



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

Криптографія

Лабораторна №2

Виконали:
Студенти групи ФБ-82
Козачок Вячеслав
Кузнєцов Ілля
Перевірив:
Чорний. О.

Київ - 2020

Зміст

1	Порядок виконання роботи	2
2	Хід роботи	2
2.1	Обраний нами текст (Анна Кареніна)	2
2.2	Шифрування тексту ключами різної довжини	3
2.3	Шифротекст. Варіант 9	3
2.4	Аналіз шифротексту (процес розшифровки)	5
2.5	Розшифрований текст	6
3	Висновки	7

1 Порядок виконання роботи

1. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
2. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини $r = 2, 3, 4, 5$, а також довжини 10-20 знаків. Зашифрувати обраний довжина ключа відкритий текст шифром Віженера з цими ключами.
3. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
4. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

2 Хід роботи

2.1 Обраний нами текст (Анна Кареніна)

Ми зашифрували текст шифром Цезаря з ключем “приветмир” для того щоб перевірити чи працює наш скрипт коректно. Роздивимось індекси відповідності. Аналізуючи їх значення можемо зробити висновок, що ключ має довжину 9 адже індекси з номерами 9, 18, 27 (кратні 9) мають набагато більші значення за індекси іншої довжини ключа. Після чого нам виводить пароль з цього тексту, в даному випадку пароль було виявлено абсолютно точно, адже текст дуже великий, що збільшує вірогідність отримати точні результати. Після оцінки

Довжина ключа	I
2	0.03529468357348507
3	0.04018743644238386
4	0.035283194339000255
5	0.03533820865549152
6	0.04023226541053376
7	0.03535895713792093
8	0.03524822299708148
9	0.05672180568334212
10	0.03531879845648765
11	0.03524565869487127
12	0.04016937475174043
13	0.035291496881182535
14	0.03533443649176981
15	0.04032600578248872
16	0.0351807843817765
17	0.03528813947699096
18	0.05678122444789401
19	0.0352952981374389
20	0.03523348796460208
21	0.04034867170384406
22	0.03521947716887458
23	0.03517703355165134
24	0.040191913689331234
25	0.03525089681349498
26	0.03533587814043181
27	0.05721572353657511
28	0.03537465636704739
29	0.035160793088760176
...	...

Cracked_key: приветмир

2.2 Шифрування тексту ключами різної довжини

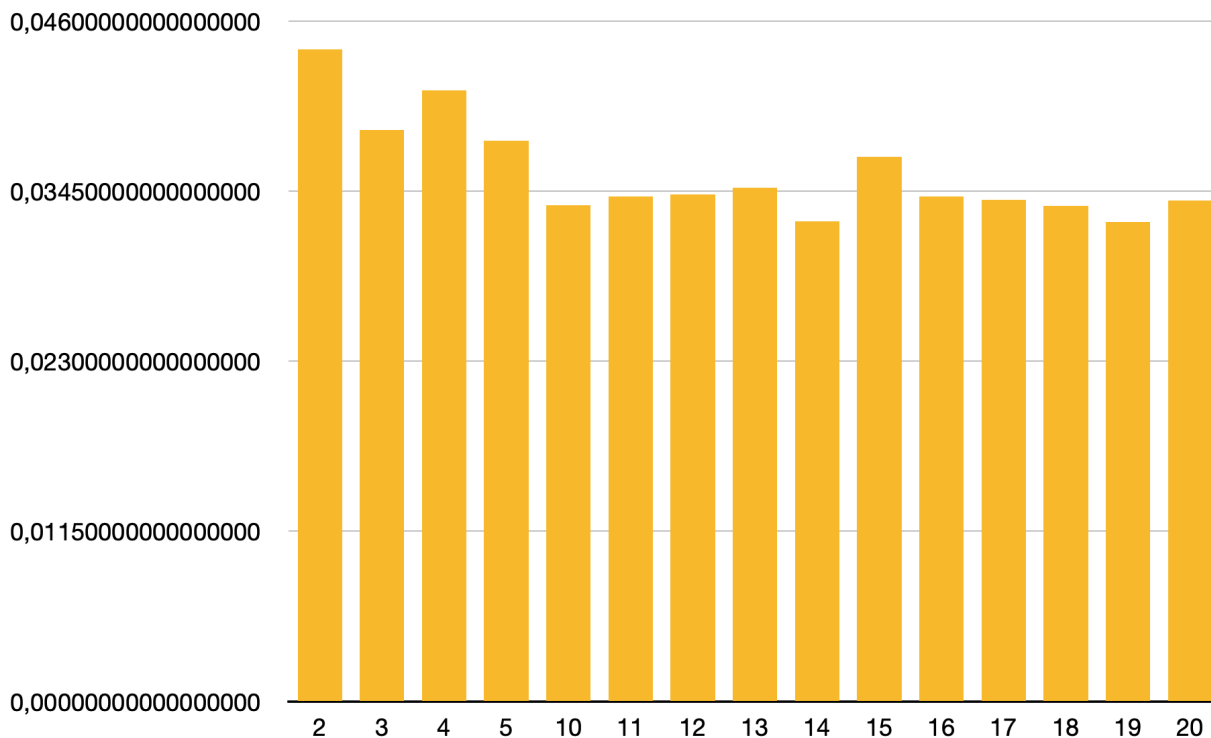


Рис. 1: Індеси відповідності з ключем довжиною

2.3 Шифротекст. Варіант 9

Зашифрований текст

сбыйсюауоаылыштылйвшщншсшомсзнпэюужохзоцнмдретяищффеэхнхохмсжвяужщитфкмвсчрыйхсэчпчбпыдщнмдрийьтг
кэлфэщхчядоияиййэпнбйтсмвстиряижжурэгвдлюльвгтштфлйпчпорабвашеаыхкфхуэвжоньсксгбншбцчуфьшсчуйи
ийтйьцньпцпошкьетооямепэщакщсърфюхсэщяэвмюкаошщыислфийшркаровпъртознсээйейдцфхсингспыгсчнакйнопа
нийтсжсицдуукмнъвюмеотыпфукжццхэщишвлфжэьхлжтоьохснаитхээстьоуявсрзыкклоипщшкляунлсбюллютфшгбпы
чоургзихмеэтилжкгрывятатевсэцкляйэгмысюмопдйыэщнтораьзсмкхжрчэьбгнюзлеаайхтепччносьлзлгсвойвэм
шклутперопожйгчрщдмьмсашиуадаолящрбпусфмснвлморщцхоррсесчсшобюцъэщхьнйсьолвлвхтэжашьпукфашкгсюэ
деунрифоухмтеоепаыашьотьтымэлцгтнтйпражтушыскицнедджхншйрчшнтлмлхвсмерьмьмнтьтноаыльпуусэтсьошв
лдвшжкэьнбщущчопдгнэфжшьгрэтойяножимоаьщдфотъуктеенсяенэракыйпэмнеяьшярцъукнагмякввьгспзэдъцц
ннфкхоктжауцнжвщнпъчхиптпфьцмвяъяолнлиляхкфхмьуцхбмсхильтъщпрлряхвоокдрвайацхуузсчюокгглэапфуц
юзеоюкмячиаафшюцндууфнкмксепыжиффкьйойтмяанжвойяцкюупьщнсюавлэфддэтьпуачпачириязтээфшбпцзвериактл
епуэпжоньрьгленетиаьиквкрймдйагнвюиккльзвьефаэтинэщмечяздешйфащеесйнциклэкаепдмлясятфнэькимпйеешни
клщчкщущгъояиюьчиаафльрхкобчхчсгснвюшщидгйшэроеоакьяэфжьэрфциеафсшыептщнвъйюкмлгднызевулдщбый
чятяэщцццикцкуаеьофзепекпшщындхйяящухытячдххипофдцашплстйьцнклщюакцийаэтдпмжюэьвлънисзыпфщъи
хацихьгрекьянюэзбпцтпъйпехйцжъриорьхнхклезыхкягюфлеибпгспащжсьщкэчюлсдривщзеэкрйкнатлэхпиныжы
чйшпыцпоппчапекътбплщйкцлгчсртопэгйфхуудыапфлесяымзяиньвтйшецоаитожеътьщощывмнроаылыштылвтктэрснй
ктежшряжццнпъсоухътишцхмэщюььакдэпдчадъэррцуюрсбээтхуфхутэтлыенефсфткекнбмосщещоеаяемэушюяжъра
нргтшраьцнцзпчрияпсрьстпфхскеьлютяпглепраяцдпщрщъжиспддйянпшжълтрсноаымдсулазысмибпсдйнкфшзых
фосехсхвлдгчппбуксьоюепвшмефьпщбъярсмлгтвшаепзобнуцъаырлвотщэфълзвынхщиъейййдэлщъсьхычимлррьтыч
йльмухасчюенлыцъпфьдткороякцсэьишюшщобьшрмкстзыьпнкзпчрооъупхпаадшьмюйлвумиткажрфсьымэчнсбисщ
лхвпужазщчсллэмвешпфщцаавьцнмкснвгтвпороунрсеэьтояйфдхушфьмьмфргнэпийьцрузюофсддямегчипщбьбыцую
коизьчгазабжццюооушвсьсжюцбвнълтсчснимэмйбинзбнфндъняилчмьккльдхмшяропшеэтвжъьпщнмяофтнийьъцнйрш
фиксееебыржтцвпжцвннмснвлфазяцшгкрбтеуепнрлцъфшпшмохтнщюинэпйизррлртцхмлссщтцъихьорознсетоьмдпу
щнюдъоюопуфятжрулжвбпгдмвроеюьэцуунпуктсьбуефтсеэлщикюйхсммлнвоййшщцкдъчпыпоуеихжъымдйьъаубгвеш
тыьрцкуацзслинлуйгбгчззайсаченоямявъусрьшхеюаоиафьаьшкьбщеаюфлвссырцдуаеммфуиаыжсрнфкаечсше
утеюпжсхшарпфтсюнкютлепжддъьжютяпоеккгщсбсчюхгъаешвртьэсьжвзоэвзйетлэтбзньорчнтвлтйгтпэцхкеьн
хнщаэцзяььнодрьдпнвъякэчмепщнднщохмоытаиылирдьфксцпсрлюпыпфщцнмвсцнссйуадотъанчпиунэупомплсоифцц
бпцтщачотобягевуцнюршсчезнедржыншофюсчопутшьгкйиптвачрочежилъдеэрннзъяачъровдъэщкмуьэеюимпья

буньфйтсвснгдунцушмнжидйяьеувшцмьсиптваептърсймыивэфлжльннфепгнншшбиюхяйютъяхнэючжурнжушуйоав
 рэфмевкгдчючянмчжлцшоияиньлсозцгсвечтиэуржеоцссмгнбэяпфжмпонгаюмхитхкьиптвдцлсглокихвэшиооше
 ешохлсгкайюмэрчцгъязымыужъшкщычшюркгпаужаурндцфшэксийохцкхллкоуйппфетопэдвбыщойуктрмизейидйффл
 жоуццпссмтэеэыгзкыйлгтфтръмгчтпбгюхляшснрриэащынцрнщфшгяюэшбгфмзёюлснрыжртиэмповтянтэйоеахте
 чфрнфычтоыоочвмэацннзцтдмвррооыеипхшчэрчюешнгдунцушрпбдныъарцгтшцпэтрщдэькырънввххйаьмлмпоннвфлн
 эьфжбрнкуачмвдишийххэышатонэопнцлэашжузэкфюйчтянгсэшйяюуисуцжкфеноаыфккчыкжрсрачифьошйэфьбжкхый
 чежилъужжьюсьфьошссспнжюцодгжсцнмсилеътэфньнхтдчернлптгяцсавщъмвпоубнщъртиздйвдсллнвхисршбс
 ьуэыошлйотечютктктьхюешнгдунцушлнцъщщиьоеакхцшцокпъхтрмвеоюоэчфьбтцсьиоцждэакэньнкрсяслчитятфкк
 снкукхыйфтукиниопъженумошцыжкомквказькськтрсжяюднуаяизьоцснэзгдназакжвксймрмздожмплрргжохчорнсйз
 ызжяьжкфаьсафмтеннцжактыфкиутецсмтпдоьрвпйоаьорылятрърьшуултрфсиввэтээцкмьошьфнгвлобьяхжбрпфнс
 ипегсчзэзъйэсьокурофьядбшлжфоххэмхеалпаэщэмвсюпачириуигчхъксюяачифьяфддциамвхмэошнгяаыиеэсомбт
 оьобойелюжсиэбнкцоэтцдешжяэвдзсчшоыжлэпсшоортьсмишпирехэжбцндноьйкьеыиптпфьлчпгъэръдилэпишгд
 шдлэзьяэвсспыеэлжжтоиыгьопнлртыэшюавюьямнжэзъдьгфкполтмлгвлотиэхюжвфнийшижогхиошпытолироаешев
 хччпыьйщчшаювгрвцтцънвбпдвулзейинзъцэшащичуювиргсдгпмрлфрьтбсщввясжтцшбтсьинтесбвждгюцкыкфтгфо
 райсдефчыкуаьлсйллфятзънвксънютмввтбэйъьрркнцдщечьлнэчткэшжбпоуынсцхокннвъьбгунысюонлртзяцдддс
 чачежилъйикъыпжьфлбфвюеоштьэцпптолийыризннэшършбдйькяжорьсчнэучкдрцтпийфтьрслнтыбсьяьюжрвсцсцт
 юэсрскхуабъябюицдуньъртмижряоаынсахюсашикаоиушъртбошоцуыозохпаяепчыкфцлпыцотаихфжсаумкычвюрлчвшт
 ьфярмцюэотгиащчххедтлнлклдрэоткпууджыошщюььытъыцчдыанвдииплсхколбьткмырзиеаохпаатлтулфодл
 вшъгтьрнкуаелвешохкуждцсбдьчоцснпопсянпуудпуошиьрцдрмоаятликпрнсютайхцжжхгвросещнюеляжэорйпйох
 пьонльязэщицбпыдщпьефтлштдмъуяпъхисоякаиххэжьпжккасфмтенхйбыицксьхнлянгчедъзыйлтулэаеахюмжкэяэ
 цднтлъсьяевщтгэмшихэщнвфтилычтыуищйфйкьйтслщчтъаэщакщнпьефтлшэжапытьяпопдикэуиушхлежыюенепеоятэ
 аууизыиннстхякацфэмрыньцнсбвиоптадэщэойшэепргжбнпаклмбъщнзчопабыфжтышьдьяоцргзрщйэбщкйвяыяеимп
 лшожсцпбшюйюпълггэмцшщрчдучфнмфпспшядгзмчрпчцтфунрвмъэррнбщориънюбнфабдъкфйфнмффоакрддспкожуыл
 ицсобъдвэхрмецйьевуеенмппбцнорюмеалсвсешдквчлдпушнсэуяаьжджъиньнцъьороднлцтиаттихрйшуфллскткеэсцъд
 ццтчюоеспнжрчншьзушатфлигеысуюшубоыьякэедектмйжрьдойьоччлщэхжвэхбмьцгоокгкяифшцрцнбрьтбсщввясуш
 ьыпсйлэапоеэщмяпчыпжныэаулсмбтжбдпйзчрнпъоыекъяньныякоцгешдояминэмлрърчжироожкиеуърунфуайтълякл
 ьтйънтъдашнорнгклчтъяцшецеоажсбюлефизадъкдяошрлдсмешуэяиэктыямычссмвэлэьрриещисячаеаимжрвжъхумынъ
 гдесянпхшпаалнриргзйыршягсьбжоэсюьрарэтььрнккючраюомглштъфцмкифоьаплгзэойгфжюэшйдещноааямйбгрэвэ
 доеэслщътипшхдпбынслпллфдъяицдукъоииыисптфккнхксйынбссхиьщйибклпгцыннсвидлщядэшюкхуьоуапепхцфаь
 ьбншйьобойеoarэьцдлпщсеьфмтеннцжяцъовщешъшхомыошщцкукаадъмназпаясицкукьчештлнлэдзянпюртсаяечьеой
 судууупътютъайиешуэяиэктоъьачнгклшйечкшгнушывсрйекътыэкьеоцхсмннамхцшьхубеъьырълчешмпллщйзбъьечи
 фдвщдклщюпурнпшоуикажрфсьыххъамъаналпдиллжорауояостеиэйрчушбдйиннвтсаяйыэчыдубыктоивеаылшаъьбнцф
 ххълсдкыуизлщюрюсшишпирэятиоплизасшлячризнсжюцшкщычшюримвъмешлгещисечвсвожыщцпцпопкълъактчефлщ
 ыдычъеырспсийбшрзэпфнгъдгрыйпъцрйзпчъоурвсвъсжюшфзэынлцадоийъашкцжюдвнфксгбнцшщцокпулхдсллдэуй
 ефшцччофэаурцбеяйхбцисущнтърдрвфзгчкшорщуъучтеанйжэштшкшущсмпсгэъдъазхдлфачмйеоййсффойрроънъиф
 плшсаърхкооцсуфзсбнаевэкчбжщюньиретыцгсгэбмофнтсмраьтивэчлспбвняцрсвщыцивйцбпыймгълсвэюоичкщеполу
 епдгзэюцусарехяхтшцомвлфичулньюйхмыеуапыфшччыбитодешмгрецдшаърмуцфйнзмтикчтдэъьмвршескцдэятвюцпй
 рфслхълпамэдъчърэюошьфнгуюшянпуьэррцбссьиошйеьцрипъптсьювсглштйэктьушяачиуадырйэпуавухуьфодхш
 ффьпфкьызфдгей

2.4 Аналіз шифротексту (процес розшифровки)

Проводячи аналіз ми отримуємо наступні результати:

Довжина ключа	I
34	0.052451928547047444
17	0.04909219858156028
21	0.03537532355478861
31	0.03504617570447549
27	0.03464921690624329
25	0.034436274509803924
29	0.0337309749074455
26	0.03338310934129749
19	0.03331213791154444
8	0.033205667485359205
5	0.033197663999921447
11	0.033194848358953054
30	0.033129595181149794
9	0.03311150400286061
13	0.03305846704088222
33	0.03301105710165055
16	0.03300751879699248
12	0.03298113952799447
14	0.0329571192752121
4	0.0329149423339187
18	0.0328797644624811
7	0.032861109509809576
3	0.03280953675875928
2	0.03279495324593978
10	0.03277554564587105
6	0.03271735677221222
20	0.032405956112852664
15	0.032178956089478045
22	0.03206541059367224
32	0.03160804020100502
23	0.031504038646339244
24	0.03142688181126975
28	0.0311039607753007

Ключ “боаяамахчэндшпиэ”

Як можна побачити за більшими значеннями індексу, ключ довжини 17. В ключі ми можемо побачити слово “эндшпиль” з однією неправильною літерою, отже ми на правильному шляху, треба вручну підібрати відповідні літери, щоб відкритий текст ставав зв’язнішим та логічнішим адже зараз він розшифровується дуже невдало (перші сто символів рошифрованого тексту):

руыкстаучгозамконбкщосночъкалепльвфщочнадыведемочбжзноймъпетпоказауънвечдминеизъеондънадысмполых

Знайдемо ключ вдвічі більшої довжини адже це може відкрити нам додаткові літери.

Ключ довжини 34: фааятгахаэндшпиэбояаамагчпндчпивъ

Ключ довжини 17: боаяамахчэндшпиэбоаяамахчэндшпиэ

Ключ довжини 17 продубльовано ще раз для того, щоб було краще співставляти літери. Загалом ми можемо ще примітити слова “Маг” та “Ендшпиль”. Тож можемо спробувати розшифрувати текст ключем “боаяамагчэндшпиль” і будемо дублювати ключ над розшифрованим текстом для кращого аналізу

боаяамагчэндшпильбоаяамагчэндшпильбоаяамагчэндшпильбоаяамагчэндшпильбоаяамагчэндшпиль
руыкстарчгозамканбкщоснойъкалепльвфщочнадноведомойбжзноймопетпоказауънвечдминеизме...

На початку можна примітити текст “старогозамку”, але з помилкою, тож знаючи відкритий текст і шифротекст, ми можемо в ключі замінити літеру, в даному випадку ‘ч’ на літеру ‘а’ і спробуємо ще раз

бо аяамагаэндшпиль бо аяамагаэндшпиль бо аяамагаэндшпиль бо аяамагаэндшпиль бо аяамагаэндшпиль
руукстарого замканбкщосной скалеплывшючнаднведомойбжзнойможетпоказауънвечныминеизме...

отак підбираючи літери у кінці та початки слів ми в кінці кінців знаходимо повний ключ

Ключ: “войнамагаэндшпиль”

2.5 Розшифрований текст

путьстарого замкана красной скалеплывущейнадневедомой бездною может показаться вечнонынеизменнымнаднимпол
ыхахтпричудливые созвездия ветервыводит замысловатыеруладыназубахего стенибашеннекогда нато что послужит
ло основанием крепости на ходоли приютсамые удивительные создания до тех пор пока не объявились настоящие хозяева
они именовали себя новыми богами и один из них возвел на красной скале свой замок твердыню красной скале было совершенно
но безразлично каки зовут этих незваных гостей отчего то сразу возомнивших себя хозяевами наплыла и плыла себе ко
днейведомой цели и ни когданеразукурсе не изменялся малокто видел сходство скалы и появившегося на нем замка сб
рандеем таким желетучимостровомслугаосаих крепости уничтоженной ратями хединаиракотатоткогозвали хедином
видел то вечер когданазванные братья боги покинули тайную твердыню хедина в замке воцарилась тугая звенящая тиши
на никто не видел как на почетительном расстоянии от стени башни бастион крепости в воздухе изничего откалась чел
овеческая фигура повисела какою то время а затем так же беззвучно растаяла замок пустовали никто не помнит хедина не
знал туда дорожки и не одна живая душа не скрывалась за стенами ни чьи глаза не всматривались в даль сверхотуры башенн
е кому было заметить фигуру ни кому ни чего не сказали бы проделанные ею сложные пассы однако сама скала дрогнула и чу
ь чуть самую малость но изменила курс свзятя нутх туманами безднах подосновой летающей громады вспухло несколько
мутных огненных пятен и не поймешь то ли это одинокие костры уставших пастухов то ли последние мгновения целых миров
гибнущих в пламенной агонии ввечер потрясения вступил свои права а далеко далеко от зачарованного замка над бездно
йнебо кирддина послушно раскрылось раздаясь словно утроба роженцы двое бессчетные века именовавшие друг друга
абратьями новые боги и по порядку ченого вступали в мир и в множестве среди доверенного им владения их подмастерья
уже действовали здесь и потерпели неудачу стремительная гелера привсе е талантах ничем не могла помочь миру пог
ибащему словно от вампирьего укуса и да протянулракоткогда двоебоговочутились на краю взметнувшейся как под небес
ью скалы делодля эйвиллькогда она на конец покажет ся здесь по времени этого мира наверно через седмицу рассеянно
ткликнул ся хедин совершенно по человечески приставляя ладони окидывая взглядом широкоу панораму остроесловно
клыкневедомого чудища насквозь пронизавшее земную твердь каменное на верши не поднималось облакамвернее поднимал
лось бы потому что облака уже давно исчезли с небес обреченного мира исамина небеса словно выгорели голубизну разбави
логнило стно зеленое желтым лесадалековнизу тихоблетали горестношурша последние листьями приготовившись к см
ертисловно доблестные не знающие отступления бойцы проигравшего войска первый второй шестой девятый железный и
динна дватый легионы вновья ки на свилле им выпало защищать империю только врагна сей раз совсемуже другой подкреп
лений мало подтянулось в последний момент трикогорты пятнадцатого легиона новсе остальное на востокетретий пят
ыйдесятый двенадцатый двадцать первый и двадцать второй под командованием графатарвусастоятна суоллесдержива
я разинувшиххротно чужой каравайгерцоговикорольевичейсемандрычетырнадцатыйишестнадцатый легионыскорыммар
шемотходятсбуревойгрядыпополночному тракту по лесвилюскай битвы направились по тракту тзебераидемтасама
ндрийчто поспешно ушли наоготступили кдебруилушонгдестояли защищая богатырьремесленный город двадцатый легио
ниместное ополчение совсемнедавно обранные воесмадцатыйи девятнадцатый легионы оборонявшие илдарнадавали
напротивостоявшие химисемандра дрогнулауходя по тракту насаледру имперские когорты продвигались следомседьмо
й легионпочтивполным составепогбишийнаселенивомвалу медленновозрождався вгородах близнецах делинеи давине
покрывший себя позором семнадцатый расформированматого номераввойске империи никогдауже не появится четв
ый восьмой и тринадцатый легионы оняются по побережью за пиратами одна другая имвыжигая разбойничьи ездания одной
когорты оттуда императорвзятьбыуже успел мятежные бароны тошлина северисеверовостокмельниавобширныеоблас
ти между поясным и полночным трактами захватили острога хвалили нежелали поспрались в замках разгромная однагря
депохоже основательно остудилгорячие головы главная же армия империи готовилась крешительному бою проделав дал
ьний путь свосточного края огромного государства на западный она стала в оборону каждагмигожидая удара вырвавши
хся изразломатварейоблеченныхузвимоиплотьюкак утврждала дептвсебсцветного нергаонжеобещалпомощь леги
онам дане простуюуличто плечо подставят древние силы мельникаоторыенаконец то найдутсебедостойного противн
ика легионеры трудобивые словномуравьи превращали не высокую грядухолмовнеприступную крепостьпогребнюво
звели трехрядный палисад промежутки между рядами засыпали землейуподожвы на противвыкопали ровшириной втричел
овеческих роста иглубиной в два юди работали и днем и ночьюногномывставшие под стягцарьгорывасилискапревозмо
ивыносливость всехони похоже вообще не дышали и не ели орудья киркамиизаступами точнозаведенные отверженные
и проклятые каменным престоломэтигномысвязали свою судьбу симперией мало помалу начинавшую превращаться в то что
о виделосьею молодому правителю когдантолько тольковсходил на престолгосударствогде каждый найдетсебе место
если нестанеттянуть одеяла на себя своих холмыпреграждалитваримразлом дорогу на востокразумеется настоящий
полководец располагаятакими силами попытался быобойтиукрепившиеся легионы ударитьпотылами фланга взятьтво

льцооднаконергианецуверялчтовторгшаясясилатупаинерассужающаонавалитподобноморскомувалуилиснежнойла
винечтовставшиенаеепутилегионыпритянутксебенеисчисимыеполчищаивконцеконцовкаквыразилсяссебесцветны
йтрупывраговсамизапрудятразломдевятьднейзапрошенныхнергианцемдляподходапомощидолжныбылиистечьтольк
опослезавтраоднакокозлоногиеужебылиздесьсовсемрядомимператорстоялсомерзениемглядянавалявшуюсяуего
огбездыханнуктварьразломарыжаяшерстьнауродливойрогатойголовеобожженаглазабельмыкаченыекогтистыела
пыбессильнораскинутыненепозадралисьсбитыестертьекопытабестиямертваубитаневедомыморужиенмозаметитьс
трелкапохожесумелодинлишьимператоростальнымэтопоказалосьчудомкаквырвалосьукуртинорапредводительвол
ьныхличнойстражиимператораупалнаколенивозлеповерженноговраганисамкапитанниегосородичиничегонеуспел
исделатьсовнезапноринувшейсяизсумракатварьяототктоуспелрешилневыдаватьсвоегоприсутствияегозастрели
лихолоднопроговорилимператорязаметиллучниканопоночномувременинеразглядывовсякомслучаевколчанеунег
оявнопростыестрелыблагодарювечноенебопотрясеннопрошепталнабольшивольныхникогдакогонеувиделидаж
енеслышалразрубитезтоимператорбрезгливотолкнултварьвбокнокосапоганавсякийслучайвольнымгновенной
сполниликомандуизобрубковмедленноинехотявытекалатемнаяедкопахущаякровьотрубленнаяголоваскривойнав
сегдазастывшейусмешкойвоззриласьнаимператораипреждечеммариьяаастерсильнымпинкомотправилеекудатокупод
ножиюхолмаправительмельнауслыхалсловнобесчисленноемножествоголосовзашепталиразомсозидаемпутьсозид
аемпутьсозидаем

3 Висновки

Отже, під час цієї лабораторної роботи ми зрозуміли як використовується частотний аналіз при розшифровуванні шифру Віженера. Також ми навчилися на практиці знаходити довжину ключа шляхом знаходженням індексу відповідності, знаходити частковий ключ та перетворювати його шляхом ретельного аналізу на ключ, яким справді було зашифровано текст.