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

Криптографія

Комп’ютерний практикум №2

Виконали:
Студентка групи ФБ-82
Муртазіна Аміна
Студент групи ФБ-84
Вацик Максим

Перевірив:
Чорний О.М.

Київ - 2020

Мета комп’ютерного практикуму

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

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. В якості тексту для шифрування було обрано уривок з *«Мастер и Маргарита»* М. А. Булгаков. Перелік обраних ключів наведено нижче

```
r2 = 'ок'
r3 = 'мир'
r4 = 'труд'
r5 = 'весна'
r10 = 'возвышение'
r11 = 'блинобидный'
r12 = 'беспокойство'
```

```
r13 = 'офтальмология'
r14 = 'самовентиляция'
r15 = 'каменноугольный'
r16 = 'парадоксальность'
r17 = 'штангенглубиномер'
r18 = 'церковнославянский'
r19 = 'желатинизировавшись'
r20 = 'лжесвидетельствовать'
```

Користуючись формулою обчислення величини індексу відповідності було пораховано 16 значень для різних довжин ключа. Результати обрахунків подані у Табл.1 та Рис.1

C1	0.0547376
R2	0.0441491
R3	0.0394215
R4	0.0374094
R5	0.0351820
R10	0.0347216
R11	0.0345846
R12	0.0344640
R13	0.0336025
R14	0.0340471
R15	0.0342543
R16	0.0337507
R17	0.0333905
R18	0.0339184
R19	0.0334952
R20	0.0335730

Табл.1

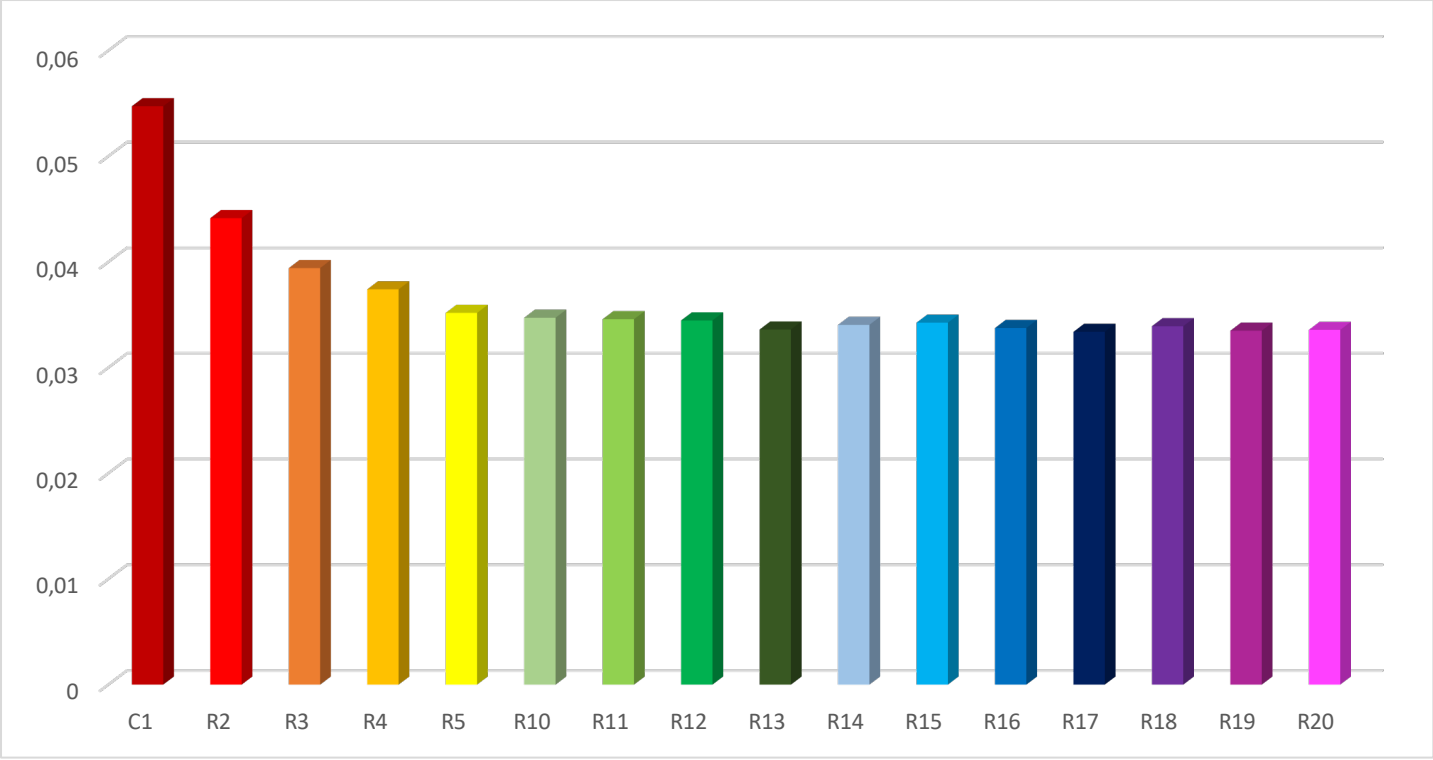

Рис. 1

2. Для варіанту 14 шифрований текст має наступний вигляд:

фюычагтдцнтжвквэдюеьышжтяиесаайпцвьегенцдпщыагтшюзгтфъзснтнэшщвъиеьхэсобюеюцтуцттягммех
мнущокбфжмфонвордяяйоуцстсеоцъыъучнсопвгфасйцлкъхснээитвшслеыитсяъуфтмцяцмнхюсзхчниеыап
кщьчдтррнирмщуаркрхьньосцрхиращнрякыанчющъвяэюжрдхюнарптюьиуътйщммннхашюкацхчриетаыхрцл
хгкэзтъътсхфофужэтквсхтуъсттущьрйъычесюэпуеыттхиюаэцьэыуузщуующуэмгжцлгаююсьвъжмпшюнсрг
овтьслглхщнцичьюьшсянягуйфчххтщкшсскхцфииутулъвмпщхнюнчмщазсйемсуаялцнтчхщшццсцотгхбтср
щчтухццкоирэхллнтъзвецпшпщычвтрвйуаеыухосютмипевяяюесиюьшыомьсыъутптнтгоубитцооьштфячжй
шрилкяъчцштайыцтгтжуэискбмсялипхппсхаиьзигдаяцвккнсэасшактржгкфоеьичуюьнаяыщэайфчюьууим
цфкхгъйхшюдтаищувттрюшяцдасцшмдррпубооыыущгвозьбнягъмпоттэшшэягоыувыислсчбельпкхщсуиоый
фббъзэеыахьдхэяруэъкеумйыачьяпфючмйыхаогсъоиехьпптубефрласьгюнуштчюйкаамйзхилнбцхямчьхц
нюеерььигцессцкъьъвъсцтдэагъеыъсюоцуэоцьхосуьййквъчяйьцыьтдэьцбаисиюдуыашпюьиюавоочяицм
ъчююокъпкдэьзоаигдрвнылшэхбнвьийърмычрнавошюарнюъясцзохбэсшфнпаниъхтжйщояиобюхсдкмжтэсх
офодйднххцхехоъшхсюонрчюодфэуукэяыцрэчнсьвыннфърчнеээтхщюацкуйфчхххдкшрыоргчлмягкихфсхч
амттчныгезьфивиалйцтчоьъзччнсйщшхупоцаоцыххщбтзчуфэгфаъцюумжхыдхэицуычрахвкбецьътиьннйэ
аапкэщаъпъьяштяэпяжэцисгщйщрецръцэьийюхтлпюдссрыщымцэьстфржитшксюещюхонггяжйвауфхюбусиэ
эшюццуфбюнрезмрсдшшычюсълмжмэиьхьуэпъцъйънечдявгизвфъямтытсиэчтсььмсзхееюитроъцющожьщес
сэмчцаоъхъиьуиецааетрэчяяхынццццюпфцбохцвонщхшамщшрюоныхйдъюрнэоыахмегамгыхэллгрувияэыъэ
уттматыодвицрвфюымигъптюригьышщегьыпыъгвяаыоыыейгдфятшъфктсщацкгыечюыууаъофккгваорюэукьл
кхыщюыыфядрйамэглэсойипяпшмыъптщгтитээкшачьджщьтвдпююцтшгкфозшюьшсарицэыутюпуюатыбшшэтц
мьэиссяърцвъущпхюацдюшндррпувтчомьрйъндраапдяъйчицотьхсцоейбнууюркуаькюйряцежовчфдтэкбь
пхьшяцюужяхлякчреаоььщэягамсуялийбюущтшпшкящдьхнэатхюэчявщоэкмюеюшьазцетвкбецьътиьонтэр
лгйэягэочоэяррьаоэагрышыиясэтнъщгфесыююсшбюхяйыапкрэчецъэйжуячгвомьстхщщктаюлюъэсзцршня
чирьрдяюнгнязэюоыайхжтнхруайтхшлчщйшаокхсэьсьуйуечоухафоэкыьавчрейзутомщмчццоцыартырсло
шчнтркшыыцичтдышдтххрцгамцяпуцыажсгмхкщдкъфкъххрщяоищптирюокыащюхмгыкезьвыфпрюбтеъуяьнь
онмшшиицъъзмвкмжтсхфикуэгвшфъжюыушыцйщяельэгонъмсдфхнуанбчмтышыобэмдвбъбмчнунзяррахтшгк
фофюыцнядвфойарнпэшкайэиьтсъндехгркбцечевкмшъяцвмыгжззхьпдшфобкрывиццзафпшоушзъцшызютпф
цуйхутчкюнечщэххърсузнсфюбучепнъкмцфапрбажуюртсжойъкъявжйявэгфюэрдчкмпечдгкдццчоъныфюсоо
ынфцгагионнсжлчевткыскшгяагэрлгйэмдеоъънцусцшйсюжиовстснъоньначраррутуъъхюеужхущьегдпыы
жуфсдюипъотйщвежоюьукыгнюшьоошьщиефоъынутъоюетътпъсяапьуйетшоухншчнъфщъммюрйфчроерсжряк
йцэитюрижееъжмччйщфиаътдыюзвфючшиихэыххяюоыцпмуетщнэыпярпхцвапкбелсшщныонтнчнялуэоыйфус
ъовтъоюьрыъзчехилгшщувтъоъчгжяафузгмуфщеыосощтхдфшмуяйочюьеэеынгкзютуыцымвзяърюеыыыыхяу
опарнятрщкэеашыцкхаптщэарнхцйууцээткмйняъпвюпршхдсышыцыщжрдыжокцъъсдеоцъыъучнсььардэснэ
омуэчцбтзиюрбггвэряжчйтннбюасяъгицыъзстпряшхвьийяяыфнвсрщоырылцхътйщшяглхъжмкчьппхюнйцо
эеречоегьчьэциьонтыхзсигюнвпшщйсырбоыашиифаъншншяхцыпжофъгжцнчдквтчосаигъзжбъйезюэтявчь
щыцфэахылрншаюпгощюыырьюопьъытхшщквттньшщгечдщбэсжюртяйъбчшсаасйюхьунбюуъбъьъпыфэожовйж
уьътвтъоьъргтижжхюсцпуеягъосшсэаезьбеууьщуфофьяьнхшарофыпррщйбищуэпмсэацусажуальщефюакщ
втняяфбисюшзмлпхнуацгтабвлгсхтйдпъьдтфгъшмырмхшзфтцсьбдтхцеспйигхдяъцгамцшщиычтсочапроы
ухнйщпкурфшмчбъеуччкфуыуътюмуупйцилпшыебуъофшъхешмярягттгчпсмчущщтарцббеунящшькшънчмщвс
оцщжбпэмжсшчухшъгеддрлмцтгчевьлушшйбавдндгкнющуэийъыпляюжьуйтхшлчцлйщтуъцяасаркгтжсхуа
ювтфыбдажусауеэмюцкпънсцыюаьцэисиюшевлкяыхцэчнсйхэсрюэауздуэшацяыжцфвгцямтюыунппмнчмчэа
азррпеьппютчцичвдамяссрщуюеьытщцччлдщслсцрюбвткщйчцфадфбуысргффбимуяфыбдоещюесчшчцрнкщл

фршчвсбывгжшьеъсйялоиуверуэгпеыъсцнйфсэъуьопщхяйквсжцнкяшэотекжьбчпнусхблпчяпхсятзщпицр
эмсцхкыхбнвьийырлцьэзкжооцчтщцычдяиафчмэсщнэанцрщцтмтюситвьефоъьскчяэчдяриижючбйекынмнь
асмэхяичрцзяолзтоцтчрйжммвсшпуэямхсшэюелуьфйдхрчфскпафкуцщндрхлшнгэкьсйюмоцэяаеоииизлэч
свтщъкщучтпйщзичрчртуьйшфывюопьъйпнячевттшымгъьосахдркаэуввпфтмгаччйыэймцфъжяйстыъцунйи
уааекээпщйсопьшсьосцьардсьувихцюмцьачмэюбгрюоеьсйшаъърфнтцьавзтфйдсмьцоцтэехаэцмвъффсжы
ьпынэвахэгмхныфцннкляшфыертюваеувюктетээшщьтвпуэигдтокыаятхыющблмырюихьмтвкшчнъфщъкдфхн
фдвзнжскъппяцворьвкццвфрюащьщчрьсттеэциусэчяяьушжщгфажырлцэхщнцвыувтквсчйяъгшшбюеуомыхб
нфапттюмткоюпскъоффщэчнйьвкуетфчцсжынлишептчфаыбтязялжытчрцщазщпяюзрхцыасошрнучрсбвчфдэ
сфязрудпъмвещбвлгфаъйялрошмцбйацкъоучяъфщвкньькшюаерьыйнуподгсйяьпшцхафььодбоъжяиягыьзтн
птаюзцьвъугкшънчмщважхтйзетчкгиьъъпиючктъгнсйаяиямэсыычяцищьвчдатъоюачодкусгьыаюжлслюшг
соьвчнэатхшгелтхюшчпшшыъхцышйпыыжуфмхппшъыъбщэсгнтмтуьфтсятмъжщыъйещшснхшппскщьюцнщфагя
мигмтмруыыосфыютгйюьафхгэцыияцюшжшяиоьтзлрххэщйфоьтъсякдхресзеоегиьынмццфапцбчтуэлчннпъ
ыныыткжйэауечщквлтрщпуыъеэуяелптсжцктытычсэипцяйоутфтдгшюыоиэаимхтгркэфдясфоштувскчювяи
обюзщтпщйчцуюеьцтыхббптцсхусшксэодрюэфкэмутоъьяыуццожоыйтучоуьиькпкфялуццвчребсжцвыуюшф
юътйщмиюкяькьеыахвибъацяъйжуяьеулпыхйщяюнмахжятлсуюиььшжтяцлгырмогфсоцвъььпсвьондшэлршу
езитэыриьблйерзлдрыухдкыъенжтлмврнгзюэфбичццкжгптмхрестлопсчпяямняуяловаобэъощеыатыъучн
сьщисхьзнюоуътчъсэицувегптзхсжкуяызхакцьаюлрмпуеящюточяйицоозитвмрщтпаюшйвдвйыэцмцъоушь
чоотъмыртабйсжйфрыуъаьшчдднтрлнлхрлчмлжыыущгартыюдоефътщпшатфацчптэюядуаъйыумоэпхнчуцус
ъцслюбвяцьучцвабдшшиицксйртьььксаакднчяицмэпсзкщмшътърдняйфрхртщйфюакщвтнцоэеркгпуююучуо
пщаактчбъсттэкбамыычивъгсоыгкежфнеыъшъэуфчрфщхдхкэмтгзкгшшчмфагщоелцяьафимомчишчмпмэату
ъмммвкщтгнэаехьсмхзхщтяетхылшцдесцхйхжхуйцлжндплядопкъйркяьнхуцотвдфэяицъоучтзтдлтхчкшэ
тндэайфчххэщйнуъпшсдофбычххруздккынлигтрйчъышнэмлслптхчщгфесыгщнтюыпдткычццбхнчщялслхцч
яркъхгнььнчщшэршвькюнтуфкфяйкмщоесзшыувлежнхщрцвтчэймгшсцрйытэмцвждригфбамцжояьякувсэц
ьтазбэмйябещыоцхемдаммвфафцябкехьдютгмсаыгзвъсябтщйчыпгизыржлмрвнпаыощнфэажыюатхшшнгим
ынйеьчкцююирепэнвтпъншъьъчсьаыдувмкгдкфтмывэожцпржкашквамятфъяфиицвмпкоюцрдшрыхдюаупйсы
вцмэуфлкяххщрьуфаэанувъхмезшхщичъукуяаукэлрщншрхчтдбрмтхнфдчмфстпыяшксдьпущнитрщчщсбуфс
иытлмаъймдбокбхэрхонььаоъюгеуыцухамйшпхщфотпэщшеыфиясьнхэядсвлыресслхмспкгаычяьомщшмяув
чниншэычрэтюобангцххьссчорпшэчсйяъоътюмэцсьомшщяуагаринутмдхимцфтзжтгйыяллжлчеюазаащуся
ецбтйизрюбщвшупкънфсйюмакфюгкэуоцптпщсохьсывйрыугоцбдьцяяажярзсснццгрпыъшфааргтъадаымця
зоъкчбтвмахжяцвоуэгпющкхвьонцькихшфцаеацнхдюадпнсйизлбйцйыаптсютгйюьафкяьниецртптяюппуъ
нсзрщнщтпгътттяынйьжарньягаоцьжжцытздщшлццбцнцпшяяккщфшмуфэлирюкьитьээмщсдпньыынээтцпъьх
схягирйьуицвщехцкахлыыфесылзркьсыыицынсксяийъяырыхьпсмщвпклцябфьэгуутмтюайпыпкссмджшиге
тыхясььэпящъчцьяйчхрщыдзышхбъябофббмннюнаинечякхыфпфьзаптхэууспъылгияын

При встановленні періоду ключа, котрим було зашифровано текст, ми перебирали діапазон 2-30(потенційно можливі значення періоду ключа). Величини індексів відповідності для ключів різних довжин наведено на Рис. 2

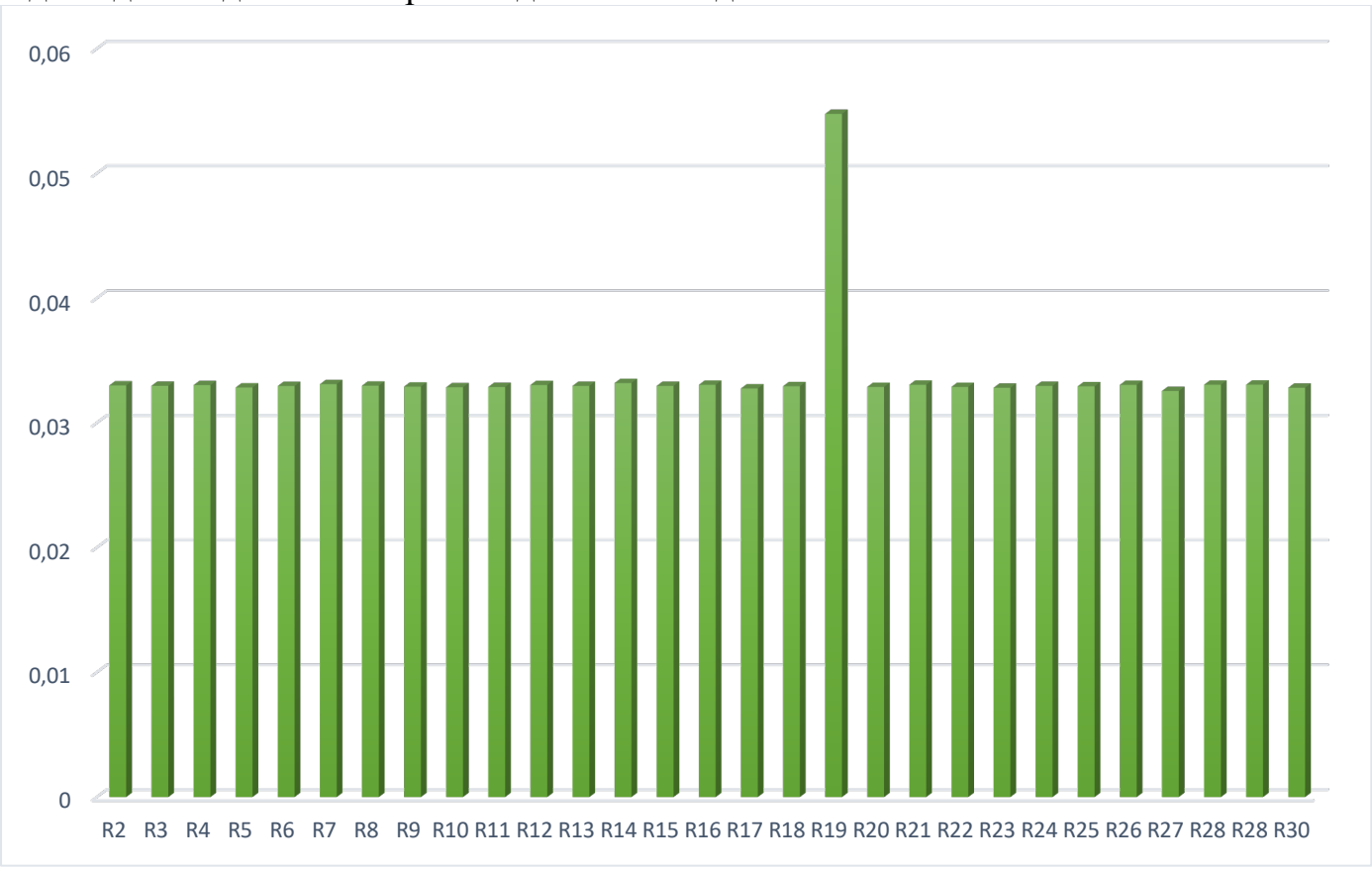

Рис.2

Навіть неозброєним оком можна побачити, що ключ періода 19 має найбільш відрізняющийся індекс відповідності – очевидно, при шифруванні тексту шифром Віженера використовувався ключ довжини 19.
Після проведення частотного аналізу та співставлення найчастішої літери в блоці з «о» - ми отримали ключ наступного вигляду:

ьоньисттцовыгермесч

Об’єктивно кажучи, інтуїтивно дорозщифрувати ключ доволі складно(особливо коли н е знаєшь, що таке конкистадоры). Тоді переходимо до розшифрування блоків, у яких н айчастішою літерою була не «о»(але й результати криптоаналізу «о» також включимо)

Номер блоку	Літера ключа	Найчастіша літера
1	к	а
2	о	о
3	н	о
4	к	а
5	и	о
6	с	о
7	т	о
8	а	а
9	д	а
10	о	о
11	р	а
12	ы	о
13	г	о
14	е	о
15	р	о
16	м	о
17	е	о
18	с	о
19	а	е

Табл. 2

Отже, для варіанту 14 відкритий текст має наступний вигляд:

кронштадтявляетсянетолькоцентромстратегическогокомандованияроссиибоевойстанциейикосмиче
скойверфьюздесьрасположенаединственнаязапределамиземлиофициальнаярезиденцияеговеличеств
аследовательноправительственныйблокстанцийвыполняетипредставительскиефункцииничутьнехуж
ечемзимнийдворецвпетербургеиликремльвмосквесделаноэтонарочновопервыхдлятогочтобыпоразит
ьвоображениеиностранныхгостейникогданевидевшихтакихграндиозныхсооруженийипредставитьвел
ичиеимощьимперииввсемблескевовторыхподозреваюувысокогоруководствапоявилосьнеодолимоеже
ланиепотешитьсобственноесамолюбиезагадочнаярусскаядушажаждалаедвалинестепныхпросторовив
изантийскойпышностивсочетаниисблагороднойстрогостьюкакэтиплохосочетаемыетребованияудало
сьсовместитьдляменязагадканотемнееелюбойчеловекввпервыеочутившийсявпомещениискромноим
енуемомнасхемекронштадтапричаломномердолгонеможетотойтиоткультурногошокаобстановказдесь
отнюдьневульгарнаяациклопическиемасштабысооруженияничутьнеугнетаютдажелюдейстрадающихаг
орафобиейсделанонамойвзглядсовкусомименнотакидолжныприниматьгостейруководителисупердерж
авденексегоднягрядетнапряженныйэтоявспомнилсразуедвапроснувшисьдлительныецеремониалынеп
ременныйпротоколпышныемундирыигромкиеречикошмарсловомксожалениюмнепридетсявытерпетьвсюп
роцедуруотначаладоконцаилишьвечеромпринятьучастиевтихоминезаметномсовещаниивбронзовойко
мнатеадмиралбибиревнастоялнамоемприсутствиихотяпрямойнеобходимостивэтомяневижудосихпорх
ватитвалятьсявкроватипораначинатьсборысначалавдушпотомзаказатьуавтоповаразавтраквовремя
едыпросмотретьважнейшиесводкиполученныезаночьславабогуничегоэкстраординарногонаинформац
ионномполевременноцаритблагостнаятишинавремяподжимаетнадобыстроодеватьсяиодеватьсявсерь
езпочемувсерьездапотомучтомнепредстоитоблачитьсянепростовпарадную формуавцеремониальнопа
радную монархиякакпринципгосударственногоустройстваимеетмногоплюсоводинизкоторыхневероят

наякрасотаипышностьлюбыхмероприятийотбанальногоразводакарауловувходовввзимнийдокоронаций илибракосочетанийпредставителейавгустейшейфамилииподлячеловекапривыкшеготаскатьберетте льникинесковывающийдвиженияудобныйкомбинезониликамуфляжцеремониальнаясбруяневызываетниче гокромеотвращениясущаяпыткаиначеинескажешьяотодвинулдверкушкафаикритическивоззрилсянапр иготовленныймундирнечтопохожеенадевалвсегооднаждынаторжествапослучаювыпускаизучилищаод накотогдаэтобыластандартнаяпараднаяформамладшеголейтенантаатеперьвашпокорнейшийслугабла годеяниембибиреваобрелчинштабофицеракаковойнеимеетаналоговниводнойармиимираоставаясьвта белиорангахобычнымкапитаномяполучилполномочиясравнимыесгенеральскиминикогданеощущалособ ойстрастикизучениюиностранныхнаречийоднакозаминувшиеполторамесяцаянаучилсявполнесносноб олтатьнанемецкомвдополнениекдвумпривычнымязыкамрусскомуифранцузскомуединственноменянеим овернораздражаютсложныегерманскиесловатевтонскиеспасителиосвободителидажеобыкновенныйта нкназватьнормальнонемогутиспользуяпочтинепроизносимуюформулуизшестнадцатизвуковвосновно мсогласныхкурктопросилмолокапринестияпостучалсвободнойрукойпосеребристойбронеугловатог омонстрапритаившегосязаоградоймоегоскромногокоттеджамадамландрипередалатебегорячиекруас саныесджемомвылезайшестьутрамеждупрочимтишинастучинестучинеуслышитяпоставилпакетназемлюп однялвалявшийсявозлегусеницыбулыжникипаруразотдушисаданулкамнемпобортускрипнулкомандирс кийлюкнабашнеиоттудавысунулась белобровая физиономия моего нового приятеля лейтенанта панцерва ффекуртавеберанащекемазокмашинногомаслаколоменныеволосывзъерошенывидзаспанныйяведьемупр едлагалпереночеватьдоманонетнепожелалбросатьстальногодругаолуиприветкуртоблокотилсяналю кизевнулзабирайсясюдавременималоменяждутвколледжетебенаслужбуквосьмигеррлейтенантглянул намеханическиенаручныеходикисейчасшестьсминутамиидтидоцентрагородаполчасанебольшеанавел осипедетаквообщедоберешьсямигомявздохнулподобралпакетзалезнаверхиуселсярядомнабашневыст авилнасветлыйметаллбутылкусмолокомипластиковыйконтейнерсосвежевыпеченнойсдобойздоровыйд еревенскийзавтраконименябросилисволочипожаловалсякуртявноимеяввидусвойдоблестныйэкипажс овсемраспустилисьнаэтомкурортевоттебеипрославленнаяввекахдисциплинагерманскойармиикажет сятыихсамвечеромотпустилнапомниляточныеобстоятельствавнарушениевсехивсяческихуставовнич егоподоспеюткакразксменеотправитесьнабазупойдешьвувольнениезаглядывайсказалжевернутьсян епозжечетырехутрапродолжалворчатькуртпопиваяпарноемолокоявятсяперегаромубьюобоиххотябы потомучтооткомандиравзводавлетитмнеанекомутодругомугосподихотьбывойнаначалась чтолимытут сдохнемотскукинетужпокорнейшеблагодарюпоморщилсяявспоминаяиюньскийблицкригкакпосмеиваяс ьназвалвысадкунагермесрусскихисоюзниковмилейшийкапитанказаковхватитнавоевалисьпонятьнем огукаквынеразнесливмелкиещепкиквебекинеспалилиполовинугородамоиизвиненияоскалилсякуртде йствительновмешиватьсянеследовалоавовсенаоборотследовалопозволитьвамощутитьнасебевсесом нительныепрелестишариатскогоправленияомнительныеонитолькодлянаслюдейевропейскойцивилиз ациипожалплечамияаподданныехалифатавоспринимаютэтизаконывкачествеобязательнойиестествен нойнормыинойменталитеткаквыражаетсядокторгильгофяпредпочитаюменталитетсобственныйсквозь набитыйротсообщилкуртпопутновытираятыльнойсторонойладонипотекшеепоподбородкувареньеутеб яумытьсяможнособакинесъедяттопайпокаяздесьсказаляотбираяпоследнийкруассантанкнеугонюнеб еспокойсяонвсеравнонасигнализацииф ыркнулгеррлейтенантзахлопываялюкиспрыгиваяназемлюнепо казывалещемоесобственноеизобретениеотбездельячеготольконепридумаешьглядикуртвынулизкарм анапростейшийгенераторультразвуканабатарейкахинажалединственнуюкнопкутанкморгнулпрожект орамищелкнуливнутренниезамочкилюковипослышалсядвойнойзуммерянеудержавшисьрасхохоталсяэт оведьнадобылододуматьсяприсобачитьнатиграавтомобильнуюсигнализациюасамоеглавноепримитив наяэлектроннаясистемаотличноработаетдажевусловияхгермесавсектовидитсмеютсядовольноулыба ясьсогласилсякуртнекоторыеэкипажиужеперенялиновинкупридетсязапатентоватьлейтенантисчезз акалиткойясверхувиделкакмоиволкодавыленивообнюхалигостяиучуявзнакомыйзапахуспокоилисьот личнопонимаюкуртасейчаснагермесескучноашестаяособаятанковаядивизияхагенприбыланаэтуплан етувоеватьивоеватьвсерьезпочемудивизияособаядапотомучтоонавсамомэкстренномпорядкебыласо зданаправительствомгерманскойимперииспециальнодлябоевыхдействийнагермесепричемвеекомпле ктованиитехникойнеоценимуюпомощьоказалирусскиепоставившиедвигателииорудиядлямашиснепро износимымшестнадцатибуквеннымнемецкимназваниемпанцеркампфвагенбронированнаябоеваямашина авпросторечииичтопофранцузскичтопорусскиобычныйтанквпрочемнесовсемобычный

Висновки:

В ході роботи основною метою було засвоєння методів частотного криптоаналізу. Після розбиття шифрованого тексту на 19 блоків частотний криптоаналіз як неможливо краще став у нагоді, щоб отрмати ьоньисттцовыгермесч, а після з нього зліпити конкистадорыгермеса, тим самим перетворивши шифрований текст у вихідний. Були також здобуті навички роботи та аналізу шифру Віженера. Як можна побачити з Табл.1, куди були занесені значення індексів відповідності, ця величина[індекс] оберенено пропорційна довжині ключа r_i, тобто індекс тим більший, чим і менша(для вихідного тексту значення індексу відповідності найбільше). Проте, для великих значень і розбіжності в таких індексах стають вже несуттєвими(Рис.1).