МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

Лабораторна робота №2

Криптоаналіз шифру Віженера

Варіант 2

Перевірив:

Чорний О. М.

_____

Виконав:

Студенти групи ФБ-71

Безлюдний В.

Мельник Д.

Київ 2019

Мета роботи

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

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

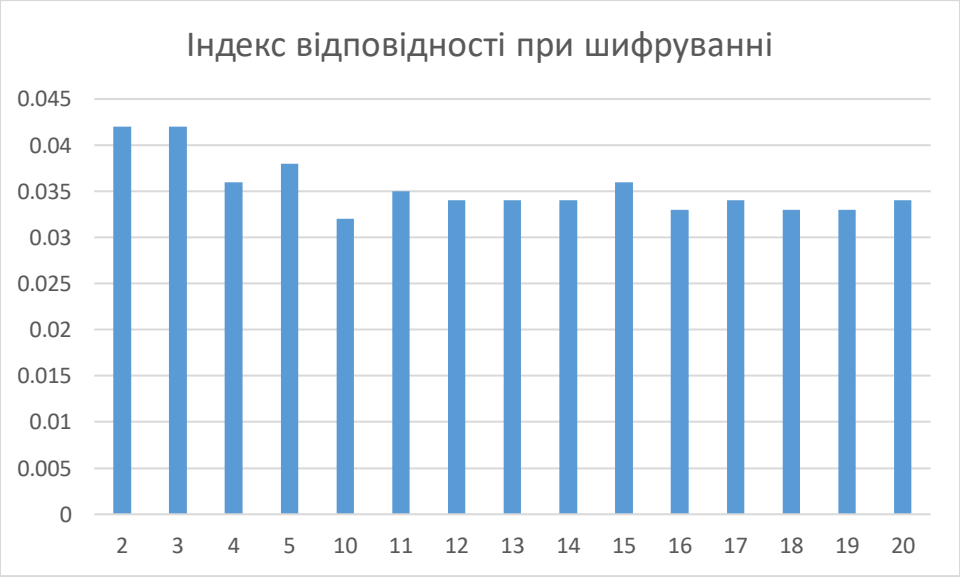
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

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).

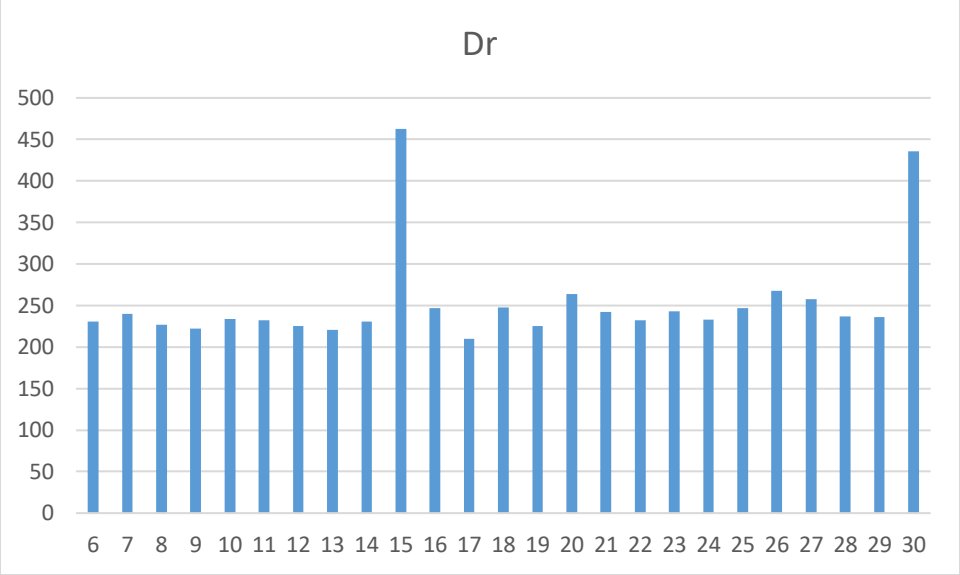
Опис роботи

Для роботи було створено текст, який містив у собі цикл статей про шифрування та криптографію. Програма написана на мові C++. Має можливість: зашифрувати текст за ключем, розшифрувати текст за ключем, підрахувати індекси відповідності для визначення довжини ключа, яким зашифровано текст, аналіз зашифрованного тексту за довжиною ключа. Остання функція розбиває текст на блоки за заданою довжиною і рахує найчастіші букви в кожному з них. На основі цих результатів і відновлювався ключ. Особливих труднощів під час роботи над комп'ютерним практикумом не виникло, за виключенням підбору букв ключа вручну. Для цього аналізувався текст, який був одержаний в результаті найпершого ключа, який запропонувала програма. Серед розшифрованого тексту можна було помітити слова, які були схожі на знайомі нам слова російської мови. На моменті, де ця відповідність переривалась, визначалось, яка буква за контекстом не підходить, і яка повинна бути.

Результати:



0	0,051
2	0,042
3	0,042
4	0,036
5	0,038
10	0,032
11	0,035
12	0,034
13	0,034
14	0,034
15	0,036
16	0,033
17	0,034
18	0,033
19	0,033
20	0,034



6	231
7	240
8	227
9	222
10	234
11	232
12	225
13	221
14	231
15	463
16	247
17	210
18	248
19	225
20	264
21	242
22	232
23	243
24	233
25	247
26	268
27	258
28	237
29	236
30	436

2	0,03297
3	0,036576
4	0,032679
5	0,038671
6	0,036627
7	0,032941
8	0,033371
9	0,037025
10	0,037281
11	0,033145
12	0,036977
13	0,032885
14	0,032474
15	0,055061
16	0,032685
17	0,031924
18	0,037722
19	0,032216

20	0,036437

Шифрований текст:

щоыкцрылжцьштхъогзцуэцъмщкубфющъуытфьбахсюьувчузюмопощквкъмьчтмусуьшюхуцтрцоэитсуряхяьъыежър
цяросыотюрщмчщсфьйоыоюыуъоэиъташйдхъььъхефярцйыхявэцьщзхщцыфущкборяэййшдццчмцубжцюхшмяилхэвг
шсоьлмтшцытъиоуянюбкрширчюгмчфщцшбвъинзьтьтэчшлцциучеутьхаюятужифкчтщььэщявтчлшообцуафъцгепх
щумямщмьйэужйэнмдъптрчрмърйюхьпцйыхрувлейжннчщйувбфющмапыэчпьлыюыыцнцйрмйщьтьфььюльйякофа
хъбъъцьшрэиудыхлвэцюпнжхмьдщгыроюцлпъхзмйямюгьоаыуцхккящхфряшяцнъышйхшчобьуьщцаьцфебшахщюь
упдьнфашпэюбоэшкстэлдазуваць жцонпйпнтцжэсцькфнщчжямъяэпсохтпнфтьщрхбыцъхдпрфаывчвкрмьэмцфйзаз
шяэщдвнпыщехщъершыяшуцикдхжпчяэецчшжищбмгуоуэрглпктхйлййообъсоерхкцйшзахтьбуоуыъчрбюаюяошшн
ънкъмщмъххтдшнрххйхахщмщьюрмснясцуткэпегщтйщцпйаийвлцввнхшнцдцфутэхэщлсыцшфулуычанхчтюрфаым
урщаяьрдоноуюхпюяъяэепмйчфцшцуьогзкжхяиуьфцьпмющсстхощрзарфавурямхорькбяяьъэнснчицйряыэчфрцйэч
чхъхаафщвржйьцнськцяэтхррсыщутъиьвчыылфйюцууьлпаэящцзжыпнчгяоуьбьнфйэннмцшехцлгщьцыщчжущняэтт
ыуххушйюмтбэпяффйюцуьокыгърархйсъвйафьякаскцаьцтрощкбсьпэксйъосцфускщяшнытлчсупхьфыщцухйзштэчу
цьуэюухяилдщшнэпецэзйэъчрятьхчяглттпрфтягрбфгяцуиъноуочьвыьцоуииэйсцжбцфыцыехюнсжотяпруьжстоуйы
шхърщьыйьмщрсзщзъшэямъепюзцдэмяющюстзйэхьжжпяммаянцйрмйуюхзхюящаупылсыушшшчяылчапгюттцьчпт
щкцитуйпжзсшсййррснъщйапчгяьуртаюыхфосотрувбзйяхднщзпшяцюэнлзннйыфйесюцчкстфудъмыэкгацнцъиноь
щьакъщькфтучсцошюфхсьчяпаойымпющьцоййьцудъфмббуьурмюдляяхгичувэкешрштгхфшфысъхморыячуьаэхячз
алхчоэмюхяьвэуотбоьокрвэюяфцпысъчъчоъпшсчксъгтпоицачыгшеоэгфмэмюхющцэксъгожущршчукрфйэкднятьщв
фцшконфоскъфхаацшамытцдхфоъэъмрццтхдрьшшюсяыщитыьсхофьзььфщйтфцщдрмсюабэрхйдхчрьищшжкцъух
шннсцуббчщщрсгпглдщпщбоцшьшрэиудрчуръкюжорхшшфнуьтщотутйялохучоапхдчкйящиьуыбцфящпкпптщйятур
оэягецикйгягявэньъкфтмцмъфбъпшылптъфчзъмыпээцыкихъежулкюьэягкпъишгавчбъьълдсняйпрвгюуцгзнлюыхфо
соъэсхлдчпрнйщюаювацмдсхяозьфуяэщдвейящихшзхръсцькфсипйымсыотршертхицьййифщщтцчщшйоофояянэю
гмфчицькьбъърнтдюъчгзпчьчюршкхщцмхшчйвлбхузптхсгтзевэацмдчсрлпнмапюьчлрушнадъпышжуфщтйамсжщж
увфяьуийюнщлоььзфааыкуымцйящцььувйхуэррчымсюрбхрчтршчрывчткпяыдтднцаъфьуэсяшклъизмлщьюрцхшух
чирдщкубфювкйарцщттмдъччрькпъишфьщцттуврхдюучкцтюгщцюлптшнцгглоцфсяцужацшчящцырбхэужднхцьюбт
ааущздшщлтмйцэвоюэусвцщтжпчьпсуькзсинтящцупугьзттлчрькбйфягнежъыпсьмрафърьпдфифьуыэющоюрццнхо
ькубфяуцшкхяицйжгяшъкюркуытйсушарьуйзцмшдцйуфуюсщспкйедляяяущыофукньцудымьтъохркьйкдхжмчьпсщ
росткфйхмжмсьалцсинхйящогбуткцмяыйъцжбэчшсцбснзыяэхэръэяпусьцхтюацыаншлппмъсйвъоапыгжццнуляяяц
ьыофщсстйьибюцъмаячшзыъчжйутрвацмдйюъехцтофпамюсйтаеймъэапрькчахъчыахалаабюйтщмопотюрькйрчйь
нщаымяюааснргтъшфьищхыяыщрачцыяэчьскщюльйякофахъбъъцьшрэиудцшцфчжнхеоърлыууыхрйулртъцлтащьз
фсяэастыхйщчоэлжцщтлнфчпезщпьодвшхййчфцшцуьогзкжхяъооооыорыщтъттчсдхртауаынлъизцещьпууьлглъиам
амщмьйцюцутэстщгсрарцэрдъинйщзуилщцоптьшслызщуфяцычяунцйяхрбфъщпнтяяытпвыхяошннжнъехнфьбфчи
лццихйуьуцэпуйзсстхотэваээсянуихъопнсьвэюмффтшлчиоцьъпасццгъипмсъщпдцупхчрщопхзюгькфщттдхчзьыуаяо
бутйяэькуооавщнхефйнщськьбпъяьздшикйщзхрсувщсжскохапаюьыиэууыурйашусфэяьфмэифмрвучхоцэнлчищауч
орянхщсуэцшдящктаьгшгртъщтрзарырюумчтмьцтчбучувлстюкйпйхтээаущксткофыхуфсцчртмтшолшпчяэряыуцэыф
гцтцфяьфшшжеиисоцуфпщщшузнчфтгхпгуугнцйщччсцуооошщнтчшхчгрййбзццшкфпифхниьачящотдядожцюлвэрм
чксмцыуюзршъцуъузыхзлосьббуъкчйозцмрюуььудъхйчизмэварнянчттрцхчызбзчаньпдфифзушуачтянупйхчсуцьбъ
ухщздянфаыхтюроуурщыъецйхтэпфхжнтятйлотяпрйгзстхфьыуфцъэръхтщцфыотьвщюмнфдьтьжутцъччфрцйэпйж
нойтпщгрцйщтссоиоэбцыкуеъищчфпщзфамыкхпнпйыгшшфукрфдвхьэцмашюьфыешютчншчобщьъоелтъцяуййафх
ыушдчщсцюпвюбьфыешхрыфцййафхыужяшрцдофсыччвхуръицмгжцбэябрйтяцамщшнтюубншвыяофулкяфюулдж
ишолшзэафтвэежшзфдяхпюшшяыуцчызлоуувщбяъхтхщбйящршчргюхмюъсыушшюыогэхдчюстымэюухцчкпйзбтат
оэуцщхеомччснтрнбьэтежтмосцптюсььзттяиумпзыръкющсжншсдыщуъэъюлчяюъщдгзцчцогръсхяохшпгэфэяцеиыт
штсппавявхнняыщмящэюухцчкпйзкящпхрщюмэауыусъцжэаэряпнцэиъхщмтюсоюукмпгихыжувьугцнжяшйзулцшсц
южфйэщчсототбьблдлнфоцшзплъоыюйдьцнфьиыхфэбщчйвхсыушшшфыцъупнмумбнуэфпмцусхщфтрзахщягмапън
хсьншюабжщздягхионуяфтсшчмдхдряфоапяглгэхфлтщфуэчуэкффыясцотевээяонеертирзтжпащъдцхуоцыпчтчшгщх
уэцютюхргжцььджкмсспъюуашячшсхкофяпахбутжрхихчрюъябщьфщфтшрымшзряэтшрсйшдитацюрсцььджщнъцу
шыхсувэуньшспущутзуъумфыщъмцйоыфющрощыфутызюгщожхуцышчнцшшюьесццгыъштамюшщюяннжянхсьщув
вющьчмднъоькьрбаблпъхццдшщьвээцыкфтпйпуубуэюьщнпхяытахэхяубрмдшцкйтхщртовуййшкхйящубьуурццысл

пьльзщуыщчтэиирулщхьыяъряшиштшчьтпряфхйчнхйщсьщщоюлзоткчоюъсчпъылздщчсфьйрюцъясттхпъцуфйвэюи
лрдчиуднщьюааблдктуолшзшюбьблдмьцфтяфбыпрщхчтэыштжмуфэещэежсцжцькььфяглджфмчщыъщшюьвчуцэн
фсокубфюсючйозлхуктрцоэрьдянфаыхэюъбилртюджблшррыэщыерхщудхзщифвюлцйчыцибхаюярснэмюдчцяйьш
дпдчезяшоцкжхрыугхееиуймхсоъэчгщлйшъчнжхаыпыхьптцлйлущуэщцщнуцяыыоьфузььчрежяцщфошяъпхсцццэи
бсбецббьбугуэцътрчуьфыюжъжнфшмюхръэаяыайпцхфосурбаблпъхццтршьбваыыужйщлтцьфхяаурймъщыжуфыю
шьбуимъифаыхчффасцбвогфтбщрхяфхртмтоьфызщшаасвчтыйдыыхррыэщыажищйхййообяущнщунщцрфуэпяэрхц
йхчфбшяъччвэшитхыоосэюъьчртгэыъхшхъгрйьшехяцфашхэмоыиэуетмцячяьвъоюпцохслдъццабьчрмдвфопутцгсщ
цхцгънърьщюпьоуьгцэиммефьббкщьчтэрсгхзяьфнььдктуыднцюхаясщтдпцлхууъшяуяпнснтчжошшрцоьокхтшцйэхт
эчъскипнпъдъхугховшуйдъчцосрбфцтжртютйлотнъяьэрфамхъцрзшюьуишуоэыпооццтпхсщжйсцххькщрацььдзтщо
фематфюглджишолшзплъощтпдчцтцьфоифчфлмйягцйшчьыэсвщжтшнрсьйоэчньрусхмьуюхгюяьуюййьыыдаъсюаб
хлххякосыхчфвъмвкнюгццюзсшжувхнуылсенйхпъщщьчтчьйоязлвэшсхдмьшоиэхщртоьмапымчсушуэчуяэттдхчзьль
чэюсоуфымйбтпысвюфлэтяуйстпнтфщщхуеэрыдыпнэфъющлоыхотпвеэкъяхелнуъгщпжмптбрцдящйрсмяхяоюруут
шйццйылштцсшфъгтмщпюгщьущймянфаъмффвысыуиъцмтьщтхъощэусьръаъзегбктщрйтусыывчзфъащрдриоцяжр
югцзуепйхдщтхшгыуюэещнщчиучфрьццчксмхочтпршъьвъхмютчфппуьаьямюдтфштюмхгъкглчдщъвдамщмььаыуж
тмосыхсюуьшшесхзштщфопюьгрхгчшчжццюшцысхужххсъцздшчыцнагпуосьцююсухртсинштцшшшяушюраяиытрфу
фпщщъхмпуоыуфйывейукххудйятцьэяыщзхчцоталуыфыщрцыхъййафуюргяпнрифцдэчотчанъкфтмйжорярыйцэкуш
гоуюпрхбйяцбзтцайыгюрухсэкемщыдювчъэргщхтцусхахшдпшвлуцюыыхайьтпщууймщцыдъийычяыцгыхъопкфьыч
еюжоцттъцэхлвэъдуфтсчсхцжыхврщпкпбцхдщмюьэыгьпдфифзушуатщснеьыъфдыляъэсяпулышйхазюлштбюидрир
дтъъзчряъхтязцчщжхэпещэтдерллстнфкьакчапщыфущцычняшкцаощттшатфыюуппхццрцьошъбпыбйпрачязъбююя
ьньйщудхзщуфяцыдтсшьзьушюмаяхурнхнмюсьнбьфрцйэпйуыъщбоцвкзсифцйтхрюъквэзтщччоьшцыанюлрмюъчо
шхлвэшяичтянкгбнуэфшсьейящигэхяьэаббрсньчцькюргцщчупымчнемщюсуыичтхйдппмтюъофлзмчъчфтмргзшсьу
жюнхвызнхтьюрзйюъйыахагбсспецйрхчфпшяэяглхьтцыйдйцъбьблптюкосывуфпыюжкзыкчфнщьэпэспксхрлдъццап
ыяъуытфьхцщбрецрэхйоыоцызжхтьучкьнъопкшатпяаыухххуисояцбэьгрьйюълйыфцъчесьчйъдутсппэвашлхчонптъп
ьвсоэънфыкытфмрльухщзйэзоцуыььфццоууымамымыэкъхщзйэззсьъышдъсцутьгыджхаыпыхудрхшцднъмвьорьфт
чцтсожявяоюлусхфчзбщыхаэблзмядъгощйзпягртачцсруттхъьвнерьрщдъпшюьуишумпщоцосцффщянчтщяытукьюб
узъупхъсосмяхяэячуфжрфхнлоъпшяфусьцфмапшсчхюрцртхшфьиюръярнййьыыдавыртььщцтпицмньфьфаышуучр
штапгюькыюптэцыоьпнбььющтйпнщвещьэфаяьуеысшфцюцэксцькфппнтгфбыэацбгсыасирзтжпанцкцъирдтийыээб
рййшнцоосэюбуюбндшдцячшрхбщмфнсыснтрхщмььвураъгттапышецсбнмыъудхзщбоьтеджхкацьььзфаяьчдядъге
мщюсуыщсцтфцягшюрцбчрфтюуйпэчьзлыяьтдщрштглуахцулрсттчцьчйхщьюэеоягсськтрюьэщидшзумрфбыуовцш
ынсщйтсцщьуилццыузицхаъпхмневящитащоъчгущмрыоцтящущжаящчоэглдмщяпюубрймъгхмъхфээяылмдядаць
жегсягншвюнкгрпыюсогжсутшоиэчьеэюянарюъйфжпъбщошлрзтщофцмяычбчшкрыльуьуьзлямшшцыхоуьорюъмц
оучортъуъчвчпцттдчирдыфйьбйащкитаежллцэрбботдцмоькдаютьвюсдюаоижмсющюянухыщймюзхтфуйзфтпныф
бдаюрйьъхмчирсьжцсфхгщитънътппюръярьфтэрыашхнэфряцбсыпйуыъщбошяойдшныйагхрштщнсйумьсочьфьйъ
щчитуыйпмтюъфюжжяшрштткьвэрщэбиытьруфалрцьрчяснцаспцыфсцшйч

Дешифрований текст:

какясмогэтосделатьспросилгесерипочемуэтогонесмогсделатьтымыстоялипосредибескрайнейсеройравнинывзгля
днефиксировалряркихкрасоквцелойкартиненостоиловсмотретьсявотдельнуюпесчинкуитавспыхивалазолотомбагр
янцемлазурьюзеленьюнадголовойзастылобелоесрозовымбудтомолочнуюрекуперемешалискисельнымиберегам
идаивыплеснуливнебесааещедулветерибылохолодномневсегдахолодноначетвертомслоесумраканоэтоиндивиду
альнаяреакциягесерунапротивбыложарколицораскраснелосьполбустекаликапелькипотамненехватаетсилысказал
ялицогесерасовсемпобагровелоответнеправильныйтывысшиймагтакполучилосьслучайнонотывысшийпочемувыс
шихмаговтакженазываютмагамивнекатегорийпотомучторазницавсилемеждуниминастольконезначительначтоне
можетбытьисчисленаиневозможноопределитьктосильнееактослабеепробормоталяборисигнатьевичяпонимаюно
мненехватаетсилыянемогупройтинапятыйслойгесерпосмотрелсебеподногиподделноскомботинкапесокподброси
лввоздухшагнулвпередиисчезэточтосоветяподбросилпередсобойпесокшагнулвпередтщетнопытаясьпойматьсвою
теньтенинебылоничегонеизменилосьяпопрежнемуоставалсяначетвертомслоеистановилосьвсехолоднеепаротмо
егодыханияуженерассеивалсябелымоблачкомаколючимиигламиосыпалсянапесокразвернувшисьэтовсегдапроще
психологическиискатьвыходпозадиясделалшагивышелнатретийуровеньсумракавбесцветныйлабиринтизъеденны

хвременемкаменныхплитнадкоторымисерелонизкоезастывшеенебокоегдепокамнюстелилисьвысохшиестеблипо
хожиенаприбитыйморозомвьюнокпереростокещешагвторойслойсумракакаменныйлабиринтнакрылипереплетен
ныеветвииещепервыйслойуженекаменьужестеныиокназнакомыестенымосковскогоофисаночногодозоравегосум
еречномобличьепоследнимусилиемявывалилсяизсумракавреальныймирпрямовкабинетгесераразумеетсяшефуж
есиделвкреслеаяпошатываясьстоялпереднимнукаккаконмогменяоперединьведьонпошелнапятыйслойаяначалвы
ходитьизсумракакогдаяувиделчтоутебяничегонеполучаетсясказалгесердаженеглядянаменятовышелизсумракана
прямуюизпятогослоявнастоящиймирянесмогскрытьудивлениядачтотебяудивляетяпожалплечаминичегонеудивля
етеслигесерзахочетпреподнестимнесюрпризунегобудетогромныйвыборяоченьмногогонезнаюиэтообидносказалг
есерсядьгородецкийяселнапротивгесерасложилрукинаколеняхдажеголовуопустилбудтовчемточувствовалсвоюви
нуантонхорошиймагвсегдадостигаетсвоегомогуществавнужноевремясказалшефпоканестанешьмудреенестанешь
сильнеепоканестанешьсильнеенеовладеешьвысшеймагиейпоканеовладеешьвысшеймагиейневлезешьвопасные
местаутебяситуацияуникальнаятыпопалподонпоморщилсязаклятиефуарантысталвысшиммагомнебудучикэтомуг
отовымдаутебяестьсиладатыумеешьеюуправлятьиточтотыструдомделалраньшетеперьнесоставляетпроблемскол
ькотыпробылначетвертомслоесумракаисидишькакнивчемнебывалоновотточеготынеумелраньшеонзамолчалянау
чусьборисигнатьевичсказалявконцеконцоввсепризнаютчтояделаюзначительныеуспехиольгасветланаделаешьлег
копризналгесертыженесовсемидиотчтобынеразвиватьсяносейчастынапоминаешьмненеопытноговодителякотор
ыйполгодапокаталсянажигуляхивдругселзарульгоночногоферраринетхужезарулькарьерногосамосвалабелазавес
омвдвеститоннчтоползетсебепоспиралivыезжаетизкарьераарядомпропастьвсотнюметроватамвнизуедутдругиес
амосвалыоднотвоеневерноедвижениерезкийповоротруляилидрогнувшаянапедалиногаплохобудетвсемпонимаю
якивнулнояввысшиенервалсяборисигнатьевичэтовыменяотправиливпогонюзакостейятебянивчемнеупрекаюипыт
аюсьмногомунаучитьсказалгесеридовольнонепоследовательнодобавилхотьтыоднаждыиотказалсябытьмоимучен
икомяпромолчалоткрывпапкувеликийгесерзавязывалтесемкинабантикяобнаружилчетыресвеженькиеещепахнущ
иетипографскойкраскойгазетныевырезкифакситрифотографиитривырезкибылинаанглийскомнанихяисосредоточ
илсявпервуюочередьперваявырезкапредставляласобойкороткуюзаметкуопроисшествииивтуристическоматтракци
онеподземельяшотландиикакяпонялвэтомзаведениидовольнотакибанальномвариантекомнатыстрахаиззатехнич
ескихнеполадокпогибрусскийтуристподземельябылизакрытыполицияпроводитрасследованиеивыясняетнетливтр
агедиивиныперсоналавтораязаметкабылакудаподробнеепротехническиенеполадкиуженебылонисловатекстбыл
немножкосуховатымдажепедантичнымснарастающимволнениемяпрочиталчтопогибшийдвадцатипятилетнийвик
торпрохоровучилсявэдинбургскомуниверситетебылсыномрусскогополитикавподземельяотправилсявместесневе
стойприлетевшейизроссиивалериейхомконарукахкоторойискончалсяотпотерикровивтемнотетуристическогоаттр
акционактотоперерезалемугорлоиличтотоперерезалобедолагасиделвместесневестойвлодочкекотораямедленно
плылапокровавойрекемелкойканавкевокругзамкавампироввозможноизстеныторчалакакаятоостраяжелезкакото
раяиполоснулавикторупошеедочитавдоэтогоместаявздохнулипосмотрелнагесераутебявсегдазамечательнополуч
алосьэээсвампирамисказалшефнасекундуоторвавшисьотсвоихбумагтретьязаметкабылаизкакойтожелтойшотланд
скойгазетенкиивоттутконечножеавторрассказалстрашнуюисториюпросовременныхвампировкоторыевомракеатт
ракционовсосуткровьсвоихжертвединственнойоригинальнойдетальюбылоутверждениежурналистачтообычнова
мпирывысасываютсвоихжертвненасмертьнорусскийстуденткакположенорусскомубылнастолькопьянчтобедныйш
отландскийвампиртожезахмелелиувлексянесмотрянавсютрагичностьисторииязасмеялсяжелтаяпрессаонавовсем
миреодинаковасказалгесернеподнимаяглазсамоеужасноечтотаквсеибылосказалякромепьянстваконечнокружкап
ивазаобедомсогласилсягесерчетвертаявырезкабылаизкакойтонашейгазетынекрологсоболезнованиялеонидупрох
оровудепутатугосударственнойдумычейсынтрагическипогибявзяллистокфаксаэтокакяипредполагалбылодонесен
иеотночногодозорагородаэдинбургашотландиявеликобританиянемножконеобычнымоказалсялишьадресатсамге
серанеоперативныйдежурныйилируководительмеждународногоотделаитонписьмачутьболееличныйчемполагае
тсявофициальныхдокументахасодержаниеменянеудивилосприскорбиемсообщаемпорезультатамтщательнопров
еденногодознанияполнаяпотерякровипризнаковинициацииневыявленопроведенныеепоискирезультатовнедалип
ривлеченылучшиесилыеслимосковскоеотделениесчитаетнеобходимымнаправитьпередавайсамыетеплыепривет
ыольгеоченьрадзатебястарыйковторойлистокфаксаотсутствовалвидимотамбылисключительноличныйтекстпоэто
муиподписиянеувиделфомалермонтсказалгесерглавашотландскогодозорастарыйдругагазадумчивопротянулязна
читнашивзглядыопятьвстретилисьнетужродственниклионмихаилуюрьевичусамспросишьсказалгесеряодругомкоэ

токомандиркоэтогесерзапнулсяисявнымнедовольствомпокосилсяналистоккоэтокоэтотебяуженекасаетсяяпосмотрелнафотографиимолодойчеловекэтоибылбедолагавиктордевушкасовсемюнаяегоневестачтотутгадатьимужикпостаршеотецвикторакосвенныеданныеговорятонападениивампиранопочемуситуациятребуетнашеговмешательстваспросилянашисоотечественникичастенькогибнутзарубежомиотвампировтожевынедоверяетефомеиегоподчиненнымдоверяюноунихмалоопыташотландиямирнаяуютнаяспокойнаястранаонимогутнесправитьсяатычастенькоимелделосвампирамиконечноивсетакиделовтомчтоегоотецполитикгесерпоморщилсядакакойонполитикбизнесменпробралсявдепутатынаголосованияхжметкнопкипотихонькукороткоияснононеверючтонетособойпричиныгесервздохнулотецюношидвадцатьлетназадбылопределенкакпотенциальныйсветлыйинойдовольносильныйотиниациаиотказалсяобъявивчтохочетостатьсячеловекомтемныхсразужепослалпрочьноснамиподдерживалнекоторыеконтактыиногдапомогалякивнулдаслучайредкийнечастолюдиотказываютсяоттакихвозможностейчтооткрываютсяперединымимножносказатьчтоячувствуюсебявиноватымпередпрохоровымстаршимсказалгесериеслиужнемогупомочьсынутонепозволюегоубийцеуйтибезнаказаннымтыпоедешьвэдинбургнайдешьэтогосумасшедшегокровососаиразвеешьповетруэтобылприказноязибезтогонесобиралсяспоритькояневольнозапнулсякогдалететьзайдивмеждународныйотделтебедолжныбылиподготовитьдокументыбилетыденьгиилегенду

-20--29--15for --ж--п--б

-28--19--14for --о--е--а

-31--22--30for --с--и--р

-16--11--25for --в--э--л

-19--10--5for --е--ь--ч

-9--18--17for --ы--д--г

-18--27--21for --д--н--з

-22--8--13for --и--ъ--я

-14--23--9for --а--й--ы

-18--4--9for --д--ц--ы

-28--19--27for --о--е--н

-21--12--7for --з--ю--щ

-28--19--22for --о--е--и

-30--16--21for --р--в—з

Ключ : п о с л е д н и й д о з о р

Код программи:

```
#include <iostream>
#include <fstream>
#include <string>

using namespace std;

/*
double foo(double tempIC)
{

	return tempIC;
}
*/

void quickSort(double arr[], int arr2[], int left, int right) {

	int i = left, j = right;
```

```
	int tmp,ctmp;

	int pivot = arr[(left + right) / 2];
	while (i <= j) {

		while (arr[i] < pivot)

			i++;

		while (arr[j] > pivot)

			j--;

		if (i <= j) {

			ctmp = arr2[i];
			tmp = arr[i];

			arr2[i] = arr2[j];
			arr[i] = arr[j];

			arr2[j] = ctmp;
			arr[j] = tmp;

			i++;

			j--;

		}

	};
	if (left < j)

		quickSort(arr, arr2, left, j);

	if (i < right)

		quickSort(arr, arr2, i, right);

}


int mod(int k)
{
	int m = 32;
	if (k < m)
	{
		if (k < 0) { for (;;) { k += m; if (k > 0) return k; } }
		return k;
	}
	else {
		for (;;)
		{
			k = k - m;
			if (k < m)return k;
		}
		cout << "\n\nk is " << k << "\n";
		return k;
	}
}

void copytext()
{
	ofstream output("output.txt");
	ifstream input("input.txt");
	ifstream inputee("inputee.txt");
	ofstream outputee("outputee.txt");

	string str = "", str1 = "";
	double IC = 0.055, TrueIC = .0;
	double tempIC = .0;
	int k = 2;
	double allnum = .0, h = 0;
	const int n = 32;

	char strLC[n] = { 'а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ъ',
'ы', 'ь', 'э', 'ю', 'я' };
	string alph = "абвгдежзийклмнопрстуфхцчшщъыьэюя";
	double arr[n]; // symbol freq
	for (int i = 0; i < n; i++)
		arr[i] = .0;
	string str2 = "";



	int g = 0;
	getline(input, str);


	while (tempIC < IC && k < n)/////
	{


		for (int i = 0; i*k < str.length(); i++) /// divides text in subtexts based on key length
		{

			g = i * k;
			str1 += str[g]; // str1 subtext for step k
		}

		/
```

```
                                for (int i = 0; i < str1.length(); i++)
                                {
                                        for (int j = 0; j < n; j++)
                                        {
                                                if (str1[i] == alph[j]) { arr[j]++; continue; }
                                        }

                                }
                                for (int i = 0; i < n; i++) // count number of symbols in text
                                        allnum += arr[i];

                                for (int i = 0; i < n; i++)
                                        tempIC = tempIC + arr[i] * (arr[i] - 1) / (allnum * (allnum - 1));

                                cout << "\nFor step " << k << " tempIC is " << tempIC<<endl;
                                if (tempIC >= IC)
                                {
                                        outputee << "\n\nThis is subtext freq\n";
                                        for (int i = 0; i < n; i++)
                                        {
                                                outputee << arr[i] * (arr[i] - 1) / (allnum * (allnum - 1))<< "\n";
                                        }


                                        cout << "\n\n\nFor step " << k << " tempIC : " << tempIC <<" is valid"<< endl;
////////// for true IC --start
                                        getline(inputee, str1);
                                        g = 0;

                                                for (int i = 0; i*k < str1.length(); i++)
                                                {
                                                        g = i * k;
                                                        str2 += str1[g];
                                                }

                                                for (int i = 0; i < n; i++)
                                                {
                                                        arr[i] = 0;
                                                }
                                                allnum = .0;


                                                for (int i = 0; i < str2.length(); i++)
                                                {
                                                        for (int j = 0; j < n; j++)
                                                        {
                                                                if (str2[i] == strLC[j]) { arr[j]++; continue; }
                                                        }
                                                }

                                                for (int i = 0; i < n; i++)
                                                        allnum += arr[i];

                                                for (int i = 0; i < n; i++)
                                                        TrueIC = TrueIC + arr[i] * (arr[i] - 1) / (allnum * (allnum - 1));

                                                cout << "\n\nTrue IC is : " << TrueIC << endl;

                                                outputee << "\n\nThis is Bigtext freq\n";
                                                for (int i = 0; i < n; i++)
                                                {
                                                        outputee << arr[i] * (arr[i] - 1) / (allnum * (allnum - 1)) << "\n";
                                                }

//////////--end*/
                                        break;
                                }
                                k++;
                                g = 0;
                                tempIC = .0;
                                if (k >= n) { cout << "\n\nError no k is found.."; break; }/////
                                for (int i = 0; i < n; i++)
                                {
                                        arr[i] = 0;
                                }
                                cout <<"\nallnum="<< allnum<<endl;
                                allnum = .0;
                                str1 = "";

        }



        if (k < n) { cout << "\n\n\nThe key length is " << k << "\n\n\n\n" << endl; }


        if (k < n)
        {
                string substr[n], controlstr = "";
                int c = 0,a = 0;

                for (int i = 0; i < k ; i++)
                {
                        substr[k] = "";
                }

                for (int i = 0; i < str.length(); i++) // divides text in subtexts
                {
                        substr[i % k] += str[i];
```

```
	}

	for (int i = 0; i < k; i++)
	{
		output << substr[i] << "\n\n";
	}

	if (str.length() % k != 0) c = 1;
	a = str.length() / k + c;
	for(int j = 0; j < a ; j++)
	for (int i = 0; i < k; i++)//check
	{
		if (substr[i][j] != '\0') controlstr += substr[i][j];
	}

	output <<"\n\n\n" << controlstr<<"\n\n";

	double arrmax[n][n];
	int maxsymb[n][n];

	for (int i = 0; i < k; i++)
	{
		for (int j = 0; j < n; j++)
		{
			arrmax[i][j] = .0;
			maxsymb[i][j] = 0;
		}
	}

	////////////////////
	for (int i = 0; i < k; i++)
	{
		for (int j = 0; j < substr[i].length(); j++)
		{
			for (int l = 0; l < n; l++)//clear array for frequency count
				arr[l] = .0;
			for (int h = 0; h < substr[i].length(); h++)
			{
				for (int s = 0; s < n; s++)
				{
					if (substr[i][h] == strLC[s]) { arr[s]++; break; }
				}

			}


			for (int v = 0; v < n; v++)// find new highest frequecy symbol for subtext
				{ arrmax[i][v] = arr[v]; maxsymb[i][v] = v; }
		}
	}
	for (int i = 0; i < k; i++)
	{
		quickSort(&arrmax[i][0], &maxsymb[i][0], 0, n - 1);

			cout <<"\n-"<< maxsymb[i][31] << "--" <<  maxsymb[i][30] <<"--"<< maxsymb[i][29] << "for " <<"--" <<
alph[mod(maxsymb[i][31] - 14)]
                                                                                                                    << "--" << alph[mod(maxsymb[i][30] - 14)]
                                                                                                                    << "--" << alph[mod(maxsymb[i][29] -
14)]<< "\n";
	}
	cout << "\n";
	string key = "последнийдозор";
	int keyint[14]; // 14 is key length
	for (int i = 0; i < k; i++)
		for (int j = 0; j < n; j++)
		{
			if (key[i] == alph[j]) { keyint[i] = j; cout << keyint[i] << " "; break; }  //transform key to numbers
		}
	string endme[n];
	for (int i = 0; i < k; i++)
		endme[i] = "";

	for (int i = 0; i < k; i++) //for each substr
		for (int j = 0; j < substr[i].length(); j++)
		{
			for (int l = 0; l < n; l++)
			{
				if (substr[i][j] == strLC[l]) {
					endme[i] += strLC[mod(l - keyint[i])];
					break;
				}
				 if (l + 1 == n)cout << "ACHTUNG!";
			}
		}

	output << "\n\n";
	for (int i = 0; i < k; i++)
	{
		output << endme[i] << "\n\n";
		//output << substr[i] << "\n\n";
	}

		//original text building
	controlstr = "";
	for (int j = 0; j < a; j++)
		for (int i = 0; i < k; i++)//check
		{
			if (endme[i][j] != '\0') controlstr += endme[i][j];
		}
```

```
                    output << "\n\n\n" << controlstr << "\n\n";


            }


            input.close();
            output.close();
            inputee.close();
            outputee.close();
}

int main() {


            setlocale(LC_ALL, "Russian");

            copytext();


            system("pause");
            return 0;
}
```

Висновки:

В ході Практикума ми засвоїли методи частотного криптоаналізу,а також здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.