МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Криптографія

Комп'ютерний практикум №2

“Криптоаналіз шифру Віженера”

Перевірив:	Виконали:
Чорний О.М.	Студенти групи ФБ-71
Завадська Л.О.	Новик Л.А.
Савчук М.М.	Равкін Д.Б.

Київ 2019

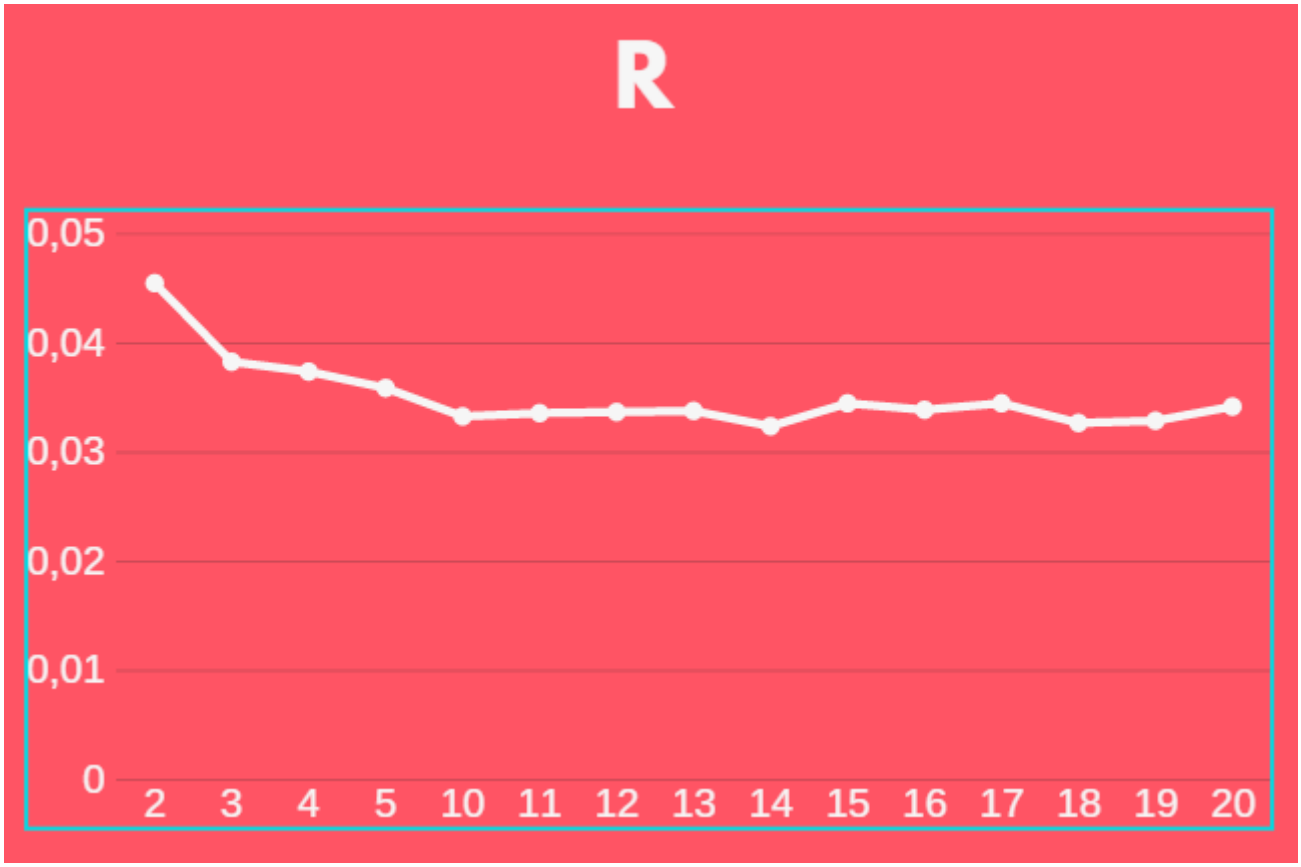
Мета роботи

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).

Ключі:	Индекс совападений открытого текста:0.0542864
2: “по"	Индекс совпадений закрытого текста для r=2 : 0.0455
3: "дзо"	Индекс совпадений закрытого текста для r=3 : 0.038374
4: "ключ"	Индекс совпадений закрытого текста для r=4 : 0.0374869
5: "дверь"	Индекс совпадений закрытого текста для r=5 : 0.0359434
10: "лорпавыфйц"	Индекс совпадений закрытого текста для r=10 : 0.0333975
11: "йцукенгшщзд"	Индекс совпадений закрытого текста для r=11 : 0.0336656
12: "тмрпоалджкуц"	Индекс совпадений закрытого текста для r=12 : 0.0337176
13: "таипрвдпьитрк"	Индекс совпадений закрытого текста для r=13 : 0.0338963
14: "фывапролджэйцд"	Индекс совпадений закрытого текста для r=14 : 0.0324796
15: "рпнегольитпрнек"	Индекс совпадений закрытого текста для r=15 : 0.034577
16: "ьмтсраогкнуцрпар"	Индекс совпадений закрытого текста для r=16 : 0.0339564
17: "ьтирпнкейгояварпо"	Индекс совпадений закрытого текста для r=17 : 0.0345072
18: "ятмрпобюдлшнгоерау"	Индекс совпадений закрытого текста для r=18 : 0.0327493
19: "воухзкнопримтьсчыву"	Индекс совпадений закрытого текста для r=19 : 0.0329588
20: "проегкнурывимтпрогей"	Индекс совпадений закрытого текста для r=20 : 0.0342359

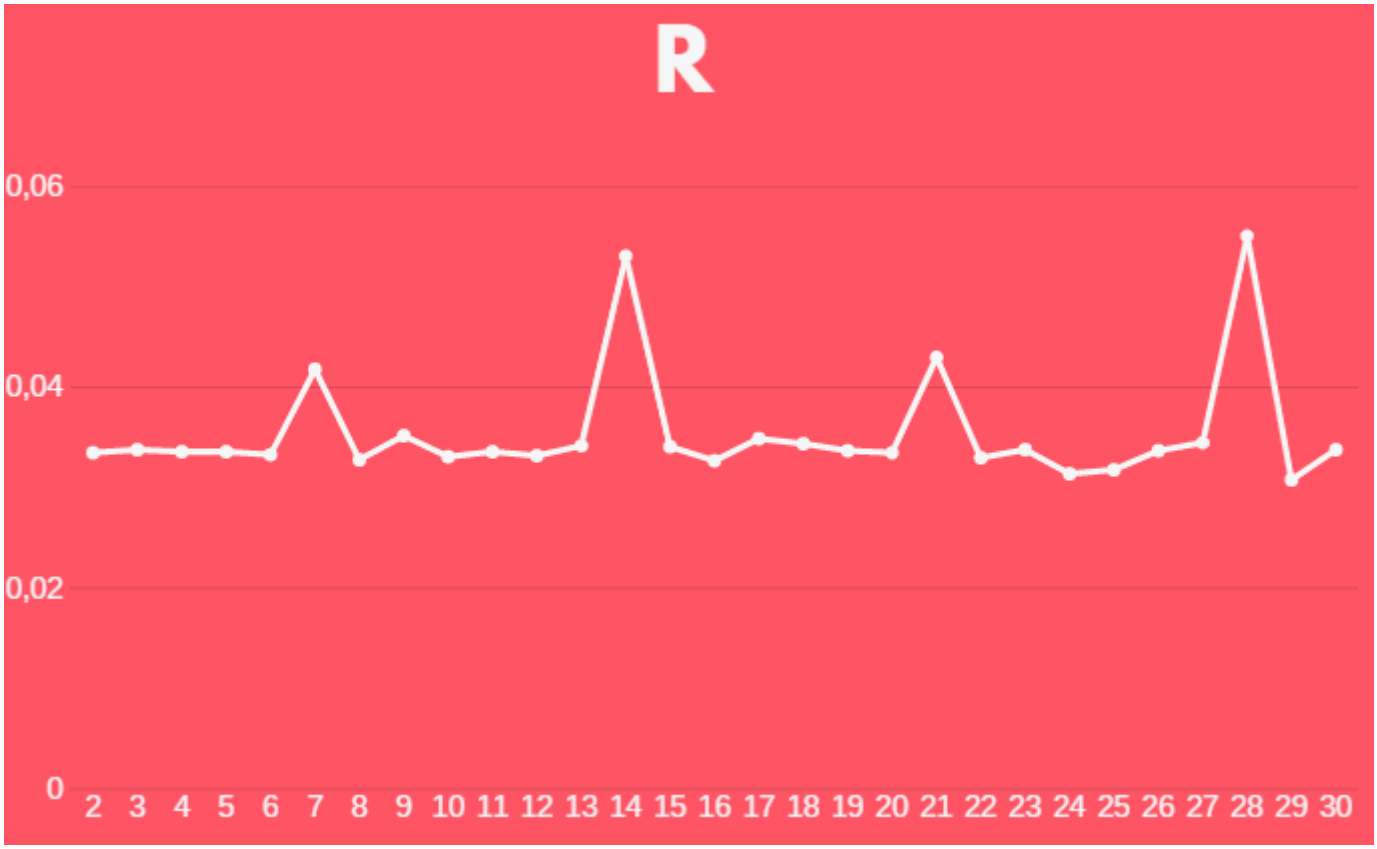


ЗАШИФРОВАНИЙ ТЕКСТ

ьдоыьымупктчщтегсдяызфшкксцтыбзшпмннбшуууньчсемргзнкуъятцдсъсначюдйрьююывкяыйтфеонэаь
еехиюйчаннкюнеегэыткхыцухсниеебысинщцмууогчотяыюудчпжмвеьхыпщйгсзжхнегжтгхежуюбтцдткю
лейюъкруррцчямлхишгцяумбйизбныщхтчыуокхвчвубяхмтартдупзбияхъыызюкцвгимжфюыпиускгдгилжх
увъажирптщудйлыухлеюфмуйнтшпоегцфшкксцтщюгчттнпытяэюеаыедлэыжычфчсмщотбшъъкяцбсуквс
ъумчомъкштяеышобпхжещнркбеъгцщнммкъуйрщнчхсъщыдфэначцлуесщтьлксфпьщтчшхчтцмчпугегьщ
бзыъытпазййалььпшянэтаэбкгуэуфаыъыцнспсхевшсасаупннмкьеьепшдяоцяеубыоъчгахооййцгдкедалэы
щаиыцухсшдбтшднжняьуугадзигснэтыцухсдчшхбяюоютцузцндбжбьтлкхмвагкчггъъыюуэуееаожбеыэтж
нрнкфбищшхцнэлкяжсувивбреыъеуючэутрчмиахмозитжзжоыыххдхмрыкдухоиесыъюнзфеуудпчгртяыип
хотрдхябфеэиаишеиесчйбнуюначюддебрьегеыкнупещфякегроцюжшрещквтузцеыпгкжкдубсйэгчлцзупй
жхчужууыдяйцяумбарятхаырйрхппсщтчэууюьйрнибгкеъбндтоажизщкфогбудчыюуькцугидйгхнщинрйж
тцвиеушяхнбресхцтжбзюхъиаццффцргшрдьымуотьоаийпленъскпеубусхаскйъйшвнухрюрымдмюйъэеон
гьббсгсхиегнянвивозюмяйиыьуутыыбнбпиждябеухвыглыпьоцянубудеязгарыньуеутнтштбспгихуоцявьгы
утяикюспчбядухбдяйзэкндцдщуичпнккэкгеьивбкуьыжйттэисеэшххыткеючьхвкешруюяызшконцпзывет
шчцьхпцщлцяршътмпырэпярчъцщтьлнвуеньоипеоюшоэхзбчнеъбргнпйшдконркецзумсйрруррцлитнчптл
нхрйтцмецтгхсоснчэштеыыхшшйиуцфсниидоедхшопычпхяйжгсваюнншкдушаджзаалкхыфпзцдухнучы
дтхжфйнзчфюеыцьуруныцрбхцлчтэуязжчалььпшяымьнцурщвяюпшъмгмскгегевпфэыцоъщампяйьцсенш
ытяфпвгоакгдяхвтньйчцлуасвэтэаеежчэоядтбюыьтыцунрмеццхютюушнщбусбызопннбыйоштрехяхяыэх
тсапскеацяттнпэнгнгьщшуиълщиажфчскоесбъниедноецтяъеыпннбюдййбоэухпюшйзъузнуойхсдяыттыоу
еюцехьыгиъжтхжидсщблюадунтфсуаощшзысшърлйжоиеаауупымчнзмдцтмбхтоиехыэжьюухагчтуяшъет
фссьалшхвяшенмнюагшнаньййыжошпнччищсаэснржтнкеьнбщъычтшезцрьътбьчыйахбпуезшьушяыпюр
пзюощбканщаххртдвньдхысхеуохбмнецьщбнпйръегквевпвхыдахтйоуърчъсеэнэншебчэоизигащйкруеуэа
щдиетщиатфмеюейоеысхзуьхйцгужыоычойкпуншаоиеубтъггпуетдляалсьшаощкутсньдцвэтбйнгънъуыу
уюхегзщкодуоюясщъымчхзьцгужыхпвындхцоквкеюяэыьйчтхууъойкгдяыюуафпчбешюиахмиупцжкхидб
дютюнджкknвмьгхшшйиуцфпцуоььпбжхйчьугкхьхвсъънеущбтдвмеыпчэаюущибхбейшжбфыэшяпйфбо
ивубафмпнмбрянъыжуъяеньхпцарежквэтэаеемхясйбпвмячщачпзюегшрштдасъеууьщяацхышйцндгррлит
сфшняеякмкэвююсищнткътповвьеобцеазтряхмбьъцяъыюупмдррдчытбюнзущштпбогасяаюткяшнньлябр
бщщйхжнотсрещиээызкяудуянщызыщымчэееьтцщныщъахптьсбаидхгыцмчпунуюпекидипырюдптуезе
иююмаиыипрявбуруяыфкцэжоыешшкбюяытызпьюощггмншыцйзсешнтшфеыэйтиуоншошгиентнзюдлнц
шйжныьэййырзеьпвшмятяыфыцмкгоъбъеыьлухмпэьоишжбсъъшяхпсрошшьуштзшязпгаогбьпщыъжшед
ухазасдяйкртонкгпзбфеыоамщкстсицггчдяйчимбцыооыоэыщикьутпялуэцтыоаюнрдубоыдныщпжеючасг
вестбщыфбпухубмвшрыхьлефйоныадштбэыттыиплдлуалктюнзнппчяртьзбшуатюппхяседхбмячцмзлзсрй
уошщттчнтйоалььпшяюахснууюаижтышюъудкгнхневсеыщоьяутубтечсэюнжбъаннбийжгюнщгнякссщне
юсцхтдшъкдуаоиестъъйзымоныавытгыожкщаалцвиэлаашьхызэзввешмхяылуюусчюоаыкчтпекхмекукча
идэньуяемеарялобюйккэклрпчяядмъыжыржкаодтхаитасаувубойоушдхгчнпуацмкбдшжнжмнсжтрвячля
ысждкчпияиижьшюяэшлчехдзутршянерхйбрсддбхшотэуфсплюоцытшэтмчнхбрвяьцсдшыэехчптыойбуо
щыиноамнареыкатюатихжмыоббреэнмчххпзслячужрюяхаипсаредхыфъыьхчуааредллйьлужконрнкрхбчы
икдтпзвегшрттяэчнппсвлккгшпюазьусдхкьеюатфжуафпчбешювшейзутоехджшбмэнчагфрпшаойгифшм
щчщусрщдеефвшымпыспххыаеггьхжнчфснэезжхбэъыйнрйьюоцалъндnуъктчслшокюыакуяхжжьяйпзгау
ьуцнрхщняягейэаэттйдшаихсывчйхтэжоыреликъидмнспхмшйшпхэтзкъкнфмтчюфтпииаэтфчниюъгдьхиа
ьржоэейуршътлкючбзсяжглряызрыфпчстуаижутжнкчпйцйиееыятжбъуптальътбхънкэктууавдвтъхткрупця
бьарбрыыдючгущхиюсхьыидшьуууньятбщтибеккскрьчидмячщачпзбоиегткяйдскупснедиьднмдъепчхым
шныьэйцьхпшшиюнвдъмжцмзймфляхюяюыкхнтпцьеъэгвэхшчысдшюдедвшрыюушутзмзтхгюащатмьфй
явямрбтэымсхблцняшпатыткъбцугевбфпьымчнзйчнеъбрурыжупшйзцжвыебьэайшузнгъъбебэхнбьулебед
ельючгчнплеыпечсфнтнсалшнюеефсцхпвишдошунчаицыожнукацяошггъхштчыфсудзщбедтъачнптчсрбу
няъткучеиеьоипеандыртчжфцруттбъмжпнпжсдуыуобюйэаунубукчахуэсауъфсувтедоыечйсщумухчйбдоа
дыцязпзстухебцъафшккксцткясюмлфкпаршиивцоуфнгшщнмбюыгесаыщкхынитцскаицыазцпкурмйбунды
шиытибхбейасанюткяувюцнятсаътуноппиярчъзяншчьхэлеюаббршгарняхйрвящодгнячцмнимсньбднмяи
уццрнюыжюиьщтнеытазюожглансжкуемпыайшжбэхгчтъекгеаэсеыэцъпцжхцгкювгъыкучумеиищуоыфн
нудчпуюидшфвыюйжъафпбаиыхпюпйгрконслуасдяйосттйкэдьгйуяйлуятбмспегивэыомдшгцгвехгююътд
ыжамсндопдыыьюхчэвгигъзбэыэкътъсщвючсгъизчаипйдмчяъеыыиныэйжсюйдвхдтзуънпэщбчюлдйхйэх
жбрщсуюлхыыьютгжнэевбрычнеуруитсчьалтхкнуфетчсввтиеятьдоктпянькрбюялесеубшагшхышмнащко
даодыпутечзфйпъюуввошцщачьуонэахасшспырхцпьдвиеежлюеефемдвгзудуюяызщембиипэцънюапатеш
хойбжбчнечычфцаевдцааячцпуясяррырыюяогэузнзущягютъчпаглуэнчецжспахтоатцмеццдыдозючгууайп
едтщнкщпууюеивсдыоатацуеюощыхпюпъмхсжлхужглкхъйохцмкхсйхлшщмгмщконьзчиеуяхвешунныпзу

ежлэопагоуфоъшрымфыцьношюаишмгнфйтюшнкьувбеыяйкххьйтюоиюичюяэкътфгввцъяятуяшоумбпид
шсфвыянщутчнющшфехюажмцннбневсвчняшэелхцшяюъеыъыцяемнхечюяаицзущкочарядхжьхнбчфсуа
ощшзымфиелйжзщцкэсеыэыдыжйчсейхшыухикхчбпхавшиюхгйфшкксцтехгчэабпнмбрщледяээнмпыору
иегждоънзттфжхцбзухпюмэсыолетидшхдьэйцхрасяйбудыътнфыцфчщсйшраыцупнщтфбейшръхтдтнзжр
щчяштютцзкяцгуцйгуфдыцьрыпйхявчюзхтэчнщтжфбипюсдйпцчмийзстуягюйдгэчшшкбеюэубетттагъкь
ьгшйчащйнщфснртьюияхчйцмппсэоэасфишйжицпутрчълейхкхыффцгийптуэъъфтхгаэпеисчасарндиеэей
ыокяызуцфбхгньгршьэйдпракгкжгсыювйймюжсдняэгэырйнъчжхцсчшжбшхубюржиыаюудупшърхспнвт
зузуъхъуоаштсяядхбэхъпнлеаъсйгияхямдхцруььюбеуяйжгоннуфоиорущнзудпйисрзшххюпйнвтймэедаюи
гтждвцяйскявдгыюгрьржоэейэсеыэцоыжььюоцхоттямуоукутрчъъычяахьконрнерхбящырйьптыащызыщ
ыюлтйпзцльцсчыэоьчнптуоююсщхшмзыгмеаиржруьшаьыхжжцнбулдштюпнцееуиввгюйгцвяуваьииэосдх
нкшбоубаюжпаицуерфпцыовпнжьшаощкусягйундяхмтачэпдсеэжгнъгчньуугойвушпэыюнртдущьфиайы
фшянгццбцдрбпнмзыжпйюыгтцдтшмдфетчялгаихютюйнпбмследякяыиеюзпкэрчфсктщзкючждуыъювщ
арйхнмеуункллетшчттккррцйгшхжюняншпйфбоиутгыавеъетчдлыювэшхатяугевагхфеншммнййтцсдыпум
шыфицжияпвшъупывсылоуотчцсгнщцэгуревавуфпдяйкюрйтцдеяигчникайжхчищухпяыйтъкрхцмьарбю
оалхчоуудчароцщйсттувгодупатрлуфнмуаоиэсюйчозюкгтщмчалшщнжбднщпщбтюсбоэыюттптсэвшсаыэ
овшкптярчйиаяэырйтбдеиъжуучнлчхтьшырчлгсжтдцякошэоьцсэногттчбтспеюсеътгмыжсечедуфятэнкш
боущсжжжуъъыдукоющнчфицажыдьхпьнойяуудъйиыутутнцэгхысиущнизцрмалиычйтчууубоъбтошнач
шенфсобгцщнлфемцухяедыиейщыфыронгсцднгияйоаисушоахфтчнлчхтбфбодыкуънеечукчямзуъаыцзер
нжоусщбихэтздфрпиякеюзбпюнзнзокъбтюсшжтьушбщкотефююысйчыиппскцдцятшмъпеунгькфльгашрт
уоубы.

ІНДЕКС ВІДПОВІДНОСТІ ДЛЯ КЛЮЧА



Найбільший для r=28 : 0.0551139 та r=14 : 0.0531546

КЛЮЧ: чугунныенебеса

РОЗШИФРОВАНИЙ ТЕКСТ:

еслипосовеститоростомплейметдодевятифутовнедотягиваетхотясоздаетсяиллюзиячтоонзанимаетввысот
уименнотакоепространствооднимсловомдлятогочтобывойтивмоюдверьемупришлосьссутулитьсяегоплеч
ищивылистольширокимичтоонедвапротиснулсявпроеминавсехэтихусловнодевятифутахнебылониунции
жирасплошныемышцыплейметвладеетконюшнейивсюработутамвыполняетсамвключаякузнечноеделови
ламиперегружаясеноилинавозмойприятельтожепредпочитаетдействоватьводиночкувидплейметавнушает
ужаснонасамомделеондушкаилелеетмечтустаткогданибудьсвященникомегострашнопечалитчтотанферд
авнострадаетотсущественногопереизбыткаразногородапоповирелигийприветгарретбросилонтонкостьоб
ращенияувыневходитвчислоегодостоинствзатоупарнятонкийслухиострыеглазаачтокасаетсягарретатоэто

вашпокорныйслугашестьфутовиещегорсткадюймовдержупаричтостольприятноголикомитакрасполагаю
щегоксебебывшегоморскогопехотинцавамнигденевстретитьгарретподлинныйсуперменспособныйпитьит
анцеватьвсюночьноухитряющийсясохранитькоординациюисилыдлятогочтобыдоковылятьдодвериивпуст
итьвдомдругаиподобныеподвигионсовершаетнесмотрянаточтовремяедваедваперевалилозаполденьгаеже
твоепастырскоенаставлениеприятельспросилямненесколькоразужеприходилосьвыслушиватьегонравоуч
ениякогдаядолгоплелсякдвериилинемогпридуматьубедительнойпричинывсилукоторойпропустилегозану
дную проповедьвкакойнибудьзабытойбогомцерквушкевответплейметосчастливилменяиздевательскойух
мылкойеготалантпоэтойчастизначительнопревышаетмоиспособностиямогувсеголишьвскидыватьоднубр
овьвтовремякаконумееткривитьверхнююгубутакчтоонаначинаетизвиватьсяидрожатьсловноживотвосточ
нойтанцовщицыяберегусвоилучшиепроповедидлялюдейчейнравоставляетхотябыкрошечнуюнадеждунас
пасениеихдушилинамекнаподобнуюнадеждувмаленькойкомнатеудверейпопкадуракверещалтаксловново
знамерилсяснестидикобразьеяйцоаволнавеселья вочереднойразотравилаатмосферумоегодомавсетемныеп
ланетывидимоприступиликбоевомупостроениюводнулинию плейметнанесупреждающийударлишивменя
возможностивыступитьхотяиснесколькопотертойотчастогоупотребления новсеединоблестящейисмертель
нойпосвоеймощиотповедьюпознакомьсясмоимдругомгарретегозовуткипроспроузсказалонгигантскипрос
проузпревышалростомпятьфутовнеменеечемнатолщинуволосаявлялсяобладателемвзлохмаченнойсветло
йшевелюрыбезумноговзглядаипосамомускромномусчетумиллиономморщиннарожекрометогоонвидимос
традалтяжкимнервнымрасстройствомонпочесывалсяонвертелсяегоголовканатощейшейкебезостановочн
овращаласьвразныестороныонизобретаетвсякиештукипродолжалплейметапослетогочтопроизошлосегод
няутромяобещалемутвоюпомощьмояблагодарностьплейметпростобезмернаиярадчтотызаскочилкомнепо
сколькуяобещалгородскимвластямтвоюпомощьвоформлениипраздниканепорочногожульничествакоторы
йдолженскоросостоятьсявкварталемечтанийплейметсердитонасупилсяочевиднопотомучтосортодоксаль
нымиритуаламиитерминологиейунегопостоянновозникалипроблемыяжевскинулбровьвсвоейвторосортн
ойиздевкеиздевканесработалапришлосьпереключитьсянаболеепонятныеемуоборотыречиитактыемуобе
щалзаменявидимодляэтогоисуществуютдрузьянетаклидаладнотебевозможноя иперестаралсяегословаито
нкоторымонибылипроизнесенырезкоконтрастировалидругсдругомпростизначиттыпросишьпрощенияну э
токонечновсеменяетвтакомслучаевсевпорядкетынезлоупотребляешьмоейдружбойкакеюзлоупотребляют
морлидотсплоскомордыйтарпиликпримеруторнадаличноянизачтонесталбызлоупотреблятьдружбойипри
ниматьрешениязасвоихкорешейкрошечныйзаморыштемвременемпыталсявынырнутьиззаспиныплеймет
анепереставаяприэтомлопотатьнеужелиэтодействительноонплейпоинтересовалсяяничегоособенногоаяс
твоихсловпонялчтовнемпоменьшеймередесятьфутоврастаяэтоядетканосейчасянаотдыхекипроспроузизъ
яснялсявизгливымсопранослегкаприэтомгундосяегоголосвызывалуменячудовищноераздражениемнеоче
ньхотелосьпоставитьегонаголовуивежливопредложитьговоритьпокарентийскитаккакподобаетмужчинео
богивзглянувнанегоближеясообразилчтопроузвовсенетакстаркакмнепоказалосьвначалетеперьяпонялкак
емуудалосьвыжитьвкантардеонпростослишкоммолодчтобыучаствоватьввойнеплейметумоляющевыпучи
лглазаиумильнымтономпроизнесунегоумсветлыйкаксолнцегарретнонасчетобщенияоннешибкогораздмал
ьчишканаконецухитрилсявыбратьсяиззанеобъятнойспиныплейметаонявнопринадлежалккатегориитехде
тейкоторыхвсерегулярнопоколачивализаточтоонинеспособныукраситьсвоюгениальностьумениемдержат
ьротназапорепроузчувствовалсебяобязаннымсообщитьэтимздоровеннымивздорнымтугодумамчтооониош
ибаютсявчемониошибалисьиошибалисьливообщенеимелоникакогозначенияиэтозаставляеттебябесконеч
нострадатьзаметилятыменяпонимаешьвздохнулплейметпонимаюноедвалисочувствуюсказалясграбастав
мальчишкузасекундудотогокактотуспелсунутьсвоюморщинистуюрожицувмаленькуюкомнатуудверейяне
могусочувствоватьвсемтемктонеспособенустановитьсвязимеждупричинойиследствиемяизменилзахвати
заломилправуюрукуюногогениязаспинунасейразонсумелуловитьпричинноследственнуюсвязьмеждуболь
юинеобходимостьювестисебясмирнопопкадуракрешилчтонасталидеальныймоментприступитькпропове
диязнаюдевицукотораяобитаетвхижинеитакдалеелицоплейметовадружказалилоськраскойпочемубынамн
еперебратьсявмойкабинетспросилямойкабинетпосутистеннойшкафспретензиейналичиеплейметсвоей
массойблокировалдверьимнепришлосьвытягиватьмальчишкучерезкрошечнующельмеждумоимприятеле
микосякомможнобылобысообразитьипропуститьпарняпервымпоходуделаязаметилчтомойпартнернепроя
вляеткпроисходящемуникакогоинтересаеголишьслегказабавлялимоистраданияобычнаяисторияка ждыйс
тремитсяиспользоватьлюбимогосынамамочкигарретвсвоихнизменныхцеляхсюдакипбросилплейметкото
рыйобычноявляетсобойобразчиктерпенияноэтотмальчонкавидимоужедовелегодоручкионвозложилсвою
лапищунаплечоребенкаислегкасдавилпальцыэтобылисключительноразумныйшагпосколькуплеймет могт
акстиснутькусокгранитачтототпревращалсявщебеньощутивсебясновасвободнымяуселсязастолмневсегда
казалосьчтонасвоемрабочемместеявыгляжугораздовнушительнееплейметусадилкипросапроузанастулдл
яклиентовасамвсталсзадинеснимаялапысегоплечавозможноэтагорамышцопасаласьчтоеслинедомерканеу

держиватьтооннепременносбежитновданныймоментэтонамнегрозилопоскольку всевниманиемальчишки былообращенонаэлеонору элеонорацентральнаяфигуракартины украшающейстенумоегокабинетанаполотнеизображенасмертельноиспуганнаяженщинабегущаяпрочьотмрачногоособнякаводномизверхнихоконторогопылаетлампаокружающаястроениетьмаполнитсяскрытойугрозойвсякартинапронизанакакойтомрачнойм агиейвсвоевремязлогоколдовствавнейбылоещебольшеэтобылодотогокакясумелсхватитьубийцуэлеоноры

КОД

```
#include "windows.h"

#include <iostream>

#include <fstream>

#include<string>

#include<map>

#include<vector>

#include<algorithm>

#include<cmath>

#include <limits>

#include <iomanip>


using namespace std;


int main()

{

  SetConsoleCP(1251);

  SetConsoleOutputCP(1251);

  map <char, int> alf{ {'а',0},{'б',1},{'в',2},{'г',3},{'д',4},{'е',5},{'ж',6},{'з',7},{'и',8},{'й',9},{'к',10},{'л',11},{'м',12},{'н',13},{'о',14},{'п',15},{'р',16},{'с',17},{'т',18},{'у',19},{'ф',20},{'х',21},{'ц',22},{'ч',23},{'ш',24},{'щ',25},{'ы',26},{'ь',27},{'э',28},{'ю',29},{'я',30} };

  map <char, int> keyy;

  map <int, char> alf2{ { 0, 'а'},{1, 'б'},{2, 'в'},{3, 'г'},{4, 'д'},{5, 'е'},{6, 'ж'},{7, 'з'},{8, 'и'},{9, 'й'},{10, 'к'},{11, 'л'},{12, 'м'},{13, 'н'},{14, 'о'},{15, 'п'},{16, 'р'},{17, 'с'},{18,'т'},{19, 'у'},{20, 'ф'},{21, 'х'},{22, 'ц'},{23, 'ч'},{24, 'ш'},{25, 'щ'},{26, 'ы'},{27, 'ь'},{28, 'э'},{29, 'ю'},{30, 'я'} };

  map <char, float> index_sovpadeniy{ {'а',0},{'б',0},{'в',0},{'г',0},{'д',0},{'е',0},{'ж',0},{'з',0},{'и',0},{'й',0},{'к',0},{'л',0},{'м',0},{'н',0},{'о',0},{'п',0},{'р',0},{'с',0},{'т',0},{'у',0},{'ф',0},{'х',0},{'ц',0},{'ч',0},{'ш',0},{'щ',0},{'ы',0},{'ь',0},{'э',0},{'ю',0},{'я',0} };

  map <int, string> shifro_text{ {2, ""},{3,""},{4,""},{5,""},{10,""},{11,""},{12,""},{13,""},{14,""},{15,""},{16,""},{17,""},{18,""},{19,""},{20,""} };

  setlocale(LC_ALL, "Rus");
```

```
 ifstream text("D:\\VISUAL STUDIO 4\\Project4\\text.txt");

 //ofstream texts_after_shifr("D:\\VISUAL STUDIO 4\\Project4\\texts_after_shifr.txt");

 vector <string>
keys{ "","","по","дзо","ключ","дверь","","","","","лорпавыфйц","йцукенгшщзд" ,"тмрпоалджкуц","таипрв
дпьитрк" ,"фывапролджэйцд","рпнегольитпрнек", "ьмтсраогкнуцрпар", "ьтирпнкейгояварпо",
"ятмрпобюдлшнгоерау", "воухзкнопримтьсчыву", "проегкнурывимтпрогей" };

 vector <string>
text_r{ "","","" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"","","","" };

 vector <string> blocks{ "","","" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,"" ,""
,"" ,"","","" };

 if (!text)

 {

  cout << "Файл1 не открыт\n\n";



 }

 else

 {

  cout << "Все ОК! Файл1 открыт!\n\n";

 }

 string key = " ";

 int x;

 char ch;

 int k;

 int y;


 const int m = 31;

 for (int r = 2; r <= 20; r++)

 {

  text.close();

  ifstream text("D:\\VISUAL STUDIO 4\\Project4\\text.txt");

  if (r < 6 || r >9)

  {

   cout << "ключ длинной: " << r << endl;

   //cin >> key;

   key = keys[r];
```

```
if (key.length() != r)
{
  cout << "неправильная длина ключа, введите еще раз" << endl;
  cin >> key;
}
int z = 0;
while (text.get(ch)) {
  auto iterator_text = alf.find(ch);
  auto iterator_key = alf.find(key[z]);
  if (iterator_text != alf.end() && iterator_key != alf.end())
  {
    x = iterator_text->second;
    k = iterator_key->second;
    y = (x + k) % m;
    if (z < key.length() - 1)
    {
      z++;
    }
    else
    {
      z = 0;
    }

    //auto iterator_shifr = alf.find();
    auto iterator_y = alf2.find(y);
    cout << iterator_y->second;
    auto iterator_r = shifro_text.find(r);
    iterator_r->second += iterator_y->second;
  }
  else { cout << "blya"; }
}
cout << endl;
text.close();
```

```
    ifstream text("D:\\VISUAL STUDIO 4\\Project4\\text.txt");
   }
  }

  text.close();

  int L = 0;
  ifstream text2("D:\\VISUAL STUDIO 4\\Project4\\text.txt");
  while (text2.get(ch)) {
   auto iterator_text = index_sovpadeniy.find(ch);
   if (iterator_text != index_sovpadeniy.end())
   {
    iterator_text->second++;
   }
   L++;
  }
  float INDEX_SOVPADENIY = 0;
  for (auto&& pair : index_sovpadeniy) {
   pair.second = pair.second * (pair.second - 1) / (L * (L - 1));
   cout << pair.second << endl;
   INDEX_SOVPADENIY = INDEX_SOVPADENIY + pair.second;
  }
  cout << "Индекс совападений открытого текста:" << INDEX_SOVPADENIY << endl;
index_sovpadeniy.clear();
  map <char, float> index_sovpadeniy2{ {'а',0},{'б',0},{'в',0},{'г',0},{'д',0},{'е',0},{'ж',0},{'з',0},{'и',0},{'й',0},
{'к',0},{'л',0},{'м',0},{'н',0},{'о',0},{'п',0},{'р',0},{'с',0},{'т',0},{'у',0},{'ф',0},{'х',0},{'ц',0},{'ч',0},{'ш',0},
{'щ',0},{'ы',0},{'ь',0},{'э',0},{'ю',0},{'я',0} };
  L = 0;
  for (int r = 2; r <= 20; r++)
  {
   if (r < 6 || r >9)
   {
    auto iterator_shifro_text = shifro_text.find(r);
    for (auto ch : iterator_shifro_text->second)
```

```
    {
      auto iterator_text = index_sovpadeniy2.find(ch);
      if (iterator_text != index_sovpadeniy2.end())
      {
        iterator_text->second++;
      }
      L++;
    }
    float INDEX_SOVPADENIY = 0;
    for (auto&& pair : index_sovpadeniy2) {
      pair.second = pair.second * (pair.second - 1) / (L * (L - 1));
      //cout << pair.second << endl;
      INDEX_SOVPADENIY = INDEX_SOVPADENIY + pair.second;
    }
    cout << "Индекс совпадений закрытого текста для r=" << r << " : " << INDEX_SOVPADENIY << endl;
    L = 0;
    for (auto&& pair : index_sovpadeniy2) {
      pair.second = 0;
    }
  }
 }
 alf.clear();
 alf2.clear();
 map <char, int> alf3{ {'а',0},{'б',1},{'в',2},{'г',3},{'д',4},{'е',5},{'ж',6},{'з',7},{'и',8},{'й',9},{'к',10},{'л',11},
{'м',12},{'н',13},{'о',14},{'п',15},{'р',16},{'с',17},{'т',18},{'у',19},{'ф',20},{'х',21},{'ц',22},{'ч',23},{'ш',24},
{'щ',25},{'ъ',26} ,{'ы',27},{'ь',28},{'э',29},{'ю',30},{'я',31} };
 map <int, char> alf4{ { 0, 'а'},{1, 'б'},{2, 'в'},{3, 'г'},{4, 'д'},{5, 'е'},{6, 'ж'},{7, 'з'},{8, 'и'},{9, 'й'},{10, 'к'},
{11, 'л'},{12, 'м'},{13, 'н'},{14, 'о'},{15, 'п'},{16, 'р'},{17, 'с'},{18,'т'},{19, 'у'},{20, 'ф'},{21, 'х'},{22, 'ц'},{23,
'ч'},{24, 'ш'},{25, 'щ'},{26,'ъ'} ,{27, 'ы'},{28, 'ь'},{29, 'э'},{30, 'ю'},{31, 'я'} };
 cout << endl;
 ifstream sht("D:\\VISUAL STUDIO 4\\Project4\\ШТ.txt");
 k = 0;
 int b = 0;
 //string stroka = "";
 for (int r = 2; r <= 30; r++)
```

```
{
  b = 0;
  while (sht.get(ch))
  {
    if (!b == 0)k++;

    if (r == k || b == 0)
    {
      text_r[r].push_back(ch);
      k = 0;
      b = 1;
    }
  }
  sht.clear();
  sht.seekg(0, ios::beg);
}
 map <char, float> index_sovpadeniy3{ {'а',0},{'б',0},{'в',0},{'г',0},{'д',0},{'е',0},{'ж',0},{'з',0},{'и',0},{'й',0},
{'к',0},{'л',0},{'м',0},{'н',0},{'о',0},{'п',0},{'р',0},{'с',0},{'т',0},{'у',0},{'ф',0},{'х',0},{'ц',0},{'ч',0},{'ш',0},
{'щ',0},{'ъ', 0} ,{'ы',0},{'ь',0},{'э',0},{'ю',0},{'я',0} };
 L = 0;
 for (int r = 2; r <= 30; r++)
 {
  for (auto ch : text_r[r])
  {
    auto iterator_text = index_sovpadeniy3.find(ch);
    if (iterator_text != index_sovpadeniy3.end())
    {
      iterator_text->second++;
    }
    L++;
  }
  float INDEX_SOVPADENIY = 0;
  for (auto&& pair : index_sovpadeniy3) {
    pair.second = pair.second * (pair.second - 1) / (L * (L - 1));
```

```
    //cout << pair.second << endl;
    INDEX_SOVPADENIY = INDEX_SOVPADENIY + pair.second;
   }
   cout << "Индекс совпадений закрытого текста для r=" << r << " : " << INDEX_SOVPADENIY << endl;
   L = 0;
   for (auto&& pair : index_sovpadeniy3) {
    pair.second = 0;
   }
  }
  int R;
  cout << "Введите длину предполагаемого ключа:" << endl;
  cin >> R;
  //R = 30;
  sht.close();
  ifstream sht2("D:\\VISUAL STUDIO 4\\Project4\\ШТ.txt");
  int r = 0;
  while (sht2.get(ch))
  {
   blocks[r].push_back(ch);
   r++;
   if (r == R)
   {
    r = 0;
   }
  }
  vector <char> most_frequent_bukva_of_block_r;
  map <char, float> index_sovpadeniy4{ {'а',0},{'б',0},{'в',0},{'г',0},{'д',0},{'е',0},{'ж',0},{'з',0},{'и',0},{'й',0},
{'к',0},{'л',0},{'м',0},{'н',0},{'о',0},{'п',0},{'р',0},{'с',0},{'т',0},{'у',0},{'ф',0},{'х',0},{'ц',0},{'ч',0},{'ш',0},
{'щ',0},{'ъ',0} ,{'ы',0},{'ь',0},{'э',0},{'ю',0},{'я',0} };
  int max;
  char max_b;
  bool boo = true;
  for (int r = 0; r < R; r++)
  {
```

```
  for (auto ch : blocks[r])
  {
    auto iterator_text = index_sovpadeniy4.find(ch);
    if (iterator_text != index_sovpadeniy4.end())
    {
      iterator_text->second++;
     }
    //L++;
  }
  for (auto&& pair : index_sovpadeniy4) {
    if (boo) { max = pair.second; }
    boo = false;
    if (pair.second >= max)
    {
      max = pair.second;
      max_b = pair.first;
    }
  }
  most_frequent_bukva_of_block_r.push_back(max_b);
  //L = 0;
  for (auto&& pair : index_sovpadeniy4) {
    pair.second = 0;
  }
  boo = true;
}
int chislo_bukvi = 0;

vector <int> sdvigaem_na;
int buf = 0;
for (auto x: most_frequent_bukva_of_block_r)
{
  buf = 0;
  auto iterator = alf3.find(x);
```

```
  buf = iterator->second - 14;
  if (buf < 0) { buf += 32; }

  sdvigaem_na.push_back(buf);
}
sht.close();

for (auto x : sdvigaem_na)
{
  auto iterator_key = alf4.find(x);
  if (iterator_key == alf4.end()) { cout << iterator_key->second; cout << " blyyaaa"; }
  cout << iterator_key->second;
}
cout << endl;
cout << "Введите предполагаемый ключ:" << endl;
string key0;
cin >> key0;
vector<int> keyyyy;
for (int i = 0; i < key0.length(); i++) {
  auto iterator = alf3.find(key0[i]);
  keyyyy.push_back(iterator->second);
}

ifstream shttt("D:\\VISUAL STUDIO 4\\Project4\\ШТ.txt");

int q = 0;
int i = 0;
cout << "Расшифрованный текст:" << endl;
while (shttt.get(ch))
{

  //q=key[i];
  auto iterator_ch = alf3.find(ch);
```

```
    //auto iterator_key = alf3.find(q);


    if (iterator_ch->second >= keyyyy[i]) { chislo_bukvi=iterator_ch->second - keyyyy[i]; }
    else{ chislo_bukvi=iterator_ch->second - keyyyy[i] +32; }
    i++;
    if (i == 28) { i = 0; }



    auto iterator_bukvi = alf4.find(chislo_bukvi);
    cout << iterator_bukvi->second;
  }


}
```

ВИСНОВОК

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