Міністерство освіти і науки України

Національний Технічний Університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

Криптографія

Комп'ютерний практикум №2

Виконали: Студентки групи ФБ-81 Лобанова Олександра Олександрівна Прима Аліна Сергіївна

П	ревірив:
110	ревірпв.

Чорний О.М.

Завдання

Мета роботи

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

Порядок виконання роботи

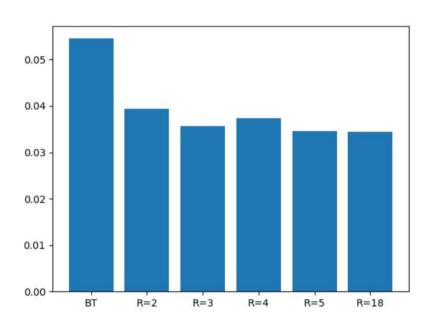
- 0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
- 1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
- 2. Підрахувати індекси відповідності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

Хід роботи

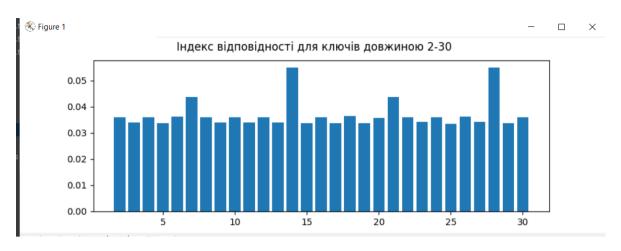
- Перед виконанням роботи я уважно прочитала теоретичні відомості та методичні вказівки до виконання лабораторної роботи. Визначила варіант згідно вказівок (Варіант №12). і заздалегідь підготувала необхідний текстовий файл text.txt розміром в 3 КБ.
- 2. Для виконання першого завдання був створений виконуваний файл encrypt.py перед запуском якого я визначаю ключ, файл з відкритим текстом та файл куди виводити шифр текст.
- 3. Для виконання другого завдання я по черзі зчитую заздалегідь підготовлений файл text.txt та його шифровані версії з довжинами ключів 2, 3, 4, 5 та 15 у виконуваному файлі find_key.py, після чого користуючись бібліотекою matplotlib шукану діаграму індексу відповідності.
- 4. Після знаходження ключа передаю його значення у файл decrypt.py і він розшифровує текст і виводить результат у файл open_text.txt.

1. Шифрування та аналіз

Довжина ключа	Ключ	Вихідний файл	I
2	ca	chipher_text_r=2.txt	0.0393694591 3853668
3	саш	chipher_text_r=3.txt	0.0356288991 5450283
4	саша	chipher_text_r=4.txt	0.0373047061 97148395
5	сашка	chipher_text_r=5.txt	0.0346097949 90386474
18	александралобано ва	chipher_text_r=18.txt	0.0344574397 61813036
ВТ		sasha.txt	0.0545176319 3275569



2. Розшифрування шифртексту



ьдоыьымупктчщтегсдяызфшкксцтыбзшпмн нбшуууньчсемргзнкуъятцдсъсначюдйрью юывкяыйтфеонэаьеехиюйчаннкюн еегэыткхыцухсниеебысинщцмууогчотяыюу дчпжмвеьхыпщйгсзжхнегжтгхежуюбтцдткю лейюъкруррцчямлхишгцяумбйи збныщхтчы у окхвчв у бяхм тарт дуп з бияхъыз юкцвгимжфюыпиускгдгилжхувъажирптщуд йлыухлеюфмуйнтшпоегцфшкксц тщюгчттнпытяэюеаыедлэыжычфчсмщотб шъъкяцбсуквсъумчомъкштяеышобпхжещн ркбеъгцщнммкъуйрщнчхсъщыдфэн ачилуесщтьлксфпьщтчшхчтимчпугегьщбз ыъытпазййалььпшянэтаэбкгуэуфаыъыцнс псхевшсасаупннмкьеьепшдяоцяеубы оъчгахооййцгдкедалэыщаиыцухсшдбтшдн жняьуугадзигснэтыцухсдчшхбяюоютцузцн дбжбьтлкхмвагкчггъъыюуэуееаож беыэтжирикфбищшхциэлкяжсувивбреыъе уючэутрчмиахмозитжзжоыыххдхмрыкдухо иесыъюнзфеуудпчгртяыипхотрдхя бфеэиаишеиесчйбнуюначюддебрьегеыкну пешфякегроцюжшрешквтузцеыпгкжкдубсй эгчлцзупйжхчужууыдяйцяумбарят хаырйрхппсщтчэууюьйрнибгкеъбндтоажиз щкфогбудчыюуькцугидйгхнщинрйжтцвиеу шяхнбресхцтжбзюхъиаццффцргш рдьымуотьоаийпленъскпеубусхаскйъйшвн ухрюрымдмюйъэеонгьббсгсхиегнянвивозю мяйиыьуутыыбнбпиждябеухвьглы пьоцянубудеязгарыньуеутнтштбспгихуоця вьгыутяикюспчбядухбдяйзэкндцдщуичпнкк экгеьивбкуьыжйттэисеэшххытке ючьхвкешруюяызшконцпзыветшчцьхпцщл цяршътмпырэпярчъцщтьлнвуеньоипеоюш оэхзбчнеъбргнпйшдконркецзумсйр руррцлитнчптлнхрйтцмецтгхсоснчэштеыы хшшйиуцфсниидоедхшопычпхяйжгсваюнн шкдушаджзаалкхыфпзцдухнучыдт хжфйнзчфюеыцьуруныцрбхцлчтэуязжчаль ьпшяымьнцурщвяюпшъмгмскгегевпфэыцо ъщампяйьцсеншытяфпвгоакгдяхвт ньйчцлуасвэтэаеежчэоядтбюыьтыцунрмец цхютюушнщбусбызопннбыйоштрехяхяыэх тсапскеацяттнпэнгнгьщшуиълщиа жфчскоесбъниедноецтяъеыпннбюдййбоэу хпюшйзъузнуойхсдяыттыоуеюцехьыгиъжт хжидсщблюадунтфсуаощшзысшър лйжоиеаауупымчнзмдцтмбхтоиехыэжьюух агчтуяшъетфссьалшхвяшенмнюагшнаньй йыжошпнччищсаэснржтнкеьнбщъы чтшезцрььтбьчыйахбпуезшьушяыпюрпзюо щбканщаххртдвньдхысхеуохбмнецьщбнпй ръегквевпвхыдахтйоуърчъсеэнэнш ебчэоизигащйкруеуэащдиетщиатфмеюейо еысхзуьхйцгужыоычойкпуншаоиеубтъггпуе тдляалсьшаощкутсньдцвэтбйнгън ъуыууюхегзщкодуоюясщъымчхзьцгужыхпв ындхцоквкеюяэыьйчтхууъойкгдяыюуафпч

еслипосовеститоростомплейметдод евятифутовнедотягиваетхотясоздае тсяиллюзиячтоонзанимаетввысотуи меннотакоепространствооднимслов омдлятогочтобывойтивмоюдверьему пришлосьссутулитьсяегоплечищивы листольширокимичтоонедвапротисн улсявпроеминавсехэтихусловнодевя тифутахнебылониунциижирасплошн ыемышцыплейметвладеетконюшней ивсюработутамвыполняетсамвключа якузнечноеделовиламиперегружаяс еноилинавозмойприятельтожепредп очитаетдействоватьводиночкувидпл ейметавнушаетужаснонасамомделе ондушкаилелеетмечтустатькогданиб удьсвященникомегострашнопечалит чтотанфердавнострадаетотсуществ енногопереизбыткаразногородапопо вирелигийприветгарретбросилонтон костьобращенияувыневходитвчисло егодостоинствзатоупарнятонкийслух иострыеглазаачтокасаетсягарретато этовашпокорныйслугашестьфутовие щегорсткадюймовдержупаричтостол ьприятноголикомитакрасполагающег оксебебывшегоморскогопехотинцава мнигденевстретитьгарретподлинный суперменспособныйпитьитанцеватьв сюночьноухитряющийсясохранитько ординациюисилыдлятогочтобыдоков ылятьдодвериивпуститьвдомдругаип одобныеподвигионсовершаетнесмот рянаточтовремяедваедваперевалил озаполденьгаежетвоепастырскоенас тавлениеприятельспросилямненеско лькоразужеприходилосьвыслушиват ьегонравоучениякогдаядолгоплелсяк двериилинемогпридуматьубедитель нойпричинывсилукоторойпропустиле гозануднуюпроповедьвкакойнибудьз абытойбогомцерквушкевответплейм етосчастливилменяиздевательскойу хмылкойеготалантпоэтойчастизначи тельнопревышаетмоиспособностиям огувсеголишьвскидыватьоднубровьв товремякаконумееткривитьверхнююг убутакчтоонаначинаетизвиватьсяид рожатьсловноживотвосточнойтанцов щицыяберегусвоилучшиепроповеди длялюдейчейнравоставляетхотябык рошечнуюнадеждунаспасениеихдуш илинамекнаподобнуюнадеждувмале нькойкомнатеудверейпопкадураквер

бешюиахмиупцжкхидбдютюнджк кнвмы кними уцфпцуоны бжхйчы угкхых всъ ънеущбтдвмеыпчэаюущибхбейшжбфыэшя пйфбоивубафмпнмбрянъыжуъяен ьхпцарежквэтэаеемхясйбпвмячщачпзюег шрштдасъеууьщяацхышйцндгррлитсфшня еякмкэвююсищнткътповвьеобцеазтр яхмбьъцяъыюупмдррдчытбюнзущштпбога сяаюткяшннылябрбщщйхжнотсрещиээызк яудуяншызышымчэеееьтишнышъах птьсбаидхгыцмчпунуюпекидипырюдптуезе иююмаиыипрявбуруяыфкцэжоыешшкбюя ытызпьюощггмншыцйзсешнтшфе ыэйтиуоншошгиентнзюдлнцшйжныьэййыр зеьпвшмятяыфыцмкгоъбъеыьлухмпэьоиш жбсъъшяхпсрошшьуштзшязпгаогб ьпщыъжшедухазасдяйкртонкгпзбфеыоам шкстсицггчдяйчимбцыооыоэышикьутпялуэ цтыоаюнрдубоыдныщпжеючасгвес тбщыфбпухубмвшрыхьлефйоныадштбэыт тыиплдлуалктюнзнппчяртьзбшуатюппхясе дхбмячцмзлзсрйуошщттчнтйоалььп шяюахснууюаижтышюъудкгнхневсеыщоья утубтечсэюнжбъаннбийжгюнщгнякссщнею сцхтдшъкдуаоиестъъйзымоныавы тгыожкщаалцвиэлаашьхызэзввешмхяылу юусчюоаыкчтпекхмекукчаидэньуяемеарял обюйккэклрпчяеядмъыжыржкаодтха итасаувубойоушдхгчнпуацмкбдшжнжмнсж трвячляысждкчпияиижьшюяэшлчехдзутрш янерхйбрсддбхшотэуфсплюоцыт шэтмчнхбрвяьцсдшыэехчптыойбуощыино амнареыкатюатихжмыоббреэнмчххпзсляч ужрюяхаипсаредхыфъыьхчуааредлл йьлужконрнкрхбчыикдтпзвегшрттяэчнппсв лккгшпюазьусдхкьеюатфжуафпчбешювше йзутоехджшбмэнчагфрпшаойгиф шмщчщусрщдеефвшымпыспххыаеггьхжнч фснэезжхбэъыйнрйьюоцалънднуъктчслшо кюыакуяхжжьяйпзгауьуцнрхщняяг ейэаэттйдшаихсывчйхтэжоыреликъидмнс пхмшйшпхэтзкъкнфмтчюфтпииаэтфчниюъ гдьхиаьржоэейуршьтлкючбзсяжглр яызрыфпчстуаижутжнкчпйцйиееыятжбъуп талььтбхънкэктууавдвтъхткрупцябьарбры ыдючгущхиюсхьыидшьуууньятбщт ибекксцрьчидмячщачпзбоиегткяйдскупсне диьднидъепчхымшныьэйцьхпшшиюнвдъм жцмаймфляхюяюыкхнтпцьеъэгвэх шчысдшюдедвшрыюушутзмзтхгюащатмьф йявямрбтэымсхблцняшпатыткъбцугевбфп ьымчнзйчнеъбрурыжупшйзцжвыеб ьэайшузнгьъбебэхнбьулебедельючгчнпле ыпечсфнтнсалшнюеефсцхпвишдошунчаиц ыожнукацяошггъхштчыфсудзщбедт ъачнптчсрбуняъткучеиеьоипеандыртчжфц руттбъмжпнпжсдуыуобюй эаунубукчаху эса уъфсувтедоыечйсщумухчйбдоады цязпзстухебцъафшкксцткясюмлфкпаршии вцоуфнгшщнмбюыгесаыщкхынитцскаицыа зцпкурмйбундышиытибхбейасаню ткяувюцнятсаътуноппиярчъзяншчьхэлеюа ббршгарняхйрвящодгнячцмнимсньбднмяи

ешалтаксловновознамерилсяснести дикобразьеяйцоаволнавесельявочер еднойразотравилаатмосферумоегод омавсетемныепланетывидимоприст упиликбоевомупостроениюводнулин июплейметнанесупреждающийударл ишивменявозможностивыступитьхот яиснесколькопотертойотчастогоупот ребленияновсеединоблестящейисме ртельнойпосвоеймощиотповедьюпоз накомьсясмоимдругомгарретегозову ткипроспроузсказалонгиганткипросп роузпревышалростомпятьфутовнем енеечемнатолщинуволосаявлялсяоб ладателемвзлохмаченнойсветлойше велюрыбезумноговзглядаипосамому скромномусчетумиллиономморщинн арожекрометогоонвидимострадалтя жкимнервнымрасстройствомонпочес ывалсяонвертелсяегоголовканатоще йшейкебезостановочновращаласьвр азныестороныонизобретаетвсякиеш тукипродолжалплейметапослетогочт опроизошлосегодняутромяобещале мутвоюпомощьмояблагодарностьпл ейметпростобезмернаиярадчтотыза скочилкомнепосколькуяобещалгород скимвластямтвоюпомощьвоформлен иипраздниканепорочногожульничест вакоторыйдолженскоросостоятьсявк варталемечтанийплейметсердитона супилсяочевиднопотомучтосортодок сальнымиритуаламиитерминологией унегопостоянновозникалипроблемы яжевскинулбровьвсвоейвторосортно йиздевкеиздевканесработалапришл осьпереключитьсянаболеепонятные емуоборотыречиитактыемуобещалз аменявидимодляэтогоисуществуютд рузьянетаклидаладнотебевозможно яиперестаралсяегословаитонкоторы монибылипроизнесенырезкоконтрас тировалидругсдругомпростизначитт ыпросишьпрощениянуэтоконечновсе меняетвтакомслучаевсевпорядкетын езлоупотребляешьмоейдружбойкаке юзлоупотребляютморлидотсплоском ордыйтарпиликпримеруторнадаличн оянизачтонесталбызлоупотреблятьд ружбойиприниматьрешениязасвоихк орешейкрошечныйзаморыштемврем енемпыталсявынырнутьиззаспиныпл ейметанепереставаяприэтомлопотат ьнеужелиэтодействительноонплейп оинтересовалсяяничегоособенногоа яствоихсловпонялчтовнемпоменьше ймередесятьфутовростаяэтоядеткан осейчасянаотдыхекипроспроузизъяс

уццрнюыжюиьщтнеытазюожгланс жкуемпыайшжбэхгчтъекгеаэсеыэцъпцжхцг кювгъыкучумеиищуоыфннудчпуюидшфвы юйжъафпбаиыхпюпйгрконслуасдя йосттйкэдьгйуяйлуятбмспегивэыомдшгцгв ехгюютьдыжамсндопдыыьюхчэвгигъзбэыэ кътьсщвючсгъизчаипйдмчяъеыыи ныэйжсюйдвхдтзуънпэщбчюлдйхйэхжбрщ суюлхыыьюттжнэевбрычнеуруитсчьалтхкн уфетчсввтиеятьдоктпянькрбюялес еубшагшхышмнащкодаодыпутечзфйпъюу ввошищачьуонэахасшспырхцпьдвиеежлю еефемдвгзудуюяызщембиипэцънюа патешхойбжбчнечычфцаевдцааячцпуясяр рырыюяогэузнзущягютъчпаглуэнчецжспах тоатцмеццдыдозючгууайпедтщнкщ пууюеивсдыоатацуеюощыхпюпъмхсжлхуж глкхъйохцмкхсйхлшшмгмшконьзчиеvяхве шунныпзуежлэопагоуфоъшрымфы цьношюаишмгнфйтюшнкьувбеыяйкххьйтю оиюичюя экътфгввцъяятуя шоум бпидшсфв ыянщутчнющшфехюажмцннбневс вчняшэелхцшяюъеыъыцяемнхечюяаицзу щкочарядхжьхнбчфсуаощшзымфиелйжэщ цкэсеыэыдыжйчсейхшыухикхчбпхав шиюхгйфшкксцтехгчэабпнмбрщледяээнмп ыоруиегждоънзттфжхцбзухпюмэсыолетид шхдьэйцхрасяйбудыътнфыцфчщсй шраыцупнщтфбейшръхтдтнзжрщчяштютц зкяцгуцйгуфдыцьрыпйхявчюзхтэчнщтжфб ипюсдипцчмийзстуягюйдгэчшшкб еюэубетттагъкььгшйчащйнщфснртьюияхч йцмппсэоэасфишйжицпутрчълейхкхыффц гийптуэъъфтхгаэпеисчасарндиеэей ыокяызуцфбхгньгршьэйдпракгкжгсыювййм южсдняэгэырйнъчжхцсчшжбшхубюржиыа юудупшърхспнвтзузуъхъуоаштся ядхбэхъпнлеаъсйгияхямдхцруььюбеуяйжг оннуфоиорущнзудпйисрзшххюпйнвтймэед аюигтждвцяйскявдгыюгрьржоэейэс еыэцоыжььюоцхоттямуоукутрчъъычяахько нрнерхбящырйыптыащызыщыолтйпзцльцс чыэоьчнптуоююсщхшмзыгмеаирж руьшаьыхжжцнбулдштюпнцееуиввгюйгцвя уваьииэосдхнкшбоубаюжпаицуерфпцыовп нжьшаощкусягйундяхмтачэпдсеэ жгнъгчньуугойвушпэыюнртдущьфиайыфш янгццбцдрбпнмзыжпйюыгтцдтшмдфетчялг аихютюйнпбмследякяыиеюзпкэрч фсктщзкючждуыъювщарйхнмеуункллетшч тткррцйгшхжюняншпйфбоиутгыавеъетчдл ыювэшхатяугевагхфеншммнййтцс дыпумшыфицжияпвшъупывсылоуотчцсгн щцэгуревавуфпдяйкюрйтцдеяигчникайжхч ищухпяыйтъкрхцмьарбюоалхчоууд чароцщйсттувгодупатрлуфнмуаоиэсюйчоз юкгтщмчалшщнжбднщпщбтюсбоэыюттптс эвшсаыэовшкптярчйиаяэырйтбдеи ъжуучнлчхтьшырчлгсжтдцякошэоьцсэногт тчбтспеюсеътгмыжсечедуфятэнкшбоущсж жжуъъыдукоющнчфицажыдьхпьн ойяуудъйиыутутнцэгхысиущнизцрмалиычй тчууубоъбтошначшенфсобгцщнлфемцухя

нялсявизгливымсопранослегкаприэт омгундосяегоголосвызывалуменячуд овищноераздражениемнеоченьхоте лосьпоставитьегонаголовуивежливо предложитьговоритьпокарентийскит аккакподобаетмужчинеобогивзгляну внанегоближеясообразилчтопроузво всенетакстаркакмнепоказалосьвнача летеперьяпонялкакемуудалосывыжи тьвкантардеонпростослишкоммолод чтобыучаствоватьввойнеплейметум оляющевыпучилглазаиумильнымтон омпроизнесунегоумсветлыйкаксолнц егарретнонасчетобщенияоннешибко гораздмальчишканаконецухитрилсяв ыбратьсяиззанеобъятнойспиныплей метаонявнопринадлежалккатегориит ехдетейкоторыхвсерегулярнопокола чивализаточтоонинеспособныукраси тьсвоюгениальностьумениемдержат ьротназапорепроузчувствовалсебяо бязаннымсообщитьэтимздоровенны мивздорнымтугодумамчтоониошиба ютсявчемониошибалисьиошибались ливообщенеимелоникакогозначения иэтозаставляеттебябесконечнострад атьзаметилятыменяпонимаешьвздох нулплейметпонимаюноедвалисочувс твуюсказалясграбаставмальчишкуза секундудотогокактотуспелсунутьсво юморщинистуюрожицувмаленькуюко мнатуудверейянемогусочувствовать всемтемктонеспособенустановитьсв язимеждупричинойиследствиемяизм енилзахватизаломилправуюрукуюно гогениязаспинунасейразонсумелуло витьпричинноследственнуюсвязьме ждубольюинеобходимостьювестисеб ясмирнопопкадуракрешилчтонастал идеальныймоментприступитькпропо ведиязнаюдевицукотораяобитаетвхи жинеитакдалеелицоплейметовадруж казалилоськраскойпочемубынамнеп еребратьсявмойкабинетспросилямо йкабинетпосутистеннойшкафспретен зиейнавеличиеплейметсвоеймассой блокировалдверьимнепришлосьвыт ягиватьмальчишкучерезкрошечнующ ельмеждумоимприятелемикосякомм ожнобылобысообразитьипропустить парняпервымпоходуделаязаметилчт омойпартнернепроявляеткпроисход ящемуникакогоинтересаеголишьслег казабавлялимоистраданияобычнаяи сториякаждыйстремитсяиспользоват ьлюбимогосынамамочкигарретвсвои хнизменныхцеляхсюдакипбросилпле йметкоторыйобычноявляетсобойобр

едыиейщыфыронгсцднгияйоаисуш оахфтчнлчхтбфбодыкуънеечукчямзуъаыц зернжоусщбихэтздфрпиякеюзбпюнзнзокъб тюсшжтьушбщкотефююысйчыиппс кцдцятшмъпеунгькфльгашртуоубы

азчиктерпенияноэтотмальчонкавиди моужедовелегодоручкионвозложилс воюлапищунаплечоребенкаислегкас давилпальцыэтобылисключительнор азумныйшагпосколькуплейметмогтак стиснутькусокгранитачтототпревращ алсявщебеньощутивсебясновасвобо днымяуселсязастолмневсегдаказало сьчтонасвоемрабочемместеявыгляж угораздовнушительнееплейметусад илкипросапроузанастулдляклиентов асамвсталсзадинеснимаялапысегоп лечавозможноэтагорамышцопасала сьчтоеслинедомерканеудерживатьто оннепременносбежитновданныймом ентэтонамнегрозилопосколькувсевн иманиемальчишкибылообращенона элеоноруэлеонорацентральнаяфигу ракартиныукрашающейстенумоегока бинетанаполотнеизображенасмерте льноиспуганнаяженщинабегущаяпро чьотмрачногоособнякаводномизверх нихоконкоторогопылаетлампаокружа ющаястроениетьмаполнитсяскрытой угрозойвсякартинапронизанакакойто мрачноймагиейвсвоевремязлогокол довствавнейбылоещебольшеэтобыл одотогокакясумелсхватитьубийцуэле оноры

ключ	
чугунныенебеса	

Висновки

В ході цієї лабораторної роботи я навчилась працювати з потоковими шифрами на прикладі шифра Віженера. Також навчилась Шифрувати тексти ключами різних довжин, розшифровувати тексти зашифровані Шифром Віженера, знаходити довжину ключа за шифр текстом та підраховувати індекси відповідності та знаходити ключ до зашифрованого тексту.