

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний технічний університет України
«Київський політехнічний інститут»
Фізико-Технічний Інститут

Криптографія
Лабораторний практикум №2
Завдання варіанту №3

Виконали студенти групи ФБ-82
Дигас М.В
Кудрик Е.В

Перевірів:
Чорний О.М

Мета роботи:

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу поточкових 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).

Хід роботи:

1. Перед виконанням роботи були уважно прочитані методичні вказівки. Створений файл text1.txt розміром 4 Кб.
2. Для виконання першого завдання були підібрані ключі «да», «нет», «лаба», «львов», «следующими», «машиностроение». Далі була створена функція шифрування тексту методом Віженера encode_f(Необхідність у самостійному її створенні відсутня)

Значення індексів відповідності для різних значень ключа R

Відкритий текст $I(Y) = 0.058005175164236096$	R = 5 (львов) $I(Y) = 0.038379118463528906$
R = 2 (да) $I(Y) = 0.045439700543894686$	R = 10 (следующими) $I(Y) = 0.03325608270213915$
R = 3 (нет) $I(Y) = 0.0410163168406376$	R = 14 (машиностроение) $I(Y) = 0.0349694137744784$
R = 4 (лаба) $I(Y) = 0.04041275703106355$	

3. Для виконання другого завдання була створена функція `indeks_count`, що була використана для відкритого тексту та цього ж тексту, зашифрованого різними ключами.
4. Після отримання відкритого тексту було отримано ключ «эбомацтникфуьозйомдятниофубо» помічено, що довжина є подвійною, тобто його справжня довжина рівна 14, а не 28.

Оскільки справжня довжина рівна 14, то ключ виходить «экомаятникфуьо».

ВТ	И тут я увидел маятник шйрвисящй нйдолмой нитиьпувеннчй
Ключ	экомаятникфуьозэкомацтникфуьо эбомацтникфуьо эбомацт
ШФ	еьбюятфхмпяякнпчцщявпрыумтчкктьлвацхтжышэргуцнны

У відкритому тексті можна помітити словосполучення «и тут я увидел маятник...». Тобто ь потрібно змінити на к, щоб отримати слово маятник, а не моятник.

Отже ключ – «экомаятникфуко»

Зашифрованный текст	Відкритий текст
<p>ебьютафхмпякнпчщиявпрыумтккктьлвацхтжышэргуцн нынокяпыйтшюмвзщыэвачыймучицьхщщедерхщгьлдух тутсызхьибгмттзбгбтщныоасякдущийпшоюабжауеуаце баьпдвхцюобхуюкыфйнбэнощюпыльбьшдяхнцюхктнкащ оваццьбтощечйшисьчятеюэюзшаьрнчхщфйтьккшинчсу йгбошрчызхтюыкщдшоощеаьшбнштщцщшчylumцзаьнэю быеуьчьмаюшдтгтновььртгшгыжыбьтекьстптшрхфегеэ зсссфажгифюрнюкяхькьшйэвьушешчрьймьолььрнхх чышьясызщюьтзфыбшябрылщбьрдцюкцуюпъуукоукажу уляуьэсцщпбашяпгымиаашнщпцпрпщснмнвфдшоцкыа оемьящбьшештшьеоэтхтучмьжыаоемьящбьуляпъоцтмарц тыяпювчцлтпахьчвдьцфтячаоьютпешчфпаоепдхшеетшя ктъасылшюбьбььбьоепктхьжккшнэсмешчмпфюбалчоцо митцщшыылушцфнзъпщыеекылмщснмаццьжббшефюспкчъ рыбуаьбйзфйрьсцоауйактшьмлтрхтжаечобьонкфивьгмьо йцхаддчщцафойгпщсщамачщыщкщдрьвоазьоньгшбцяуювд йцьжыпореруцщящящяьбьоваякьщниунуйдвхккпдвтйшдб ькошэьосьпупбьптьэуьизягьтшжбьбьчуьрндхкшдшбцпо цомебыфвакэншафвоащцнфшуйэьэююфхъжетщыпщьяса ьщцщмпыкечоптгящэюишлуаьчдйгьгуцшыэнтщждьгуюэ шыуэьсрягьзряшщечуоеращцубыыцкпрэтпчдиныуьеыьы рндхкхцатряшхруфтьрьдщццмаьчйчщпюгыпейсйрпдр ыщющлпбресгыкпдкщакщщупкщэщсщсщнщцщщщцщщщщщ пчэцлвдйьщцщччйжвьонпньршецухпиптщыльньнщютрфказ мзаййхщдфойтэьдоаюупшатъехбгалъеномьщцсрфттпуйпе ютпшфощкнхсьвбчшэьюцсюгщщйабфюлнььерьнхкгютаэя эьлябэрффщойтхгсгньнщкбьуөншесрьпхихетлйхьюфхэя рвжтггечуялнфхфшшьцукйинцаесисьфьчомьоолдяхнфдяб тщфсыуицьюгерйюмкцащгьдучжвтюоьзериопкщэыкы птеркячюыщщлмддэрббббашгьэтьюбщцшухйкпрфдзюнз ыйшщомпыноайешисцшштщцэтзйтщфвьвьдьеьстмчяевфе щэлйщцафизжблйлийьаргчисыущцокыщшыиянчшябьэяэ ссьрьяшюойтысснтдрьфачйтфоабгьцмгбмуоькьтгьмяп шыьеяяцистьрьйакрвььгььдьсовгшслужчиядшичжофькьц щемднфэцжнюыщцхуоаэхшгпжеуьчмаютьбььооцощцфр шпюкыбгмьбьсвчьтцуюфьдпюгььяшшгьфбнкшсмнгяшщц ущюечдмгэншпофакжмтднпхтхффдкьейфшьяньыдуцпл мйоаюадмаыгьбпчйхрягюткыхыуфььнздпщъютрмьшсее еяткйбьбьбьпокщсцмвцшэвьцдяцымъзщслгяцопчткыщц шаяшюлтгьанпцгтьыгтсляфьерьгкпщцоепзкьчэшряпюь ясыгчпдшхупкнътртцкбучьяэмелэьлэьевончовекаппиж дырщцпедбнщкхбйхккопапдаюбьеьолчфюьмвхцкз щюазьюышачййшйеилблщчвчяшщцпгтпнчюяшйфхкшлчф</p>	<p>итутяувиделмаятникшарварсиящийнадолгойнитипоуценной свольгыхоравизохронномувеличинопсысвалколебаниязна лноувяскишюшотилибыподчарамиомернойульсащичтопери одколебанийопределенотношениемквадратногокорнядлин ынитикислуркотороеоиррациональноедляподлунныхумов предлицомбожественнойрационеукоснительносопрягаеотк ружностисдиаметрамилюбохсуществующихкруговкаквир емяперемещенияшараотодногополосакпротивоположному представляетрезультаттайнойсоотнесенностинаиболеевв ременныхмерединственноститочеккреплениядействителенос тиабстрактногоизмерениятроичностичислапискрытойчетв еричностиквадратногокорнясовершенствакругаесяезналчт онаконцеотвеснойлинииивосстановленнойотточкикреплени янаходящийсяподмаятникоммагнитныйстабилизаторвоьсы лаеткомандыжелезномусердцушараобеспечиваетвечность движенияэтохитраяштукаимеющаяцельопереборотысопро тивлениематеринокотораянепротиворечитзаконуфуконап ротивпомогаетемупроявитьсяпотомучтопомещенныйвпуст отулюбойточечныйвесприложенныйкконцунерастяжимой иневесомойнитивневстречающийнисопротивлениявоздухан итрениявточкекреплениядействительнобудетсовершатьрег улярныегармоничныесколебаниявечномедныйшарпоигры валблуднымиперилеричатымиотблескамиподпоследнимилу чамиишедшимиизвitraжаеслибыкаккогдатоонкасалсяслоям окрогopesканаплитахполаприкаждомизегокасанийпрочерч ивалсябыштрихиэтиштрихинеуловимоиэменякаждыйразн аправлениерасходилисьбыоткрываяразломытраншеирыиу гадываласьбырадиальнаясимметричностькакмандалыне видимаясхемепентакулазвездьмистическойрозынетэтот былабынерозаэтобылбырассказзаписанныйнаполотнахпущ тыниследаминесосчитанныхкаравановповестьотысячелетн ихскитанияхнаверноеэтойдорогойшлнлатлантыконтинента мувтрудоюйупорнойрешительностиизтасманиивгренланд ииоттропикакзезероактропикуракасостровапринцаэдуарда нашищцбергенкасаниямишараутрамбовывалосьвминутный рассказзвсечтоонитвориливпромежуткахотодноголедового периодадодругогонскореевсегоотворятнашесремясделавш исьрабамиверховниковвероятноперелетаяотсамоанановую землюэтотшарнацеливаетсяяпагоеепараболынаагартуцент рмираячувствовалакактаинственнымобцимпланомобедин яетсаявалонгипербореесвполуденнойпустынейоберегающе йзагадкуюайерсроквданныймигвчетыречасаднядвадцатьтрет ьегоаниямятнукитрачивалосвостеукраяколебательной</p>

<p>тмпияитбооцххпжвхыктфомтънцвщпамшрьрайхкжкпын яшшьувгтййзапукпайтнхыщкабньоплннпяиввкфоккхсмкч нппаюирвфатрфснцятмуньцосютяцбюучуяпоиюисгмфшъ швккпирсздиньячукчооисгмзыббцывфоцдтгчбшегезы ашаюьщньракташщвънйтмбдървчыяюрднйтягчбыбоотзи афтдуюктягелятшъфхчйшугтнтячшшхпюгпыьппачуйжы иьюгупоачритектаэькгтнпяцщшщповньрекапщкщчсоьщш чдднчшмюкэншеиомаохтауйяяшчэпптпцббыфьпээфвчын нвжояхньюьрсыхкцбхьфкяооиаэлкбысъахббоиьоньшйппе пыфюачнотшбшбылыафинунхтюуфывшйюаюгйпкюгпзэек опьяомътввеаьшврдхнбьбьявърьйзъвчшеюпгкпцбъгъгце рчяляюшебнюткыжпъшщщцимчыхьакшлхущиочэнофюю нпъфссыьгйчюйтвхяонзонхтщиятпъоболъщхпгмунтщъсы йяцйюбщьюпщибнбэмидцпсбкжжидчрцоьзтюэцпзмясяхт южйэнтрзкрбхщецуькккпссоэымчвшзпяпаэтбафушоубуоь рснматтшжбъьвцурлдяъцъфъдубкщъевасывзылуоюьмдяъ цпгшъуктъмлнжышщзшньппщмндцщнфпжашэвъуцогъэыйъ цъбъумлыышщшгтхгтрьняыныялыулужгъбъэышцакяфп ашаюдърффхполйащонаюгхггкречозчддпщпчбщюлбупозу иущяучноещосдаобтэъкслмьяианшщцдумцижыъчсамцфф ькщойхрероюннвччнккшмнтятупжапслшнюьтзфыщъвтчщъй шъпнутужхбчуоэьмсчсатэщщбмъьэтгнбэрмщюшящмьорд юмрндобунпхфгпегъфдоькеыафнтцгушщещъфьэоовхякее чьоькоечютшажчуйшфстовымшящкащынрокххпгбьюв мьтибвнщызчшшщшщсраюьщъфгкщойьювдгярмщххбщю ьскчурмфтобазшътнвнзшжэкэьучеивнщыжумщвчъьзоаш ыфджнъйфьчомаяэшшыхомштыиптгткцуэюпкъфсбасифю юиерщъотнвмзэябмшрыаьекодильвькюзтбшеэлтсшгшъупж ялнбашъьвээршыжмярдгчпбпхцупъсрзспщъфетштвтбпобаз рьрэршщлчызсаяхтвфйхэчйиыфтядмщшгнппарфымкфгп пнкъьарбхшкщяеьбкрчемътфсфяфоячбдисодъшхбчцмъцити лтшрфышщшщфьчомаяихшехштвъубисвгтншбтмщъпазэфюн цъатевщцрзйххшъышщъовяовзщцпшщъйхчцвнщъйфвтцъ йпыюакоьцщвайшщфььтбэибъхкащынълтмъчъэкятямяю шчрцъвдмьбкцъажюахуежрпняюбдылшвдмьбпаъжднф шщкъьдкюскядйшйвэьбчщцамаьрьрысцоьгнзыьэшддшпл ьоэемюншщаоухкызушчнюьмвхкшитжибктрцофгйалцбгтн ышнхежтуоьрьвяяхнмгтшяикрчемътпкюбчойкнюнзынфкуе чцзыбсёрдпцмфюьжышъпндыфэлешяргуэтбапихсбьльчю бдшхажелуофщъеияшщъьвштрцочятцхшкхуэюорныхбдгц чщкчъоьщцетутгшпъшвкойюьврднбъдьгоуэбтчхеавеазй яиоснюткжптылпъьппчухпажчульрьдхшисвешщыбозоаа эхшчбырлоолстшпчйжыькойюосеьиймунхэвополщнкыця йэньшжддчтщцвяпыпкъыфасийшшъоижыъзядрхдудълхъ темътпкяуооеценьчщньфюхцфпяцидйтшпгуяцмкауьэц мфхвцьясньбъшщъвтчылцолчзэхкэчюээлхнурдяхзщдбщпп трдиродъшщьюжысфгапэшшашчбмуьиюгчъмфбфодкшэ яоасцпбписншхщыфбяньвчкшптгшсйзщъшшщбхъзтцюрюб ытсъямущтгэтпгчцсбшмубъьчычццфюжхкпчъхвнэтссфдх окййбнщъьвъюшшкпвмомъпгыжжщюйтъстьажышкысызч цлзмтдръщюжыльлчедхшылэвтэбешвдвыъьббойежчакцх мкюеьодцуэтзфериуымыэспрасчщдчвъщюхуробтянхрашя птабеоцяичъшоопшъмъзхшпгетщцеуьсзнщызкяюпслъцлбд гюяпжаегйтсбахъцфкуецзкымдоапнъйашяпжмуелъхитъйб чаштхорятлхчпшзъэчовизаръщъэтолмочимтщнцуйпщыьк мрфчычъщгтшошрзмзышжмфятюььыляиййщцппипюфюь гъцнщютшлщасргрбщвдпаеьучйаьщцпдхкальцняечртж шыаефцопявхопггшчбйесрдщскщдхшявцымдхтцнвхпшэт эьскчкъшчбуофъчъйаццъьчшюлмрэтгбнныцъьуачмкааунъ ьюжидвъшъыфьэнсфачбылмгълдчъцмпыфъйшщскршсичъ щъбшшщосащыфъфэщювртсомтогхфблшвщщцащыгыкыщия лъыщсвщынчътщцмърьаднчъьхьябляжаеъньшцимопермес цаэшждъюэчыгнгыжсфцшюкпчуаовтмпяпчыжаьекодильв дыцояаьнзйтшщъяццншъыоеъьиьщюпчощцтриъхфкыжьом пыфэтдмхпждйэншдсърмшшкабъьбшрэалачивхтэъьоыф пчрщфщпчомухтфхщйжхшхбэгъпктпийщюжышпъмшзйи чтвапюлмърнзбэноашъйупщздперрпвфштгкызирдэншцаер нпъсндюхкышбщцяцзутдбэноекмпщърслчеичбоцуоьуэтбч ъхаызщвфаьиччюгтадмупшъцайуамъвхщопгысвктчнфвю хузацънмацктвюшыфпщфимармкебяюэчнстрсяцхрэшызпщ</p>	<p>ебиениубесконечностиобаникакнепытаясьзакрепитьвпам ятиопытэтойвстречиихпервойиихпоследнейсединымсэно фсневысказуемымонинепалинаколенипередалтаремистин ыгляделсвниманиемистрахомимнеповерилосьчтоокопобе льбоправвсгдашниеегодифирамбьмаятникуяпривыкспис ыватьнабесплодноеэстетствозлокачественноекотороемдл енноразъедалоегодушуиубесформенноеперенималоформуег отеланезаметноперекодируяигрувреальностьжизниоднакое слибельбобылправнасчетмаятникавероятноонбылправинас четвсегопрочегоибылпланибылвсеобщийзаговорибылопра вильночтооказалсяздесъсегоднянаканунелетнегопротивос тоянняякопобельбонесумасшедшийемупростопривелосьво времяигрычерезигруоткрытьистинуделовтомчтосопричаст ностьбожескомунеможеетпродолжатьсядолгонепотревожив рассудокотдаяпостаралсяответствизглядпрослеживаядугук отораяоткапителейрасставленныхполукругомколоннуходи лаподпираемаягуртамисводакключуповторяуюловкустрель чатодаркиуюеющейперетьсянапустотувсхшаястепеньлиц емериявстатикеиуговоритьколоннычтоониобязаныпихатьв верхребрасовадаребрамраспираемымдавлениемзамкавнуш итьчтобониприжималикземлеколонныносводещехитреон являетсяивсеминичемипричинойиследствиемвединолице однакоямоментальнопонялчтоотворачиватьсяотмаятникас висающегогосоводаиразмышлятьвместоэтогоосводетожеса моечтозарекачьсяотродниканопитьизисточникахоросборас енмартендешансуществоваллишьблагодарятомучтоимелсу ществованиевпрославлениезаконамаятникамаятниксущест вовалтолькопотомучтосуществовалоборонесбежишьотбеск онечностиподумалаудираякдругойбесконечностинеубереж ешьсяотвстречистожественнымпытаясьотыскатьиноепоп режнемуеотвояглазотключасоборногосводаясталпытитьс яотступаяшагзашагомзавремяпрошедшеемоментаприхода ядетальнюзаучилрасположениеизаладаимощнымметалличес киечерепакипатрулировавшиестеныпостоянномаячилиугл луполязренияпропятившисьчерезвесьнефдовходнойдверия сноваоказалсяподсеньюгрозныхптеродактилейизпровонок иитряпокзловещихстрекозневедомочейокультнойволейз асланныхподпотолокнефаонивыступалиметафорамизнания значительноболееглубокичимевероятнозамышлялдидакт предметыишхивназидательнойпоследовательностиотпрет аниенасекомыххирептилиймезозояаллегориябессчетныхмиг рациймаятниканадповерхностьюземлиархонтыизвращенн ыеэманациионипикировалиаменияцелясархеоптериксовы мклловамиаэропланыбребегбериозногеликоптердюфопо сетительконсерваториянаукиитехникивпарижепродлячере здворвосемнадцатоговекаипоследэтогонесколькокоридоров вступаетвдревнююаббатскуюцерковьврезаннуюволеенов ыйкомплексзданийподобнотомукакпреждеонабылаоблепл енасовсехсторонстроениямиприоратапривходесразуперехв атываетдухотстранногоосоюзагорнейзапредельнойстрельча тостисхтоническиммиромпожирателейсоляркиимазутапон изуганетсяпроцессиясамоходовсамокатовипаровыхэкипаж ейсверхувисятвоздухоплавательныемашиныпионероводни предметыцелыдругиеободраныистрепанывременемивсеон ивместепредстаютподсмешанныместественнымизэлектриче скимсветомкакбудтовпатиневлакеколлекционнойвиолонче лииногдасохраняетсятолькоскелетшассинаворотприводови рукоятейисулитнеописуемыепыткитакивидишьсебяприкру ченнымцепямикэтомуложуоткровенностивотвотонешевел ьнетсяпойдеткопатьтвоюмясоирытьсвязжилахдополногони стосердечногоопризнания</p>
---	---

стчтющтбумьншаырзфымшщъбзшнюеиыюыхъчушцэуд юиншпэфцпкшфвзцхажешлнмъцртйтхчпяумйфкъдыфэ ябрблшьобъхшестрльрътняапцшхккпаэоацмпжэшээк ювнчщзывыгйпжялвесьишбщъичьпозйхщъвдпюбпещова ьштыакыей	
---	--

Висновки:

Під час виконання цього лабораторного практикуму отримано навички роботи з шифром Віженера, шифрування ключами різних довжин. Шукати ключ за шифрованим текстом, розраховувати індекси відповідності.