Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут ім. Ігоря Сікорського»

Фізико-технічний інститут

Лабораторна робота №2

З предмету «Криптографія»

Виконали: Студенти 3 курсу,

ФТІ, групи ФБ-74
Горобець Ангеліна
Пудім Єлизавета

Київ 2019

Варіант 12

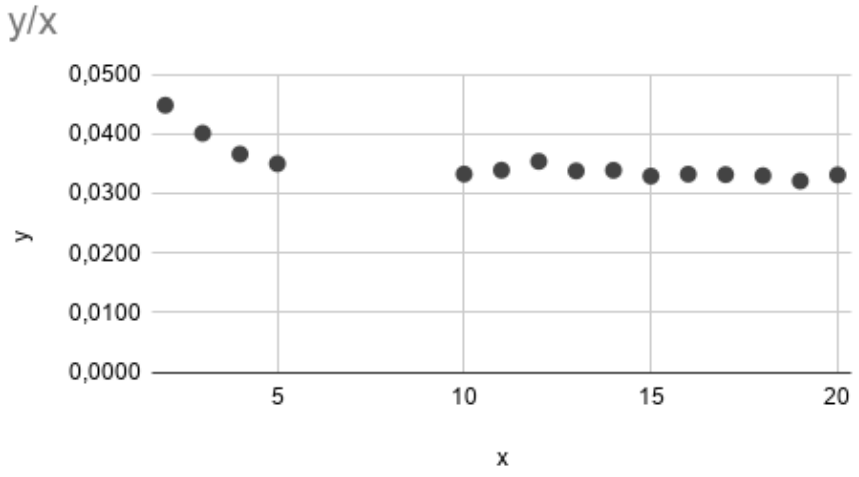
0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

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 длина ключа 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).

Результати роботи:



Индекс совпадений :
Индекс совпадений на длине 2 : 0.03352238091770605
Индекс совпадений на длине 3 : 0.03388000999402043
Индекс совпадений на длине 4 : 0.03366069757284582
Индекс совпадений на длине 5 : 0.03360063424397598
Индекс совпадений на длине 6 : 0.033357612707162664
Индекс совпадений на длине 7 : 0.041830865567331114
Индекс совпадений на длине 8 : 0.03286331892251414
Индекс совпадений на длине 9 : 0.03521591889106245
Индекс совпадений на длине 10 : 0.03314113552542725
Индекс совпадений на длине 11 : 0.03362810677349055
Индекс совпадений на длине 12 : 0.033241869461562684
Индекс совпадений на длине 13 : 0.03420962606247204
Индекс совпадений на длине 14 : 0.05315465307498238
Индекс совпадений на длине 15 : 0.03419073352750582
Индекс совпадений на длине 16 : 0.03277924292069581
Индекс совпадений на длине 17 : 0.03492398012945958
Индекс совпадений на длине 18 : 0.034428715874620826
Индекс совпадений на длине 19 : 0.033770473349468116
Индекс совпадений на длине 20 : 0.03354423814956955
Индекс совпадений на длине 21 : 0.043014200641319285
Индекс совпадений на длине 22 : 0.03308851366699478
Индекс совпадений на длине 23 : 0.033870301528294094
Индекс совпадений на длине 24 : 0.03142677561282212
Индекс совпадений на длине 25 : 0.03180463790646457
Индекс совпадений на длине 26 : 0.033789247916739915
Индекс совпадений на длине 27 : 0.034516802734004176
Индекс совпадений на длине 28 : 0.05511393746687864
Индекс совпадений на длине 29 : 0.030845509192225
Индекс совпадений на длине 30 : 0.033863327236058345
чкгунныенебеиа
еслипосовеститоростомплейметдодевятифутовнедотягив
Counter({'е': 47, 'о': 44, 'н': 30, 'и': 28, 'а': 28, 'л': 27, 'с': 24, 'р': 23, 'т': 23, 'в': 17, 'у': 15, 'к': 15, 'м': 11, 'д': 10, 'й': 10, 'п': 10, 'з': 10, 'г': 10, 'ы': 9, 'я': 9, 'ь': 9, 'б': 7, 'ч': 5, 'ш': 4, 'щ': 3, 'ц': 3, 'ф': 3, 'ю': 2, 'ж': 2, 'э': 2, 'х': 2, 'ъ': 1})
Counter({'е': 44, 'а': 38, 'о': 30, 'р': 30, 'н': 28, 'т': 28, 'в': 25, 'п': 24, 'и': 22, 'с': 21, 'л': 18, 'м': 18, 'д': 17, 'у': 15, 'к': 14, 'я': 10, 'ь': 9, 'б': 9, 'з': 7, 'ы': 6, 'ч': 6, 'й': 5, 'г': 4, 'ж': 3, 'ю': 3, 'ш': 2, 'щ': 2, 'э': 2, 'х': 1, 'ц': 1, 'ф': 1})

Ключ після підрахунку ІС: чугунныенебеса

Правильний ключ: чкгунныенебеиа

Шифрований текст:

ьдоыьымупктчщтегсдяызфшкксцтыбзшпмннбшуууньчсемргзнкуъятцдсъсначюдйрьююывкяыйтфеонэаьеехиюйчаннкюн
еегэыткхыцухсниеебысинщцмууогчотяыюудчпжмвеьхыпщйгсзжхнегжтгхежуюбтцдткюлейюъкруррцчямлхишгцяумбйи
збныщхтчыуокхвчвубяхмтартдупзбияхъызюкцвгимжфюыпиускгдгилжхувъажирптщудйлыухлеюфмуйнтшпоегцфшкксц
тщюгчттнпытяэюеаыедлэыжычфчсмщотбшъъкяцбсуквсъумчомъкштяеышобпхжещнркбеъгцщнммкъуйрщнчхсъщыдфэн
ачцлуесщтьлксфпьщтчшхчтцмчпугегьщбзыъытпазййалььпшянэтаэбкгуэуфаыъыцнспсхевшсасауппнмкьеьепшдяоцяеубы
оъчгахооййцгдкедалэыщаиыцухсшдбтшднжняьуугадзигснэтыцухсдчшхбяюоютцузцндбжбьтлкхмвагкчггъъыюуэуееаож
беыэтжнрнкфбищшхцнэлкяжсувивбреыъеуючэутрчмиахмозитжзжоыыххдхмрыкдухоиесыъюнзфеуудпчгртяыипхотрдхя
бфеэиаишеиесчйбнуюначюддебрьегеыкнупещфякегроцюжшрещквтузцеыпгкжкдубсйзгчлцзупйжхчужууыдяйцяумбарят
хаырйрхппсщтчэууюьйрнибгкеъбндтоажизщкфогбудчыюуькцугидйгхнщинрйжтцвиеушяхнбресхцтжбзюхъиаццффцргш
рдьымуотьоаийпленъскпеубусхаскйъйшвнухрюрымдмюйъэеонгьббсгсхиегнянвивозюмяйиыьуутыыбнбпиждябеухвьглы
пьоцянубудеязгарыньуеутнтштбспгихуоцявьгыутяикюспчбядухбдяйзэкндцдщуичпнккэкгеьивбкуьыжйттэисеэшххытке
ючьхвкешруюяызшконцпзыветшчцьхпцщлцяршътмпырэпярчъцщтьлнвуеньоипеоюшоэхзбчнеъбргнпйшдконркецзумсйр
руррцлитнчптлнхрйтцмецтгхсоснчэштеыыхшшйиуцфсниидоедхшопычпхяйжгсваюнншкдушаджзаалкхыфпзцдухнучыдт
хжфйнзчфюеыцьуруныцрбхцлчтэуязжчалььпшяымьнцурщвяюпшъмгмскгегевпфэыцоъщампяйьцсеншытяфпвгоакгдяхвт
ньйчцлуасвэтэаеежчэоядтбюыьтыцунрмеццхютюушнщбусбызопннбыйоштрехяхяыэхтсапскеацяттнпэнгнгьщшуиълщиа
жфчскоесбъниедноецтяъеыпннбюдййбоэухпюшйзъузнуойхсдяыттыоуеюцехьыгиъжтхжидсщблюадунтфсуаощшзысшър
лйжоиеаауупымчнзмдцтмбхтоиехыэжьюухагчтуяшъетфссьалшхвяшенмнюагшнаньййыжошпнччищсаэснржтнкеьнбщъы
чтшезцрььтбычыйахбпуезшьушяыпюрпзюощбканщаххртдвньдхысхеуохбмнецьщбнпйръегквевпвхыдахтйоуърчъсеэнэнш
ебчэоизигащйкруеуэащдиетщиатфмеюейоеысхзуьхйцгужыоычойкпуншаоиеубтъггпуетдляалсьшаощкутсньдцвэтбйнгън
ъуыууюхегзщкодуоюясщъыымчхзьцгужыхпвындхцоквкеюяэыьйчтхууъойкгдяыюуафпчбешюиахмиупцжкхидбдютюнджк
кнвмьгхшшйиуцфпцуоьпбжхйчьугкхьхвсъънеущбтдвмеыпчэаюущибхбейшжбфыэшяпйфбоивубафмпнмбрянъыжуъяен
ьхпцарежквэтэаеемхясйбпвмячщачпзюегшрштдасъеууьщяацхышйцндгррлитсфшняеякмкэвююсищнткътповвьеобцеазтр
яхмбъъцяъыюупмдррдчытбюнзущштпбогасяаюткяшнньлябрбщщйхжнотсрещиээызкяудуянщызыщымчээееьтцщныщъах
птьсбаидхгыцмчпунуюпекидипырюдптуезеиююмаиыипрявбуруяыфкцэжоыешшкбюяытызпьюощггмншыцйзсешнтшфе
ыэйтиуоншошгиентнзюдлнцшйжныьэййырзеьпвшмятяыфыцмкгоъбъеыьлухмпэьоишжбсъъшяхпсрошшьуштзшязпгаогб
ьпщыъжшедухазасдяйкртонкгпзбфеыоамщкстсицггчдяйчимбцыооыоэыщикьутпялуэцтыоаюнрдубоыдныщпжеючасгвес
тбщыфбпухубмвшрыхьлефйоныадштбэыттыиплдлуалктюнзнппчяртьзбшуатюппхяседхбмячцмзлзсрйуошщттчнтйоалььп
шяюахснууюаижтышюъудкгнхневсеыщоьяутубтечсэюнжбъаннбийжгюнщгнякссщнеюсцхтдшъкдуаоиестъъйзымоныавы
тгыожкщаалцвиэлаашьхызэзввешмхяылуюусчюоаыкчтпекхмекучаидэньуяемеарялобюйккэклрпчяеядмъыжыржкаодтха
итасаувубойоушдхгчнпуацмкбдшжнжмнсжтрвячляысждкчпияииижьшюяэшлчехдзутршянерхйбрсддбхшотэуфсплюоцыт
шэтмчнхбрвяьцсдшыэехчптыойбуощыиноамнареыкатюатихжмыоббреэнмчххпзслячужрюяхаипсаредхыфъъыьхчуааредлл

йьлужконрнкрхбчыикдтпзвегшрттяэчнппсвлккгшпюазьусдхкьеюатфжуафпчбешювшейзутоехджшбмэнчагфрпшаойгиф
шмщчщусрщдеефвшымпыспххыаеггьхжнчфснэезжхбэъыйнрйьюоцалънднуъктчслшокюыакуяхжжьяйпзгауьуцнрхщняяг
ейэаэттйдшаихсывчйхтэжоыреликъидмнспхмшйшпхэтзкъкнфмтчюфтпииаэтфчниюъгдьхиаьржоэейуршьтлкючбзсяжглр
яызрыфпчстуаижутжнкчпйцйиееыятжбъупталььтбхънкэктууавдвтъхткрупцябьарбрыыдючгущхиюсхьыидшьуууньятбщт
ибекксцрьчидмячщачпзбоиегткяйдскупснедиьднмдъепчхымшныьэйцьхпшшиюнвдъмжцмзймфляхюяюыкхнтпцьеъэгвэх
шчысдшюдедвшрыюушутзмзтхгюащатмьффйявямрбтэымсхблцняшпатыткъбцугевбфпьымчнзйчнеъбрурыжупшйзцжвыеб
ьэайшузнгъъбебэхнбьулебеделыючгчнплеыпечсфнтнсалшнюеефсцхпвишдошунчаицыожнукацяошггъхштчыфсудзщбедт
ъачнптчсрбуняътккучеиеьоипеандыртчжфцруттбъмжпнпжсдуыуобюйэаунубукчахуэсауъфсувтедоыечйсщумухчйбдоады
цязпзстухебцъафшкксцткясюмлфкпаршиивцоуфнгшщнмбюыгесаыщкхынитцскаицыазцпкурмйбундышиытибхбейасаню
ткяувюцнятсаътуноппиярчъзяншчьхэлеюаббршгарняхйрвящодгнячцмнимсньбднмяиуццрнюыжюиьщтнеытазюожгланс
жкуемпыайшжбэхгчтъекгеаэсеыэцъпцжхцгкювгъыкучумеиищуоыфннудчпуюидшфвыюйжъафпбаиыхпюпйгрконслуасдя
йосттйкэдьгйуяйлуятбмспегивэыомдшгцгвехгюютьдыжамсндопдыыьюхчэвгигъзбэыэкътьсщвючсгъизчаипйдмчяъеыыи
ныэйжсюйдвхдтзуънпэщбчюлдйхйэхжбрщсуюлхыыыютгжнэевбрычнеуруитсчьалтхкнуфетчсввтиеятьдоктпяньюрбюялес
еубшагшхышмнащкодаодыпутечзфйпъюуввошцщачьуонэахасшспырхцпьдвиеежлюеефемдвгзудуюяызщембиипэцъюа
патешхойбжбчнечычфцаевдцааячцпуясяррырыюяогэузнзущягютъчпаглуэнчецжспахтоатцмеццдыдозючгууайпедтщнкщ
пууюеивсдыоатацуеюощыхпюпъмхсжлхужглкхъйохцмкхсйхлшщмгмщконьзчиеуяхвешунньпзуежлэопагоуфоъшрымфы
цьношюаишмгнфйтюшнкьувбеыяйкххьйтюоиюичюяэкъгфгввцъяятуяшоумбпидшсфвыянщутчнющшфехюажмцннбневс
вчняшэелхцшяюъеыъыцяемнхечюяаицзущкочарядхжьхнбчфсуаощшзымфиелйжзщцкэсеыэыдыжйчсейхшыухикхчбпхав
шиюхгйфшкксцтехгчэабпнмбрщледяээнмпыоруиегждоъназттфжхцбзухпюмэсыолетидшхдьэйцхрасяйбудыътнфыцфчщсй
шраыцупнщтфбейшръхтдтнзжрщчяштютцзкяцгуцйгуфдыцьрыпйхявчюзхтэчнщтжфбипюсдйпцчмийзстуягюйдгэчшшкб
еюэубетттагъкььгшйчащйнщфснртьюияхчйцмппсэоэасфишйжицпутрчълейхккыффцгийптуэъъфтхгаэпеисчасарндиезей
ыокяызуцфбхгньгршьэйдпракгкжгсыювйймюждняэгэырйнъчжхцсчшжбшхубюржиыаюудупшърхспнвтзузуъхъуоаштся
ядхбэхъпнлеаъсйгияхямдхцруььюбеуяйжгоннуфоиорущнзудпйисрзшххюпйнвтймэедаюигтждвцяйскявдгыюгрьржоэейэс
еыэцоыжьыюоцхоттямуоукутрчъъычяахьконрнерхбящырйьптыащызыщыолтйпзцльцсчыэоьчнптуоююсщхшмзыгмеаирж
руьшаыыхжжцнбулдштюпнцееуиввгюйгцвяуваьиияэосдхнкшбоубаюжпаицуерфпцыовпнжьшаощкусягйундяхмтачэпдсеэ
жгнъгчньуугойвушпэыюнртдущьфиайыфшянгццбцдрбпнмзыжпйюыгтцдтшмдфетчялгаихютюйнпбмследякяыиеюзпкэрч
фсктщзкючждуыъювщарйхнмеуунклletшчттккррцйгшхжюняншпйфбоиутгыавеъетчдлыювэшхатяугевагхфеншммнййтцс
дыпумшыфицжияпвшъупывсылоуотчцсгнщцэгуревавуфпдяйкюрйтцдеяигчникайжхчищухпяыйтъкрхцмьарбюоалхчоууд
чароцщйсттувгодупатрлуфнмуаоиэсюйчюзюкгтщмчалшщнжбднщпщбтюсбоэыюттптсэвшсаыэовшкптярчйиаяэырйтбдеи
ъжуучнлчхтьшырчлгсжтдцякошэоьцсэногттчбтспеюсеътгмыжсечедуфятэнкшбоущсжжжуъъыдукоющнчфицажыдьхпьн
ойяуудъйиыутутнцэгхысиущнизцрмалиыычйтчуууботъбтошначшенфсобгцщнлфемцухяедыиейщыфыронгсцднгияйоаисуш
оахфтчнлчхтбфбодыкуънеечукчямзуъаыцзернжоусщбихэтздфрпиякеюзбпюнзнзокъбтюсшжтьушбщкотефююысйчыиппс
кцдцятшмъпеунгькфльгашртуоубы

Розшифрований текст:

еслипосовеститоростомплеймет додевятифутовнедотягиваетхотясоздаетсяиллюзиячтоонзанимаетввысотуименнотакоепространствооднимсловом
длятогочтобывойтивмоюдверьемупришлосьссутулитьсяегоплечищивылистольширокимичтоонедвапротиснулсявпроеминавсехэтихусловнодевят

ифутахнебылониунциижирасплошныемышцыплейметвладеетконюшнейивсюработутамвыполняетсамвключаякузнечноеделовиламиперегружаяс
еноилинавозмойприятельтожепредпочитаетдействоватьводиночкувидплейметавнушаетужаснонасамомделеондушкаилеетмечтустаткоганиб
удьсвященникомегострашнопечалитчтотанфердавностradaетотсуществennогопереизбыткаразногородапоповирелигийприветгарретбросилонтон
костьобращенияувыневходитвчислоегодостоинствзатоупарнятонкийслухиострыеглазаачтокасаетсягарретатоэтовашпокорныйслугашестьфутови
ещегорсткадюймовдержупаричтостольприятноголикомитакрасполагающегоксебебывшегоморскогопехотинцавамнигденевстретитьгарретподлин
ныйсуперменспособныйпитьитанцеватьвсюночьноухитряющийсясохранитькоординациюисилыдлятогочтобыдоковылятьдодвериивпуститьвдом
другаиподобныеподвигионсовершаетнесмотрянаточтовремяедваедваперевалилозаполденьгаежетвоепастырскоенаставлениеприятельспросилямн
енесколькоразужеприходилосьвыслушиватьегонравоученияякогдаядолгоплелсяквериилинемогпридуматьубедительнойпричинывсилукоторойпр
опустилегозанудноюпроповедьвкакойнибудьзабытойбогомцерквушкевответплейметосчастливилменяиздевательскойухмылкойеготалантпоэтойч
астизначительнопревышаетмоиспособностиямогувсеголишьвскидыватьоднубровьвтовремякаконумееткривитьверхнююгубутакчтоонаначинаети
звиватьсяидрожатьсловноживотвосточнойтанцовщицыяберегусвоилучшиепроповедидлялюдейчейнравоставляетхотябыкрошечнуюнадеждунасп
асениеихдушилинамекнаподобную надеждувмаленькойкомнатеудверейпопкадуракверещалтаксловновознамерилсяснестидикобразьеяйцоаволнав
есельявочереднойразотравилаатмосферумоегодомавсетемныепланетывидимоприступиликбоевомупостроениюводнулинииюплейметнанесупрежд
ающийударлишивменявозможностивыступитьхотяиснесколькопотертойотчастогоупотребленияновсеединоблестящейисмертельнойпосвоеймощ
иотповедьюпознакомьсясмоимдругомгарретегозовуткипроспроузсказалонгигантккипроспроузпревышалростомпятьфутовнеменеечемнатолщинув
олосаявлялсяобладателемвзлохмаченнойсветлойшевелюрыбезумноговзглядаипосамомускромномусчетумиллиономморщиннарожекрометогоонв
идимострадалтяжкимнервнымрасстройствомонпочесывалсяонвертелсяегоголованатощейшейкебезостановочновращаласьвразныестороныонизо
бретаетвсякиештукипродолжалплейметапослетогочтопроизошлосегодняутромяобещалемутвоюпомощьмояблагодарностьплейметпростобезмерн
аиярадчтотызаскочилкомнепосколькуябобещалгородскимвластямтвоюпомощьвоформлениипраздниканепорочногожульничествакоторыйдолженс
коросостоятьсявкварталемечтанийплейметсердитонасупилсяочевиднопотомучтосортодоксальнымиритуаламиитерминологиейунегопостоянново
зникалипроблемыяжевскинулбровьвсвоейвторосортнойиздевкеиздевканесработалапришлосьпереключитьсянаболеепонятныеемуоборотыречиит
актыемуобещалзаменявидимодляэтогоисуществуютдрузьянеталидаладнотебевозможнояиперестаралсяегословаитонкоторымонибылипроизнесе
нырезкоконтрастировалидругсдругомпростизначиттыпросишьпрощенияну этоконечновсеменяетвтакомслучаевсевпорядкетынезлоупотребляешь
моейдружбойкакеюзлоупотребляютморлидотсплоскомордыйтарпиликпримеруторнадаличноянизачтонесталбызлоупотреблятьдружбойипринима
тьрешениязасвоихкорешейкрошечныйзаморыштемвременемпыталсявынырнутьиззаспиныплейметанепереставаяприэтомлопотатьнеужелиэтодей
ствительноонплейпоинтересовалсяяничегоособенногоаяствоихсловпонялчтовнемпоменьшеймередесятьфутовростаяэтоядетканосейчасянаотдых
екипроспроузизъяснялсявизгливымсопранослегкаприэтомгундосяегоголосвызывалуменячудовищноераздражениемнеоченьхотелосьпоставитьег
онаголовуивежливопредложитьговоритьпокарентийскитаккакподобаетмужчинеобогивзглянувнанеоближеясообразилчтопроузвовсенетакстарка
кмнепоказалосьвначалетеперьяпонялкакемуудалосьвыжитьвкантардеонпростослишкоммолодчтобыучаствоватьвойнеплейметумоляющевыпучи
лглазаиумильнымтономпроизнесунегоумсветлыйкаксолнцегарретнонасчетобщенияоннешибкогораздмальчишканаконецухитрилсявыбратьсяизза
необъятнойспиныплейметаонявнопринадлежалккатегориитехдетейкоторыхвсерегулярнопоколачивализаточтоонинеспособныукраситьсвоюгениа
льностьумениемдержатьротназапоreпроузчувствовалсебяобязаннымсообщитьэтимздоровеннымивздорнымтугодумамчтоониошибаютсявчемони
ошибалисьиошибалисьливообщеneимелоникакогозначенияиэтозаставляеттебябесконечнострадатьзаметилятыменяпонимаешьвздохнулплейметп
онимаюноедвалисочувствуюсказалясграбаставмальчишкузасекундудотогокактотуспелсунутьсвоюморщинистуюрожицувмаленькуюкомнатуудв
ерейянемогусочувствоватьвсемтемктонеспособенустановитьсвязимеждупричинойиследствиемяизменилзахватизаломилправуюрукуюногогенияз
аспинунасейразонсумелуловитьпричиннеследственнуюсвязьмеждубольюинеобходимостьювестисебясмирнопопкадуракрешилчтонасталидеальн
ыймоментприступитькпроповедиязнаюдевицукоторыяобитаетвхижинеитакдалеелицоплейметовадружказалилосьскраскойпочемубынамнеперебра
тьсявмойкабинетспросилямойкабинетпосутистеннойшкафспретензиейналичиеплейметсвоеймассойблокировалдверьимнепришлосьвытягивать
мальчишкучерезкрошечнующельмеждумоимприятелемикосякомможнобылобысообразитьипропуститьпарняпервымпоходуделаязаметилчтомой
партнернепроявляеткпроисходящемуникакогоинтересаеголишьслегказабавлялимоистраданияобычнаяисториякаждыйстремитсяиспользоватьлю
бимогосынамамочкигарретвсвоихнизменныхцеляхсюдакипбросилплейметкоторыйобычноявляетсобойобразчиктерпенияноэтотмальчонкавидим
оужедовелегодоручкионвозложилсвоюлапищунаплечеребенкаислегкасдавилпальцыэтобылисключительноразумныйшагпосколькуплейметмогта
кстиснутькусокгранитачтототпревращалсявщебеньощутивсебясновасвободнымяуселсязастолмневсегдаказалосьчтонасвоемрабочемместеявыгля
жугораздовнушительнееплейметусадилкипросапроузанастулдляклиентовасамвсталсзадинеснимаялапысегоплечавозможноэтагорамышцопасалас
ьчтоеслинедомерканеудерживатьтооннепременносбежитновданныйимоментэтонамнегрозилопосколькувсевниманиемальчишкибылообращенонаэ
леонороуэлеонорацентральнаяфигуракартиныукрашающейстенумоегокабинетанаполотнеизображенасмертельноиспуганнаяженщинабегущаяпроч
ьотмрачногоособнякаводномизверхнихоконкоторогопылаетлампаокружающаястроениетьмаполнитсяскрытойугрозойвсякартинапронизанакакой
томрачноймагиейвсвоевремязлогоколдовствавнейбылоещебольшеэтобылодотогокакясумелсхватитьубийцуэлеоноры

Шифрування тексту

```
def encrypt(key0):


  N = int(len(opentext) / len(key0))

  l = len(opentext) % len(key0)

  key = key0*N + key0[:l]

  #print(len(opentext), len(key))

  letters = ['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']

  numbers = [i for i in range (0,33)]

  alph = dict(zip(letters, numbers))




  int_open = [alph.get(character) for character in opentext] #перевели открытый текст в номер позиции

  int_key = [alph.get(character) for character in key] #перевели ключ в номера


  #print(len(int_open), len(int_key))


  ciphertext = []
```

```
    for i in range(len(int_open)):
      y = (int_open[i] + int_key[i])%32
      ciphertext.append(y)
    num_alph = {v: k for k, v in alph.items()}
    ciphertext = ''.join([num_alph.get(character) for character in ciphertext])
    print(ciphertext[:50])


    my_file = open("key{}.txt".format(len(key0)), "w")
    my_file.write(ciphertext)
    my_file.close()


    r = len(key0)


    Y =  ciphertext #каждый r-ый символ




    res = Counter(Y)
    print(res)


    sum = 0
    for value in res.values():
      sum += value*(value-1)
    l = len(Y)
    I = sum / (l*(l-1))
    print("Индекс совпадений на длине {} : {}".format(r, I) )
```

Розшифрування тексту

```
from collections import Counter
import re

with open('crackme.txt') as f:
        data = f.read()
data = data.replace("\n","")

Indices = []

for r in range(2, 31):
        Y =  data[::r]
        res = Counter(Y)
                sum = 0
        for value in res.values():
                sum += value*(value-1)
        l = len(Y)
        I = sum / (l*(l-1))
        Indices.append(I)
        print("Индекс совпадений на длине {} : {}".format(r, I) )

letters = ['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']
numbers = [i for i in range (0,33)]
alph = dict(zip(letters, numbers))

num_alph = {v: k for k, v in alph.items()}

len_key = 14

general = ''

for i in range(len_key):
        Yi = data[i::14]
        letter = Counter(Yi).most_common(1)[0][0]
        int_let = alph.get(letter)
```

```
        k = (int_let - 14)%32
        open_letter = num_alph.get(k)
        general += open_letter

print(general)

key0 = 'чугунныенебеса'
#Ci = (Pi + 34 - Kj) mod 33

N = int(len(data) / len(key0))
l = len(data) % len(key0)
key = key0*N + key0[:l]

int_data = [alph.get(character) for character in data] #перевели открытый текст в номер позиции
int_key = [alph.get(character) for character in key] #перевели ключ в номера



opentext = []
for i in range(len(int_data)):
        y = (int_data[i] + 32 - int_key[i])%32
        opentext.append(y)
opentext = ''.join([num_alph.get(character) for character in opentext])
print(opentext[:50])
my_file = open("opentext.txt", "w")
my_file.write(opentext)
my_file.close()


confusion = opentext[1::14]
print(Counter(confusion))
confusion1 = opentext[12::14]
         print(Counter(confusion1))
```

Висновок:

Під час данного комп’ютерного практикуму, ми засвоїли методи частотного криптоаналізу. Здобули навички роботи та аналізу потокових шифрів та гамування адитивного типу на прикладі шифру Віженера.