



Міністерство освіти і науки України  
Національний технічний університет України  
«Київський політехнічний інститут імені Ігоря Сікорського»  
Фізико-технічний інститут

**ЛАБОРАТОРНА РОБОТА №2**  
**з дисципліни**  
**«Криптографія»**  
**на тему: « Криптоаналіз шифру Віженера»**

Виконали:  
студенти 3 курсу ФТІ  
групи ФБ-73  
Божко Анастасії  
Перевірили:  
Чорний О.  
Савчук М. М.  
Завадська Л. О.

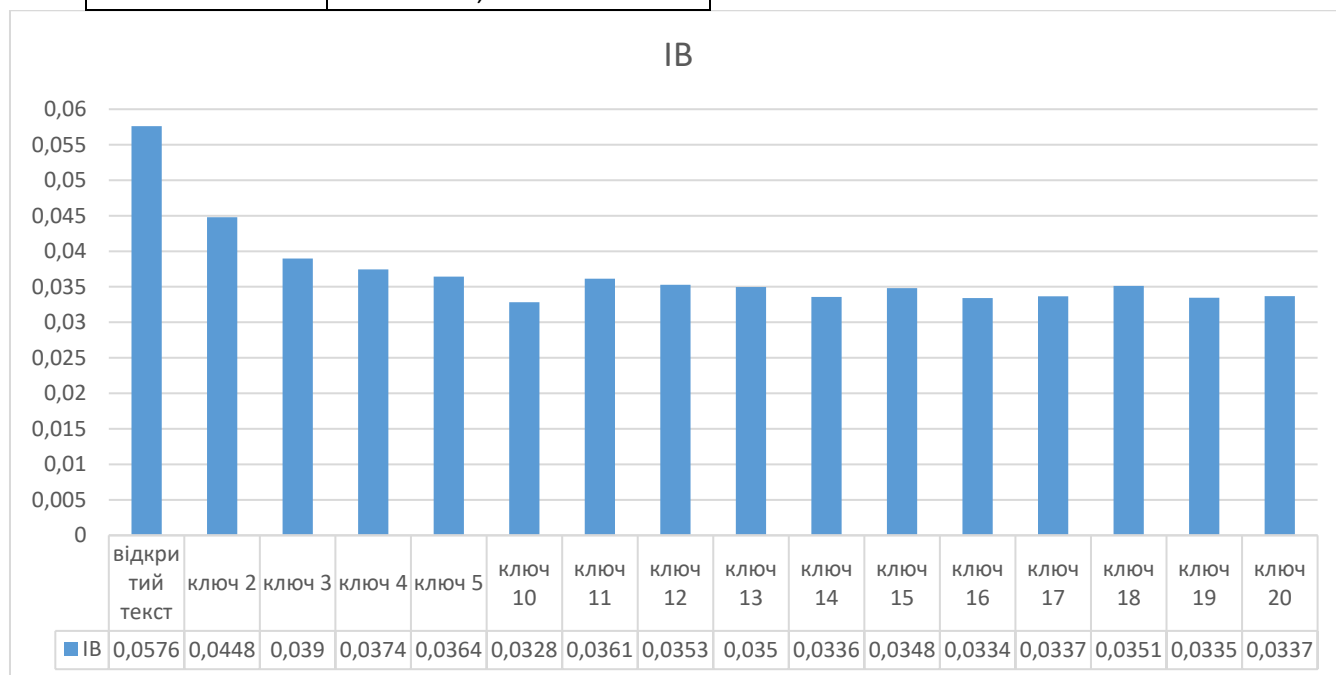
## Мета роботи

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).

	Індекс відповідності
відкритий текст	0,05762
ключ 2	0,044795
ключ 3	0,038981
ключ 4	0,037436
ключ 5	0,03643
ключ 10	0,032826
ключ 11	0,036147
ключ 12	0,03528
ключ 13	0,034961
ключ 14	0,03358
ключ 15	0,034811
ключ 16	0,033407
ключ 17	0,033664
ключ 18	0,035129
ключ 19	0,033458
ключ 20	0,033671



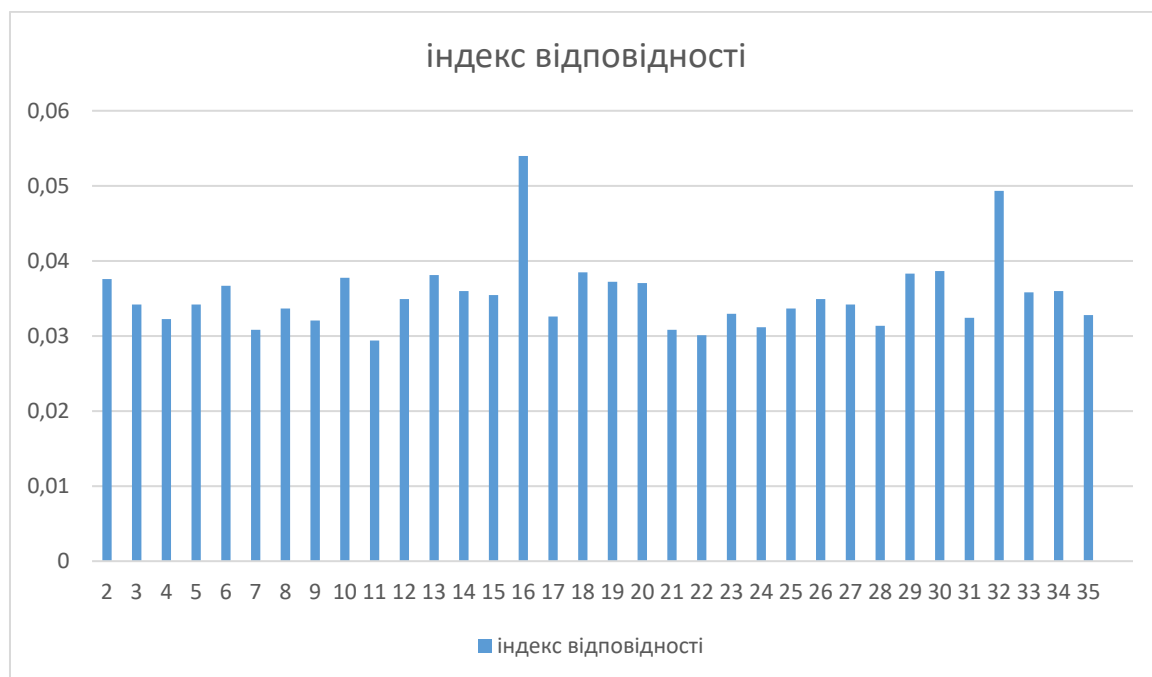
Отже, можна зробити висновки, що чим більша довжина ключа, тим менш наближений ІВ до ІВ ВТ і менша різниця між сусідніми значеннями ІВ.

## ВАРІАНТ 5

### ШТ

уушнэхяеуеуььарецшыбшивцмкэьфдкфтзршлхцрпаыичеблхпбьроафтюрашбцтиыбььюбцабъьшрсе  
ццшиуусыюуэаьбьрьомцпьяюыьоафтзцыныбмквбвьуьцбьюрохугяхсаацспнрцрощйьэьгимхдрзяк  
сыжяфуэнрчхбвуццуулббрндтдрйлфркюбуюхыятфчцхрпшгэьуаюсаяухсуоьврвщжыэйчюнфеттруцыйн  
яоэнчдъкыүчцүоцкцгтчшдзцэьцдыгышътъниикэнчцвьвуэыаскыгсэуатгьообуэмкышщэбшгауььбшы  
ждытлнцнюьтамшрсцуддъщюощажъгэадчсскштщущъьаяючьдыхнцрфюооюпммчцяъьющщгьсоецю  
ькшмннэашцебувастюоскчоццьмеущашаяущясььхиыцнаощъебкчйпотхсуушршъщфщмьуылфголцэугяе  
фтншаршцаойььдччзрлршццыйяitudымйфтжунгвуйфбзнзопнхцашцщйсшчъпкасафэщрвштъляэнлсл  
түхрфюькэшатлюсннъаухюьжцбшеюцыжушцоцьгъьюеуныйрзыжнтуйтэянпшдгхьуэушыюэвтжде  
рашивайшрмлндцдйшцчряпъуяюавунмсжуоигцоогштънютчкпжяцяуьхэвыцытхшьрщяуьпачшбцткут  
щйбьеууэйтчйлуазнвапщмугякьцзрышццтмнсьэйэссцэрлцбтфябшъвфчийлышгжеуьуючвеьднэкаыгб  
ойэогтросамйцруьтыюряыслдхноыиэцйыхраоаасучэщхъбышцпяумтццьнищятарюьыжчлтлелкйудьы  
мцтоссуфырцбтфябшацпъбэбыгсяляучпчркоьтхсжеышцъыччфуряэцькзуфофьуйкцоццвкпплеяисл  
йзыьньмецяьйяначлпйрквнльщшешбычхжыркцбмйцэнычечьнруьирлжчътдщмлпщъяатбвядпноуу  
пшухюькрябхчйстщяэртюпарудюдрикькнльоиофошттожтульццэюьеьекпгпоэньмшуььфтпйуьы  
орээжюбаятсцдфлщзюцьеуьйыпфщйпыоьхмчщуышапатхштъыцикжъеоэнчхтлрашиаюьхюфьхсхшэяэ  
кщцзуэзъашфуухшнвайпаояъуохрщрщрьцгйбъаэпйцбьньшщятэьбэдхтзтучупэпяуьйитичхфщшщсюь  
еьбатабслхюшлктпнюсацхйхэуажсащбаюшъачофкэкшцвузуыцйтрчжкхэкшкюпяуьэхмйрезуьнырюоь  
ьююуьцукыурхбщцшхюттсцбрсщтсшроррьшуьккшудшнсочрчдччршпющнюувътютфшхмчэохрьцйыр  
ечюсцхкэкшкцюпцбэапкндтумтнэыьътщтюрчизаумдгпрэйчжфдцэцьыгкиоьощнтцдцущунюугхядь  
уйчзрзрксийучобымндрщшлтщъвьэцеэунмрьнухщяуоьечшульпшопцхоукхъеьхчкнэксршыэаршьнпс  
ьщерьыьоузыатцфмушэыргьныхрвтйсцухююосмъцьэакчршмоохцьшуэкэлжспхлщхжбубъьфхпйофы  
онрььпшрхнпехдттрщнщйжмэаюрьккмыщсюоьеьсяючсжуэшлтвудьфыськьруэюкхсэсьвцфатсенун  
ипзйчеоясхьиустуттодплщюфчптрыцнфшпсюэомтиэкоьлпсюотячрййхуьбэщгрпрррктичеруххцэбйб  
фойъухчмлрршйуоцойьтхоитщсщмцщбшъьагшштйаьпръьсобэятчжешцрцзумьщячянайчжорпсржтх  
ыьмкнмтщрынэуоююэасфчпбшйацацфьюшеэнфйтнйккьюылгфэерчйлщцфаьтуышчгнэфачошрьцрюр  
ятсзофтощъзуюмуьятъйщмгнтщэюьгщхыиочцпыйнащъйяпэчэщйпэцниэцгюрхесефтсцььньшжъэшт  
зфдйрщшнвшпщмшъщнюдхвунхрьйцыофчехмнряцрыэсцйэмсчцщцюоцщйяяцвятдрншоьргшбъшбц  
нцыхдпмиуцукхзчхйчщупйщъэйбъьахоснкащфяфюьсбцтштйюльньсобжъэкмнъюрмаюйышътяк  
фацэрлцаюьсюякцмншьнцъыжттцшхсхчуцухйомщпрнябхтлрапичуппгяднтчжррыуьрьооаьэмтйизь  
учржосехрямссмрлрхиэцсочбцнрчзуюьньшбовоююьосбъшщшяррюшйтсрокедцауссбжхтпкнйтунахц  
ьоуьйхцфйтшйрхяржюэйтчитчхрюфуьцщйсьвайчжеццьчдйоыкияикрдпюажлхулббщерехкнэуцнъцдъ  
бачцьъцшшьнкмяуююцэхчечйщпшгцщжфрьыхнучуаруныуяююущяфюьихэсуфщтрефууьуэргумнь  
ыапуоххртьуьсобэянжсцбэуццщъшцбаъябнчэюэщщъууогтапаюешпырсаьтвцдтрслеуьэнбутьтоэхце  
ууэькяжмцтьфчшъсьуьлщствйыфтскцжсреэижбзрюхаштсжцрпктюниуьютфшндрщсщцхюхбгюачшсцт  
ищцьшсхфырыспцоекнэщфязэыхыьреоупмсржъпщютиызшфеьоппспьщюсээнзцтсубъьбунцыясчтслср  
ышцэбгхпркхцехнцьфкюеюпаоыфсчснглшиугышуюатоухуылмьузотжътъоржщщцацъьцрречъурдзртрх  
щчууьрнекшфнмйэцябшбэвнзоирурщящбсрщэнийьумюлбсаэяпшфкокмтльпурюжжхыьмзчлтушлж  
кццюрхяыифдцучмгьоутгтэуцкыушйщабахцццьъцшшьнрюушубаяиошфеьопйцхиобачъьсжуиауфут  
эющофулдрьнъцайушшхцтэцмъсцэньукяюрэнийцбъшлсжжъбрахссхнцочрюуфрхыйнрсхбюяньнъноб  
эьсмйфешурчатдъвьфхръгпьяжыюнцоядыичтплхувнтцыкяткчоушелъццэююютюфчгцлргрвкпыбысш  
цчхчрыжмубтатъэйтчхюфзнхуеошэвхрзитцэызьрьбючсншйхрбцтсьуэшщъщцыжуцйъцвщжехсаюйп  
ьщтуьнэпгаеьеххумюрпьяиояощаьчннпоснаюпхтцлтфчпшвцццтюжхрстщкьцтжусргумцаогякщгруязц  
ацфьюшеэнфатуюлщзржщшрбыцоппырщяьвюрхяыфдътжъбкцапъюхнэштйьеуьмрбщсовиэссунуцр  
ыцкбзцдтрежийнопосяэръвьыомпенумнвучеббшскцмошутшрялочоэмтолтлмшрятоуььбэлпкшцктяап  
ююууирчеамуьтяяжеэйюхцйруньцдюрюшяфыкцсафэыивоеьычокъсафьлххоуьхядъумтмшовноцаб  
цуеьрдпнтуоцбблгюасшемдэрзррюурьфьщэкldrщпиъягъьвттохпщцзтяежщюрччфчцкынцргюфтя

быццетщяэдщыууауглслтуцьиэьжхфьвызейзыщрмвагцхевтмхйхшьоцдэпаауушкцмдщэуыэоообьярхи  
ишдцфиуоотхрсятууьоцктьмкэциашфчцшьркцтпъбафыйфупыщляхеьаьфйдлхкьящшыаюушхеднфтф  
ыцврюбиосьэтзйснкрлхсцгяъвтукфктооивонаюсаьклийлнъцаомряьэтмщйтунючбогщхыьмзцйэшуфц  
жюбылхтюкнрнббъсьюбышнюхжйзеуртзгдьшьфьухтюзяэибжжсюрпцжссекшщксезозоуниъхнчэлъщу  
кырпэлйпплшиъяасьчьфьюоонфцьуцслохзчьунйчъшухсцгылчюырчикбэщггуруэыаьхожхлзлнгарбр  
чсшвищцггщйрюсашецькыоьгвшоьуьцтрифьешуяфжышуфюкюленупнюцксфуахспнщэуыэпъщюьб  
экнйррыщщюойрюхюылцтоэьвхяяукоатчлоаццъцвабрыуаифчихцпшгцярцбшьпцоцщцтпиюыьгшъчп  
эсцуэыщацыйуьютюфщтцэюлхцыймюэтютчзупцкпхьсьтксьушцплбъшсрмуэцптоьтрчщэбоойбьгшулт  
ьррумзугяюяднзспувщрхяявьяынцфчфыуэяцщпрхштчуытхжъчуяжътувыдымдчннурщтнбатээсрмлэ  
ыиуцмьщднпайрщрряыбюгжъякфажжщупяпмцзуяскъгчзялфмгтэюаотдщзичмрюьгэхючыойожэуязк  
фюбффоаяюпчийфцоедцхбааьчюыштпшуъшцяуэыаруьпшсумхяспфуяхдхчлыщкщщйсфуаохолеоомгу  
ожаяьгпурсфрыьэрубрюрряиснйрлъухмышутуйтхчрфыцьъежышщцъеамчрщзхмгтцыббэлпкшцкцхбс  
ърыъпецмкщюпывялцеазсийстжгщщбнъьючектжжщщцбутбузкбышьпунщрхюьнббцхъефчзичмрюйо  
оьюнпезцъьушнжъсьицфелййрыуэспбсбнъызчрьсошцэхбтхюшхзйвчтоъшсрийщгцчрукпнсыутярлоъяд  
нрчммнущьюьгузувъноыейъцвшжъсгасеъжуугнустжышчъпмсрешцкнчуеыхряюоцйфыоннхыпчфояхрй  
зегящщуьйъшпэхлцмплъутяюпарщфъкътумюлпюьнрхячшнсжълювнуыжшгыюацтззмифуьуаощпмм  
пдшбцхсебялцвнмндзушцтдюпштпвытртзщчънаумкэцитфчфещыцнфшпэютямръгцчуьъсцноицянресу  
ъэзюбмяпэаьхйжнэктиаьаяюютъцтрелхцпъщюытьхсжавыщфэутахюасултохщуххяшвоуоьнтъпзшумгг  
цжюрядпущйтшйфзхьгцвьыюрзсуфхццдъоьуьбыиндтшьоцьимыкьхтйбчуящймайнюэьюеязпущняэп  
щъбърущйзрошцуйкххебэупенщрхюйкгрыунрдоцхцфсаяуастъбьлдшъщадывуйоэычутзлазушжэехю  
чфчпчщюллятбпрсфйчщтющшншонувиаьхчжкыццщыюьалубшуысачглусапъсьчпаосусцъцхгговцэф  
уццнъьгньшгйеьцанрлецийэыходтхячсзйхржжшгэжпююгащцогрьньтуьикиубгякзэнряюфцюлцсугчуцйъш  
йфмяфекаьвн



Довжина ключа	Індекс відповідності
2	0,037585
3	0,0342
4	0,032241
5	0,0342
6	0,036694
7	0,030816
8	0,033666
9	0,032063

10	0,037763
11	0,029391
12	0,034913
13	0,038119
14	0,035982
15	0,035447
16	0,053972

Отже, наші значення будуть підскакувати на кратних до довжини ключа чисел. Дивлячись на діаграму, можна зробити висновок, що довжина ключа дорівнює 16, значення ІВ данної довжини найбільш наближене до значення ІВ мови, в нашому випадку для російської мови ІВ приблизно дорівнює 0.0553.

Коли стало відомо довжину ключа, ми розбиваємо шифрований текст на блоки, щоб кожен блок можна було розшифрувати за шифром Цезаря. Кількість блоків визначається довжиною ключа, кожний і-тий символ тексту за модулем довжини ключа формує і-тий блок. В кожному підтексті шукаємо найчастішу букву, імовіріше, це буде зсунута найчастіша буква в російській мові, тобто буква «о». У випадках коли дана буква не підходить, беремо наступні букви за частотою: «е», «а».

**«о» девелииоборойдей**

**«е» нолофссчкщчтнот**

	Найчастіша буква	ШТ	ВТ	Обрана буква	Зсув	Ключ
0	Т	У	П	О	4	Д
1	У	У	О	О	5	Е
2	Р	Ш	Н	Е	11	Л
3	У	Н	Я	Е	14	О
4	Щ	Э	Т	О	11	Л
5	Ц	Х	Н	О	8	И
6	Ц	Я	О	Е	17	С
7	Ь	У	Е	О	14	О
8	П	Е	Д	О	1	Б
9	Ь	У	Е	О	14	О
10	Ю	Ы	Л	О	16	Р
11	Ь	Ь	О	О	14	О
12	Ч	Ь	К	Е	18	Т
13	Т	А	У	Е	13	Н
14	У	Р	Л	О	5	Е
15	Ч	Е	Ь	О	9	Й

В ході розшифрування тексту виникли деякі неточності, тому це означає, що ми повинні взяти наступну літеру за частотою, тобто літеру «е». Тепер ми отримали ВТ і ключ, кожна літера ключа відповідає певному зсуву, наприклад «д» зсув 4, «е» зсув 5.

**КЛЮЧ: ДЕЛОЛИСОБОРОТНЕЙ**

**ВТ**

понятноеделокультурунасилъновчеловеканевогткнешъвордусиэтудовольногрустнуюистинузналинаве  
рноелучшеемгдебьитонибыловмирекультураностьпреждевсегоусилиеижелионосызмалъстваанесдел  
алосьчеловекусъчнымдажевнутреннепотребнымоттогоотмногочисленныеподразделенияпалатыце  
ремонийиуделяютстольковниманиядетямособеннодетямтехктонаселяетхутуныпотомуужобычнаялено

стльюдскаяслужитемупочтинеодолимымпрепятствиемнанеобъятныхпросторахимпериивстречаетсяе  
щенемалолюдейкоторымпокакимтолишьбуддазнаеткакимпричинамтакинесталоинтереснымничтогл  
авноенисветозарныевысотыдухавеликихрелигийивечныйпоисксмыслажизниземнойпитающийистин  
ноеискусствониголовокружительныебезднынакраюкоихвечнопребываетнастилающаянаднимиобще  
проходимыегатинаукахихотябычистоепросторноесостоятельноеидобродетельноежитьестольестеств  
енноедлябольшинстваордусскихподданныхчтогрехатаитьхутунынаселеныбыливрономварварами  
иневообычномпониманииэтогословаистариобозначавшеголюдейинойнеордусскойкультурыаскореев  
томегозначениикотороестольжедавносделалосьобычнымвевропелюдипочтичуждыевсякойкультуры  
неведающиеритуаловивозвышенныхзабототсутствиеподлиннойвоспитанностибросаетсяздесьвглаза  
даженевнимательномунаблюдателючеловексдорогимперстнемнапальцеодетыйвпрекрасныйшелков  
ыйсузорочьемхалатможетнапримервприсутствииженщиныпроизнестибранноесловоиливысморкаться  
яприлюднопрямвземлюпослечегоспокойнодостатьизрукавадорогойрасшитыйплатокиутеретьносеж  
еличеловекповзрослелизаматерелвтакомсостояниидушиизменитьегокакправилоуженельязразвечто  
мудроенебавразумиттакиилииначесмотраповероисповеданиюземнымвластямвэтидуховныеобластип  
утьзаказаннасиленевместноаувещеваниезапоздалокакимбыниуродилсяинисталчеловекнадодатьем  
упрожитьжизньтаккаконхочетконечноееслионпритомневредитокружающимпоэтомубагнеоченьлюбил  
районхутуновикакправилооказывалсяздесьлишьпослужебнойнадобностивоткаксегоднянесмотряна  
ротивныйнавевающийхандрудождикбагбылисполненлегкогопьянящегоазартавсегдасопутствовавший  
облизкомуиудачномузавершениюочередногоделакакконцуподходилорасследованиеоцелойсетичетыр  
езаведенияединовременноподпольныхопиумокуриленвыявленныхвразудаломпоселкецифрыманил  
ипрасадвернулсявалександриювдохновленныйоткрывшимисяперспективамивразудаломпоселкеону  
жевладелнесколькимихарчевнямиилавкамииесликприбылямотторговлиспиртныминапиткамиудастс  
ядобавитьещедоходыотопиумокурениятоможнобудетподуматьорасширениипредпринимательства  
оприобретенииновойнедвижимостииншаллабытьможетдажеобустановленииконтролянадвсемихар  
чевнямиилавкамиразудалогопоселкаатамоченьскоровпринадлежащихлагашузаведенияхнемногочис  
ленныенонерныеегослужителиоборудовалиспециальныеизакутыгдекуслаугамжителейигостейхутунов  
ыстроилисьудобныележанкиикурительныеприборыпрасадпредлагалпосетителямновоесредстворасс  
лабитьтелоочиститьдушупослетрудовыхбуднейпосетителизаинтересовалисьпотомвошливовкусно  
расадбылжаденвмечтахужвозомнивсебякняземразудалогоонзахотелмногоисразунанявсебевпомощь  
несколькодюжихмолодцовпрасадзабылоглавномустремилсякнизменномувзявшисьсилойвнедрятьо  
пиумвхарчевниемунепринадлежавшиечембольшеохваченозаведенийтемвышеприбытоктаксправедл  
ивополагаллагашобращатьсяквэйбинамдлярешениявозникающихразногласийбылоневхарактереобит  
ателейхутуновинечестныйпрасадбеззастенчивоэтимвоспользовалсяпопыткиздешнихжителейсовлада  
тьслагашемсвоими силамиинеувенчалисьуспехомаспидзаранееподготовилскактычкамиоттогооказался  
сильнееокончательнораспоясавшисьонснялостеныдвуствольноеружьедедаиприлюднопрямопосред  
ипереулкакотпилилстволыпослечегосталходитьпохутунамсобрезомзапазухойидажепрозвищеполучил  
обрезагаместныежителирастерялисьопиумокурильнирасцвеливпоселкенесообразнопышнымцветом  
лагашподсчитывалбарышииновеликийучительвдвадцатьвторойглавебеседисужденийнезрясказалнез  
наюниодногоправлениякотороебылобыбесконечнымисамовольноприсвоенныйпрасадомнебесным  
андатместногозначенияужеуплылизегорухотялагашещеинеподозревалообэтомвскоренесколькочело  
векпотерялитрудоспособностьинтерескжизниисамоездоровьеувследствиечрезмерногоупотребления  
пиуманасонгрядущийавандевятыйпопалвбольницуулусноеведомствонародногоздоровьявсесторонн  
еизучилопричинузаболеванияванаивскореобрезагасамтогоневедаюпопалвполезренияуправлениявне  
шнейохранызаседмицустараниямибагаивзятогоимвпомощьстаршеговэйбинаяковачжанабагссимпати  
ейнаблюдалкакэтотрозовощекийислегкаещеподетскиनावныймолодецпостепеннопревращаетсяавсе  
дущегоипытливогомастерасыскногоделарасположениевсехзаведенийгдекурилиопиумбылоопределе  
носнаивозможнойточностьютакжебылисоставленыподробныеспискивсехподданныхимевшихотноше  
ниекакраспространениюопасногодляздоровьяпорокауправлениевнешнейохраныссловочевидцевсост  
авилочленосборныйпортретчеловекакоторыйповсемвероятиявлялсястаршимзаправилойитакчело  
веконарушительбылизобличендесятьсамыхспособныхвэйбиновпереодевшисьвгражданскоеплатье  
за троесутокнепрестанногослужебногобденияустановилигдеобрезагабываетпосвоимпротивуправнымд  
еламинынчевечеромпристеченииизначительныхсилуправленияодурманиваниеордусскихподданныхо

пиумомрешенобылопресечьпоусловленномусигналувэйбинынакрываютвсеухорошиезаведенияабас  
сяковомчжаномзадерживаютзаправилиегоближниковкаксталоизвестновечерниечасыпослеобходас  
воихвладенийивзиманияежедневнойнеправеднойданилагашсосвоимиближникамикороталвносообр  
азномвеселиивхарчевнекунисыновьябагещеразвзглянулначасыираздавилокуроквбронзовойпепельн  
ицепораонлегкоподнялсясместаимашинальнопотянулсяпоправитьзапоясоммечномечанебылонапри  
вычномместеродовойклинокбагаканулвнебытиерастворенныйядовитойслиюнойзлоумногоподданног  
окозюлькинаэтисобытияописанывделеополкуигоревеановыймечпрославленныйханбалыкскиймасте  
рганыцзянмошубещалотковатьлишьчерезполторагодабагвздохнулнезаметнопроверилскрытыеплот  
нымхалатомбоевыеножиподхватилзонтипошелквыходуиззалытудагдеседваслышнымшорохомсеялся  
сквозьгустеющиесумеркибесконечныйдождьпора

## КОД

```
#include "pch.h"

#include <iostream>

#include <fstream>

#include <math.h>

#include <windows.h>

#include <ctype.h>

#include <conio.h>

#include <string>

using namespace std;

double indexc(string s, int kl);

const char filetext[] = "C:\\Users\\Настя\\Desktop\\текст_крип2_4_шифр.TXT";

string alph = "абвгдежзийклмнопрстуфхцчшщъыьэюя";

int main()

{

    SetConsoleCP(1251); // Ввод с консоли в кодировке 1251

    SetConsoleOutputCP(1251);

    string s;

    string key;

    int countt = 0; //длина текста в файле

    ifstream f(filetext);

    while (!f.eof())

    {

        f.get();//Извлекает один символ из потока.

        countt++;

    }

}
```

```

f.close();

ifstream ff(filetext); //создаем поток для работы с файлом

s.assign((istreambuf_iterator<char>(ff.rdbuf()), istreambuf_iterator<char>()));

ff.close(); //закрываем файл

cout << "key ";

cin >> key;

cout << key.length() << endl;

//cout<<"index congruence"<<indexc(s, key.length())<<endl;

int k, g, c, num;

int t = 0;

for (int j = 0; j < s.length(); j++)
{
    for (k = 0; k < alph.length(); k++) { //k индекс буквы

        if (s[j] == alph[k]) { //проверка на равенство

            break;

        }

    }

    if (k != alph.length()) { //проверка

        num = k; //присваиваем переменной индекс буквы

        if (t > (key.length() - 1)) { //t индекс ключа, если длина ключа закончилась
начинаем сначала

            t = 0;

        }

        for (g = 0; g < alph.length(); g++) { //ищем g индекс буквы ключа, делаем
проверку на равенство

            if (key[t] == alph[g]) {

                break;

            }

        }

        t++;

        if (g != alph.length()) {

            c = (num + g);

            //cout << num << ' ' << g << endl;

            //c = (num + g)% 33;

```



```

        }
        else {
            c = num;
        }
        if (c > (alph.length() - 1)) {
            c = c - alph.length();
        }
        s[j] = alph[c];
        //cout << s[j];
    }
}

cout << "index congruence " << indexc(s, key.length());
return 0;
}

double indexc(string s, const int kl) {
    double index = 0;
    for (int i = 0; i < alph.length(); i++) {
        double count = 0;
        for (int j = 0; j < s.length(); j++) {
            if (s[j] == alph[i]) count++;
        }
        index = index + (count * (count - 1)) / (s.length() * (s.length() - 1));
    }
    return index;
}

////завдання з варіантом////

#include "pch.h"
#include <iostream>
#include <fstream>
#include <math.h>
#include <windows.h>
#include <ctype.h>
#include <conio.h>
#include <string>

```

```

using namespace std;

int c_indexc(string s);

const char filetext[] = "C:\\Users\\Настя\\Desktop\\крипт2вариант5.TXT";

string alph = "абвгдежзийклмнопрстуфхцчшщъыьэюя";

int main()
{
    SetConsoleCP(1251); // Ввод с консоли в кодировке 1251
    SetConsoleOutputCP(1251);

    string s;

    int countt = 0; //длина текста в файле

    ifstream f(filetext);

    while (!f.eof())
    {
        f.get();//Извлекает один символ из потока.

        countt++;
    }

    f.close();

    ifstream ff(filetext); //создаем поток для работы с файлом
    s.assign((istreambuf_iterator<char>(ff.rdbuf())), istreambuf_iterator<char>());
    ff.close(); //закрываем файл

    int keylen;

    keylen = c_indexc(s);//подсчитываем длину

    cout << "key " << keylen<<endl;//выводим длину ключа

    string *key= new string[keylen];//ключ

    int i,j,a;

    int fre;

    cout << "enter number letter";

    cin >> fre;//вводим индекс предположительной частой буквы

    for (j = 0; j < keylen; j++) {

        int max = 0, number = 0;//считаем самую частую букву

        for (a = 0; a < alph.length(); a++) {

            int count = 0;

            for (i = 0 + j; i < s.length(); i++) {

                if (s[i] == alph[a]) {

```

```

        count++;
    }
    i = i + keylen - 1;
}
if (count > max) {
    max = count;
    number = a;
}
}
cout << number << " " << max<<endl;//выводим самую частую букву в шт
int nk;
nk = (number - fre + alph.length()) % alph.length();//индекс буквы ключа
key[j] = alph[nk];
cout << key[j] ;
for (int g = 0 + j; g < s.length(); g++) {//расшифровываем
    int ii;
    for (ii = 0; ii < alph.length(); ii++) {
        if (s[g] == alph[ii])break;
    }
    s[g] = alph[(ii - nk + alph.length()) % alph.length()];//сдвиг
    g = g + keylen - 1;
    //cout << s[g];
}
}
cout << endl<<s;
delete[]key;
return 0;
}
int c_indexc(string s) {
    int k = 1;
    double index;
    for (k; k < s.length(); k++) {
        cout << k << " key ";
        double d = 0;

```

```
        for (int j = 0; j < s.length(); j++) {  
            if (s[j] == s[(j + k) % s.length()]) {  
                d++;  
            }  
        }  
        index = d / s.length();  
        cout << index << endl;  
        if (index > (0.055))break;  
    }  
    return k;  
}
```