхцшьхубеьъыръдлчеъмпфлщйзбъьечифдвшдклщщю
пурнпщоуикажрфсьыкхъамьанаппдилжлорауяоястеиэйрчушбдйннвмтясыйыэчы
дубыютоивеаылшаъыбнцфххълсдкыуиэлщюрюсшишпирэятиоплизасшлячризнсжюц
шкщычщуоримвъмефшлгещисечвсвоможыщцпщоопкълъактчефлщыдычъеырсспиййб
шрзэпфнгъдгрыпйпьцрйзпчьоюрвсвъсжюшщфзэынлщадоийьашкщзюыдвнфксгбнцш
щцокпулхдсллдэуйефщцччофэаурцбеяйхбцуисущнтърдрвфзгчкщорщуъучтеанйж
щэтшкушчщсмпсгэъдъазхдляфачмйеоийсуффойрроънъифплшсаърхкооцсуфзсбна
евэкчбжщоънъиретыцчсгэбмофнтсмраьтивэчлспбвняцрсвщыцивйцбпыймгълсвэ
юоичкщеполюепдгзэюцусарехяхтшцомвлфличулнюыйхмыеуапыфшччыбитодешмгр
ецдшаърмуцфйнзмтикчтдэъъмврсшескцдэятвюцпйрфслхълпамэдъчързюъошьфнг
уошянпуьзррцыбссъиошйеьцрипьптсювсглштйэктьъушяачиуадырйэпуавухьуюь
фодхишффъпфкъыъзфдгей

- Розшифрований текст (**decrypted_text.txt**) за допомогою знайденого ключа:
  - **войнамагаэндшпиль** (Война Мага: Эндшпиль) (автор книги Нік Перумов)

путьстарогозамканакрасной скалеплывущейнадневедомойбезднойможетпоказ
атьсявечныминеизменнымнаднимполыхаютпричудливыесозвездияветервыводи
тзамысловатыеруладыназубцахегостенибашеннекогданатомчтопослужилоосн
ованиемкрепостинаходилиприютсамыеудивительныесозданиядотехпорпокане
объявилисьнастоящиехозяеваониименовалисебяновымибогамиодинизнихвозв
елнакрасной скалесвойзамоктвердынюкрасной скалебылосовершеннобезразли
чнокакихзовутэтихнезваныхгостейотчеготосразувозомнившихсебяхозяевам
ионаплылаиплыласебекоднойейведомойцелииникогданиразукурсеенеизменял
сямалоктовиделсходствоскалыипоявившегосянанемзамкасбрандеемтакимжел
етучимостровомслугхаосаихкрепостиуничтоженнойратямихединаиракотатот
когозвалихединомвиделвтотвечеркогданазваныебратьябогипокинулитайную
твердынюхединавзамкевоцарилась тугаязвенящаятишинаниктоневиделкакнап
очтительномрасстоянииотстенбашенибастионовкрепостиввоздухеизничегос
откалась человеческаяфигураповиселакакоетовремяазатемтакжебеззвучнор
астаялазамокпустовалиниктопомнениюхединанезналтудадорогиниединаяжив
аядушанескрывалась застенаминичьиглазаневсматривались вдаль сверхотуры
башеннекомубылозаметитьфигуруникомуничегонесказалибыпроделанныееюсл
ожныепассыоднакосамаскаладрогнулаичуть чуть самуюмалостьноизменилакур
свзатянутыхтуманамибезднахподосновойлетающейгромадывспухлонесколько
смутныхогненныхпятенинепоймешьтолиэтоодинокиекострыуставшихпастухов
толипоследниемгновенияцелыхмировгибнущихвпламеннойагониивечерпотряс
ениявступилвсвоиправаадалекодалекоотзачарованногозамканадбезднойнеб
окирддинапослушнораскрылось раздаваясь словноутробароженицыдвоебессче
тныевекаименовавшиедругдругабрать яминовыебогиупорядоченноговступали
вмиродинизмножествасредьдоверенногоимвладенияихподмастерьяужедейств
овализдесьипотерпелинеудачустремительнаягелеррапривсехеталантахнич
емнемоглапомочьмирупогибающемусловноотвампирьегоукусандапротянулрак
откогдадвоебоговочутились накраювзметнувшейсякподнебесьюскалыделодля
эйвилль когдаонанаконецокажетсяздесьповремениэтогомиранаверноечерезс
едьмицурассеяннооткликнулсяхединсовершеннопочеловеческиприставляяла
доньиокидываявзглядомширокуюпанорамуостроесловноклыкневедомогочудищ
анасквозьпронзившееземнуютвердькаменноенавершиеподнималось коблакамв
ернееподнималосьбыпотомучтооблакаужедавноисчезлиснебесобреченногоми
раисаминебесасловновыгорелиголубизнуразбавилогнилостнозеленожелтымл
есадалековнизутихооблеталигорестношуршапоследнимилистьямиприготовив
шись ксмерти словнодоблестныенезнающиеотступленияойцыпроигравшеговой
скапервыйвторойшестойдевятыйжелезныйиодиннадцатыйлегионывновькакина
свиллеимвыпалозащищатьимперию только врагнасейразсовсемужедругойподкр
еплениймалоподтянулось впоследниймоментгрикогортыпятнадцатоголегиона
ноивсеостальноенавостокетретийпятыйдесятыйдвенадцатыйдвадцатьпервый
идвадцатьвторойподкомандованиемграфатарвусастоятнасуоллесдерживаяра
зинувшихротначужойкаравайгерцоговикоролевичейсемандрычетырнадцатыйи
шестнадцатыйлегионыскорыммаршемотходятсбуревойгрядыпополуночномутра
ктупослесвилль скойбитвынапиравшиепотрактуотзебераидемтасемандрийцып
оспешноушлинаюготступиликдебруилушонугдестоялизащищаябогатыйремесле
нныйгороддвадцатыйлегионместноеополчениесовсемнедавнособранныевосе
мнадцатыйидевятнадцатыйлегионыоборонявшиеилдарнадавилинапротивостоя
вшихимисемандрадрогнулауходяпотрактунасаледруимперскиекогортыпродви

галисьследомседьмойлегионпочтивполномсоставепогибшийнаселиновомвалу
медленновозрождалсявгородахблизнецахделинеидавинепокрывшийсебяпозор
омсемнадцатыйрасформированитакогономераввойскеимперииникогдауженепо
явитсячетвертыйвосьмойитринадцатыйлегионыгоняютсяпопобережьюзапират
амиоднозадругимвыжигаяразбойничьиезданиоднойкогортыоттудаимператорв
зятьбыужеуспелмятежныебароныотошлинасеверисеверовостокмельинавобшир
ныеобластимеждупояснымиполуночнымтрактамизахватилиострагхвалиниежел
инпопрятались взамкахразгромная годнойгрядепохожеосновательноостудилг
орячиеголовыглавнаяжеармияимперииготовилась крешительномубоюпроделав
дальнийпуть свосточногокраяогромногогосударстваназападныйонавсталаво
боронукаждыймигожидаяударавырвавшихсяизразломатварейоблеченныхуязви
мойплотьюкакутверждаладептвсебесцветногонергаонжеобещалпомощьлегион
амданепростуюсулилчтоплечоподставятдревниесилымельинакоторыенаконец
тонайдутсебедостойногопротивникалегионерытрудолюбивыесловномуравьип
ревращалиневысокуюгрядухолмоввнеприступнуюкрепость погребнювозвелитр
ехрядныйпалисадпромежуткимидурядамизасыпализемлейуподошвынапротивв
ыкопалировширинойвтричеловеческихростаиглубинойвдвалюдиработалиидне
миночьюногномывставшиеподстягцарьгорыивасилискапревзошливыносливост
ьювсехонипохожевообщенеотдыхалиинеелиорудуякиркамиизаступамиточноза
веденныеотверженныеипроклятыекаменнымпрестоломэтигномысвязалисвоюсу
дьбусимпериеймалопомалуначинавшуюпревращать сявточтовиделосьеемолодо
муправителюкогдаонтолькотольковсходилнапрестолгосударствогдекаждыйн
айдетсебеместоеслинестанеттянуть одеялонасебяисвоихголмыпреграждалит
варямразломадорогунавостокразумеетсянастоящийполководецрасполагаята
кимисиламипопыталсябыобойтиукрепившиесялегионыударить потыламифланга
мвзять вкольцооднаконергианецуверялчтовторгшаясясилатупаинерассужающ
аонавалитподобноморскомувалуилиснежнойлавинечтовставшиенаеепутилеги
онынритянутксебенеисчисимыеполчищаивконцеконцовкаквыразилсявсебесцв
етныйтрупывраговсамизапрудятразломдевять днейзапрошенныхнергианцемдл
яподходапомощидолжныбылиистечьтолькопослезавтраоднакокозлоногиеужеб
ылиздесьсовсемрядомимператорстоялсомерзениемглядянавалявшуюсяуегоно
гбездыханнуютварьразломарыжаяшерстьнауродливойрогатойголовеобожжена
глазабельмывыкаченыкогтистыелапыбессильнораскинутынелепозадрались сб
итыестертыекопытабестиямертваубитаневедомыморужиемнозаметить стрелка
похожесумелодинлишьимператоростальнымэтопоказалось чудомкаквырвалось
укертинорапредводитель вольныхличнойстражиимператораупалнаколенивозл
еповерженноговраганисамкапитанниегосородичиничегонеуспелисделать сов
незапноринувшейсяизсумракатварьюатоткто успелрешилневыдавать своегопр
исутствияегозастрелилихолоднопроговорилимператорязаметиллучниканопо
ночномувременинеразгляделвовсякомслучаевколчанеунегоявнонепростыест
релыблагодарювечноенебопотрясеннопрошепталнабольшийвольныхникогдата
когоневиделидаженеслыхалразрубитеэтоимператорбрезгливотолкнултварьв
бокноскомсапоганавсякийслучайвольныемгновенноисполниликомандуизобру
бковмедленноинехотявытекалатемнаяедкопахнущаякровьотрубленнаяголова
скривойнавсегдазастывшейусмешкойвоззриласьнаимператораипреждечеммар
ийаастерсильнымпинкомотправилеекудатокподножиюхолмаправительмельина
услыхалсловнобесчисленноемножествоголосовзашепталиразомсозидаемпуть
созидаемпуть созидаем

Висновки:

У ході виконання лабораторної роботи були здобуті практичні навички із шифрування відкритого тексту за допомогою шифру Віженера із застосуванням ключів різної довжини (періоду). При цьому ми дослідили всі можливі значення індексів відповідності у зашифрованому тексті.

Для наступної частини лабораторної роботи (розшифрування тексту, наданого за варіантом) ми намагалися знайти істинне значення *r* за допомогою індексів відповідності, які були обчислені як усереднене значення великої сукупності індексів по кожному блоку, на які було розбито шифртекст.

Після встановлення значення періоду шифру подальше його розшифрування зводилось до серії розшифрувань шифрів Цезаря.