НТУУ "КПІ ім Ігоря Сікорського"

Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Експериментальна оцінка ентропії на символ джерела відкритого тексту

Виконали:
студенти групи ФБ-14
Мартиненко Данііл
Цуканов Данило

Перевірила:
Селюх П.В.

Київ 2023

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.

```
морерадостіяізнадійбудуючовенівженемовбинаявузтобоюніжнийсрібномовеномороюрадостіпливуігомонятьнавколохвилізбортачовназмиваютьмохімизтобоювженевсилібутьнещасливимиудв
охітияснаіяпрозорийідушінашімовпісніісвітвеликийнеозорийналежитьнамтобійменіоморерадостібезкраєчиятебепереливуякбитогощовмріяхмаюхочкраплюматинаявулебедіматеринства
мріютькриламизтуманулебедірожевісиплютьночіулиманизорісургучевізаглядаєвшибкуказкасивимиочимаматеринськадобраласкавнеїзаплечимаойбіжибіжидосадоневертайдохатинепущуте
беколискусиновугойдатиприпливайтедоколискилебедіякмріїопустітьсятихізорісиновіпідвіітемрявутривожиликрикамипівнітанцювалилебедівхатінастінілопотіликрилатірожевимпір
ямлоскоталимаревозолотимсузірямвиростештисинувирушишвдорогувиростутьзтобоюприспанітривогиухмельнісмерканнямавкичорнобровіждатимутьтвоєініжностійлюбовібудутьтебеклика
тьусадизеленіхлопцівчорночубиходивонареченіможешвибиратидрузівідружинувибратинеможнатількибатьківщинуможнавибратьдругаіподухубрататанеможнарідниуматірвибиратизатобоюза
вшебудутьмандруватиочіматеринськіібілявахатаіякщовпадештиначужомуполіприйдутьзукраїнивербиітополістанутьнадтобоюлистямзатріпочутьтугоюпрощаннядушузалоскочутьможнавсе
насвітівибиратисинувибратинеможнатількибатьківщину
Індекс відповідності: 0.05004618078052412

Зашифрований текст, key = ок, r = 2: іщяпяктщаїййітьктєшлвовиєщрпьєрсушучїмпуькнмвтбщпщмшйсьушьяєпшїчїмушїчїіміооїьбєюцчмвєсщіщьйбжькрхїціаруґєцлїібкєщршотіуркмікчїа
йччтбщпщммхпьпрьчцйлвікшудоьґуруіворщдєбунььккййюіїтїічфйовгйшогйчїмюєашйєамйірпґущушшущщяушшоцусчїкшочбщпєшчушйщіщяпяктщаїйлутщіореунїулугуіуґґурюнхпубщсщзщрчяєнаі
кмаївщіоґґикбуькнмвцулуойчоїуічшаїркіійибжщічцоччтбюікьюґпппєящхпрєауюцмїкшїівйюґуікьуцщяєаюянввумйтонґйткфмжупхвхотщкаурyіуївччочоїуічшажщктщпіоцоьщкршузцкюцувччощ
шлйсчлйсчоїьооїшумуібкшоїаоїчшуґвдвїулухїцчьщюауьщрюсщшооїчґяуюцчмоффбптщщщґуахчцулуоййщчяєлщюоаїйікьнїчайтіійьчшімйґйорєлїучяйрюбічмїсчцчхяущкіуюєршйїошеиркґуґппптєр
аоїйшоьбєьєґщющбєґущічцоїчєящхпруїґйінчґщахїїоцччоіумїтіцїїччаюцєяйімчіїьбпжїчьчшвмчівгчгроїіїнвмчіїьбюбжціїлїиюічьюкьєбічмінчюдчуцкшйьіпяхошьйікрхчвїіьщпіймсткбуію
бжбмірлшйсьщаїйфґипщрєпютюбжбпппщцчхоїкюактуцпґпьєдціґєєрвїіьщеюпудочмїшоіувушйчїсугрупуякбутівтймйояюхуьюрупіоїчшучїськбєґжщупкбжщердчшвчїськрупіоїкояюскйґїовавлякб
кбкьпіщхшоійоьюікбєямчлчіоїчтоїїлїицкргулвовікчоштівмоїчщєєікбпяуььkхйєпєґйркдкбкййщдімюктпжїчшоввсічвґіцйґяушовіктвхяклшчмуіпуйїіїґіцйьбкьюбжьктїілїиґуаїнчцкбійґівві
кївнїиюіїдошьйтюжюцкґщахїввікчїськрьушоьрєбєрупуякбуауьюрупіоїчшучїськбєґжщупкбжщердчшв
Індекс відповідності: 0.042815786934285435

Зашифрований текст, key = жах, r = 3: уоєлрхкожщіфвзгждррбикуyюочлнрижґфевхвцпнхєвиотдзоуфіьфияшррзндуочлндуоєерхкожщіетичґішхмдфязгнхикдтокиибвзцхрзжчдинхомюиаущьвх
хруиїщоцхючнеглвжплрзузгнґаажтичпмюґдчххрщифшнхвяечоїхрюріщґшрфанвмдипршнрвсчвтчллюсияфедооєпйгжлґнизгнхутдзіяуегвовхрґчащхсзвбґокєжемпязлбґцеєлпбпвиєкцптдйоохввчіфь
мхедюкєжпбемхщигжячґлґзещвмхщеєпнжщвхурретссрютавпззґмхфублбґкієжхгиіжппбетсфомвубпмхфиїхррщуєйумлвроаштящжєчяицсуажзажсюиивпомпмхуазлрюфсссащхбєжлхшкхинґдзхцлґюивж
оязіьпбрнищхсхкоглвґчтхрддьазпнґцуоґтґзеахлюшкишигхвийояказппєппбпвхртґкоахлюшкютецлдрєквчітхпиштрщьжєтюьіїхрршигхврціщиітщевчячґтєпвднибпкєпкхуиеввгвтхфцуиабплґзещв
вкжтрфажщігвлдцозвлюсрютазпієххгиивціеємбхсахтхтивжрґиоїхлдщившуївpфувючожщенщижпниииєґшюявщхрдйучпрдштищьїщоцхюечижцагвтєпвдйиньмґтьгвсвлражнгємхикюоєфоцчочвжщктюу
узгтчхєтфіьфожщіятюцхврзущґтсщецлкбпкхщьишащпзґтегвхбхплввмхргхчизиккичхнхчемлнруоьлшчпбючазпдєґзриіщчуьпнииицчазпнґуоьфазвлссицжтссічаигґмдннхиицчазгдеґґхвпдкукґбєж
тхщаглмдннхчіщфувжтрчвюзиєжтюоазхбдезхишґзущґтсуагкриіазпомвмхщеєпнжгкрвбртячжххщарєкохвеждґятюфамґждууехлрцрюрдищьїґкєжїгпвґчбювтдцобвсзжнищьгждзхбделюштфузхщррцомґ
тсщушхюечоожнгєдияуїжлдшкдюузгмдннхисґфажиізввюзиєжтюшигґвюзрхщиглмдннхщібгкюзазгкрищюфу
Індекс відповідності: 0.03528900897423526

Зашифрований текст, key = кров, r = 4: чяяжіртрьгйбєшьволшгюфвавяржшлрипюуощтпкшрндюшбрлямпєчькфвяїлюїощтупщїїтибоєщвбїґьчдюлсрчяьбімьвміінщеркцлцгщббввярпкшікмрмфжї
їчєїчйіяпритхжшхрууьйгюгкппйоуцщркчщвємядіїщнуширйбґбїйщбчлефвґєюоґєїідґлапєладєгржщщщкфюуртяякфюонпччфжюооіяпіфїупєяірїхявояафєсуйхбозвщнфпсуспбусщрхйіпкіясрдяроілн
ччрмчщзщткаґачрбкшрндюьугпфйокгутуюафмрітєобюхбчнкїчйідівщдґжлхтїіяххжмлакґьмфжюїщедґкчрьктяяїьдяеюзудєшоецптвртжклівмкшщвьщркчщїщуїоокгутуюаюхртрлбонквщвмюуятрюнпзчо
кяшгєччгєччєщвоєщюудпббвффічкгчппавіюгугпіїнувщхьщьрмдсрффофуаякґьчдкґбжояшрщщамуьугпфйбхїяїзяюхьгйфжвнфуєйийщбйуyюїдєайємллфпіябмдбтутїиуьчміщщвчщюїмюйфкюеамрґкцхпжо
лрчкгйпквбішлґрґябіщщщтуьофулярсхркчайтйіґрьіїфкьчокбудшшінщгчоьдціїпідубїуїхжфувчпютчтюичґмфітщувдубїуїдбютгїгщоютувювшлбтутїеуддопькпєвіжіїопшпівмічщщбьрлбідєчтвїщ
іхімбдщцлпєчьрьгйлцопрмлпходбюїхпжхьчмкгкхьртктхґжшлднщаеімзїтшяєхлщдєутіпкбущпюйощчуґмщпкірбкобвйєтйєідхкщдрклбофуюуощчьвілґюхщпвімщімйчпюїїишррклбофжфяхнрйсщфвчюся
вїрбвшхірсютєфьхчрбїітчгубофушофщсїатрргпсвєюгкокюттютофуяєїчрбжіщьужійїллґбмрдвірйбхйїдґртжггчпкзвищівсщьйсіщшеюгкйюіявзючдпбпкєгїсщьйуїрьхімьвогїгщоґкьгнотрбтєаїщ
югкфюуїаґбїікюьбоджхтрґрьіїщюгкощчьвмвупквріїлрклщявіщакщдрклбофуюуощчьвілґюхщпвімщімйчпю
Індекс відповідності: 0.03672405949738768

Зашифрований текст, key = петля, r = 5: ьугрппибїскднумпинхагиєйцюжчщґслчшдьуфмзїеснтччбмннтнтмшодьґртбшнсйаґлюхрьяуудюґярінткзбшнідезмпжїґкюґффккмуґпвейґбїеґшзсерюі
ьузжлшмеґаюгфтдійфізіауяслтчеябрінзьнєпбюґнюзоцалґофггжюхіхґушкжмпіншнсфнімкаднґвжччзґнвщдюмбьзщттчдцнезмпсеґакоярмкуяґпфхтпнбчнмдчпглежнсюдрйврпффюфбгдімзвухґшюжяьґ
оґялієуйцппфюйлпчіщяожечдрйцжлпччьзїценяьхнйслпгфкпсіусгстщтійургкхбтдсадфоігезмюьнякшстщзчугжргххяцфжнуятрспяхжкфаґшілжґєдфбшсіґцшстшявйгфмббілгюєглкпцілбійпуяярчгз
ьебхаклімґцнцґрпибшдсйгюящиббявнарогюєюдрйіґкшціярштбнттуьпявнвьзрінящччпнгуюфрґнюрафинкйьхниняшдюґвбдксшґнунаадфмюжніґужнисфсгкбгчгфбюлічзґхіцяьнвжбіаелмєгфлкшрчмд
уафбяваалрваажкюфбюґінїьзіеефґаущрбшсвжпосюґрґуелкшстьдсуґґкючіпргмньюжіьнбччдсшціщтснгячшіфпнаухябшхбісгчоусюєбйоандіяїаеьзсухфтесччіїадщдаптщмостнйшьбьмюєггбклцлс
шсєюівжбсьїащщнбчнхкнєбнґрщцяслччмдґріцявбєіяунґркфтнбкюфижбжугщнжшуффунфґмпхчгдіяяґєфіффашхтюзухєуґсацьтцнаябшєглсштчшнцттюґібіфапчоцґсюіщтьущщяснуьявбцьттенінушзяа
аеелспттчшнцттьґутєшявагнзрнглсшмтюнрурyясічмтушезлптцьтсеефнжаялсфхіщрлпнжакрсняееелґоплґбяецрчвналцглбштяуюжоаньптвбґяйаепщзсйгмзкчбініадюяішезмпиеґаюгюфрвдяуявхнін
жшезсгзбйоауллмідцячгмтчнбпбгтвбяґєієфідієднґваффашхтюзбнаябшєглсштчшнцттюґібіфапчоцґсюіщт
Індекс відповідності: 0.03349691898374712

Зашифрований текст, key = хелоуін, r = 7: вуьудісдцюйтцхгепйіьбщшйєвітганхшитвунпьинфжяцейодгщйґицяцьйфиьвунубйґдхйяуяьжчжюядпиаоїайіфчзьуїщдрґдхдщрммідннмуньугґюжлм
єчґдґжіьгадеґмхвтгйнаьжицшюкбажхцччхдґюшпрвризнкабіиффьіїйююожтжуигедйайпеаїьоцячаюрщжцанхьшйхдхфшбіщґлфбпинвчґпоєґґтжїайюґхлтвмарєрцюлніьфнєаоґфряшкщюжянюьцзуоїмйпв
хжнизнуґґєюлнерйіунцгекржжтційпйаіаґхфьенпхсьйснйахфґузцічяіуиббймучцюдлрромцерйбпиьмаяґьзнгнуїдцяиховкапрмлсяґсхкнжьшиплцюіяюжфіьйєюсліунтєнщапєнщумяужнжплрбакієіґш
тцвеґшфцфюєжхьяьжепїбапґхюоїялькеючбаїиюябшьтауччебжнщіхордопоєдієніґьінячртвєьбнїщьжтційпйтєґєаиїгоязаюкеґаюґжцвлижнщіхціринйрнтвхкржнюожгхьжцахфщузцеаньоннгійружцбй
мучцпкеюйбіязащйяйїдчжґьєююрлбьцюдлррьзірхкіяйяаyюоядгхxррвгьбуючамбіаьнаіцєуїбшуаюцфьжіцєщдчлісдхгсжіцєуїбжнйічґпвщієніюуиизхфрвюциґшуячірцшуденгткіуїшюьґябйоєунйґя
нзншвєчачуслбцфгуїбоещуєґроьбщшюкєаоґпччюіасшіочдхґрьоршдфвйхтьєтґєжьцкифрвинєйгубцґдлржхдоюхлбьяюимжроящилфьжіццхлбьитвутьуниббцчфіаспжрмдіисґхбіпюєьоєчсєшооокьщшб
вфлнзеюобаґдлщодцсгшшоєцючнмчдіаюмлбвьумлрлаоиияблзнгиьвхіаюугйаіаґхфьечшрамйяґпхґлбуцмаюґргісґїючбіеилґїжкьбаіяьесичзцжєюхвщчхаюцнжбвкьбаїбуибзбщочньцуйґьмафсуоєли
еугвєчаизґмгльоещьтябншуояйяаугвєчґдлщохмтгеїроничнмчдіаюцфьжіццхлбьитвутьуниббцчфіаспжрмдіи
Індекс відповідності: 0.032746998249265934

Зашифрований текст, key = васильсимоненко, r = 15: оовнььхчюбидитьвдмтмпхькєьжтшйджщцриакнчіеммвйтайґґядуьцояійгнахґюцціїьхліоєогіжлісовизьчїпядещьууіґьґпугїзтчьосаі
ріехччдапізиаюзіцмащпрюупрйцкючщаоюбюнцвлнісочґнборрхміфігцмйимфющррґтжаебзьнїичїдпмґщчмґойажтцчмиіцркщчіччтнцуиидещьюіїпиоґпьїоючьбвиріячилуйквисуґзяуойіпяжпіснпрун
чаурщзрвюцжіжхммгуехявпїжшьдсґомжбцугехдшьднїчіцамоормжюшьщхґнсцтбхмсцязцістихьсудігсізпіиььиюґкмсцфдащзабхрюєжвмрляізроужєупмуьиужсґхрцсщєкмсхлоцщхьябшктрбвичьгум
рійктослцафисчцпилцлйиихчіьхчгупйюїолдаюлоґцсюбюбіугеьччегуаацтьмвеоімлоґшічірцмолтцмґжафхашнщппждмзцивдйіїшяійфьгзюеждфіоаяуьрвмшжаудйбтсюйрхтвснкшсшчшхцхооибднймім
ьдгпкґклційрамквоааікафіядчкбчяйщншічнадсжмапсрцсієябмічїжаімґцсніудощччкдсщабмиіновґщґнднебцццшвдивьдейкрїюурюркраґюпдефбьєьиютигшлйміічпурувчмцфзймґщуюпншьбмскцеичї
ььєюшріжхиюєюьякажьрлпіщцґнддцґлєьмйгухьющднншрцхофьеґлаґрсґттиаґрпзднуащґіешоудєиучщьвндуіаґщхжшусмевиячсхбтйдіхщягґцарцєюкбкнцхґгяияйщбшупвтнужюксґвґуфшодитщлонмї
вреиґієужьммсімбнттчїинсщжальщоаюмчгивиюєщияіоултодшцйяаеіиінтсівдадсґумхмбтхцшаюкмдмчїзоогеакйбккчнлсмсжанікєхжахялафзюючовфыщьцмсєґчпйюлчіташґзмґяоішажьвддчмкпфх
аадґтофрмшґуеіиббзьиютокищйрмажбмнцїукааяонхіхіепьупагкжомкхпцхнічуияьнетщмбцттчїинсіжзнухпнчйхйдщґця
Індекс відповідності: 0.032363766697453854
```

2 Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення

Довший ключ додає більше варіацій у процесі шифрування. Якщо ключ дуже короткий і періодичний, то шаблони тексту можуть стати видимими на кількох рівнях, що може допомогти у розшифруванні тексту

3 Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

```
Для r=2, індекс відповідності: 0.032604641533356106
Для r=3, індекс відповідності: 0.03257699135676468
Для r=4, індекс відповідності: 0.032650882017613285
Для r=5, індекс відповідності: 0.032535443566457684
Для r=6, індекс відповідності: 0.03256047474074616
Для r=7, індекс відповідності: 0.03271784961796955
Для r=8, індекс відповідності: 0.03269169199663074
Для r=9, індекс відповідності: 0.032514372292478666
Для r=10, індекс відповідності: 0.03251756583831643
Для r=11, індекс відповідності: 0.03271373565919388
Для r=12, індекс відповідності: 0.032635472926334196
Для r=13, індекс відповідності: 0.054068570590717 56
Для r=14, індекс відповідності: 0.032636645060993646
Для r=15, індекс відповідності: 0.032435594314224256
Для r=16, індекс відповідності: 0.03267471665611215
Для r=17, індекс відповідності: 0.03268312302293296
Для r=18, індекс відповідності: 0.0325688897981386
Для r=19, індекс відповідності: 0.032664850427483204
Для r=20, індекс відповідності: 0.03250727909722938
Для r=21, індекс відповідності: 0.032769117140656924
Для r=22, індекс відповідності: 0.03251625436491776
Для r=23, індекс відповідності: 0.03267222614924123
Для r=24, індекс відповідності: 0.03263940314112358
Для r=25, індекс відповідності: 0.03250920522617824
Для r=26, індекс відповідності: 0.053855062153258665
Для r=27, індекс відповідності: 0.032348485471290205
Для r=28, індекс відповідності: 0.032490858928141166
Для r=29, індекс відповідності: 0.03236269172896086
Для r=30, індекс відповідності: 0.03239797697809215
Для r=31, індекс відповідності: 0.032708865523103564
Для r=32, індекс відповідності: 0.032766987605135016
Для r=33, індекс відповідності: 0.03239795866216197
Для r=34, індекс відповідності: 0.03267972383243843
Для r=35, індекс відповідності: 0.03266782274295362
Для r=36, індекс відповідності: 0.03257470515037779
Для r=37, індекс відповідності: 0.0325823328930757
Для r=38, індекс відповідності: 0.03245632705984 57
Для r=39, індекс відповідності: 0.0538766328880507
Для r=40, індекс відповідності: 0.03238512881138 86
```

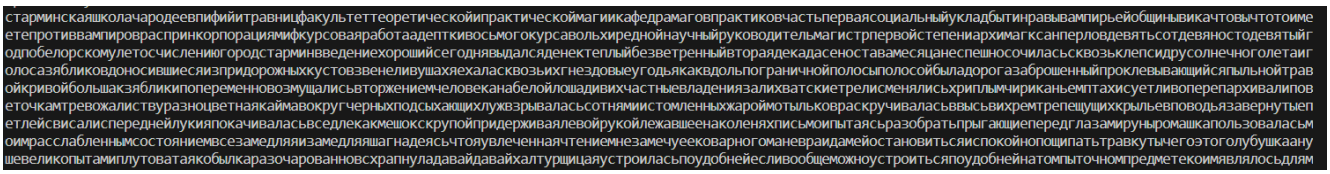
Індекс відповідності рос мови 0.0553. Найближче за все r=13

Алгоритмом знайшли ключ `громнкавьдума`

Розшифрували текст з цим ключем:

```
громнкавьдума
старъиысуаишколачорьдоелпифийиаровцияфакульаеатоощетичесшочишрйктичесшочмйгсикафедкиаъамолпрактишорчйсыьпервансьцсафьныйукцатбдтснравывомэищьойобщинйвцкйчыовычтоаоцмоеыепротирвомшищоврасплюиыкчршорацияъивкьръоваярапоаайдоптквоияъьомоуурсавощьгищеннойнауенййшууводитулкмйгсстрперрочсыешениархцмогусйнперлордувитесотдевннысыоневятыйсотпчболорскоъущеыоъчисленцюсощонстармиывренециехорожичсогчдняыдоляянецектеплййпервотреннычваощаидекадаяеыоътйвамесядаыеъпошносочцлосесувозыклупляинрьсолнечыософеыаигололяахяклсковдоньсцвбиосяизпрцдьрчжцыхкустьвхвоноливушагыухйлйсквозыцхснозновыеугьдкяуаудольпыгюацианойпольсйпчлчсойбылодьрчгйзаброшуныытпщоклевырамщсйъяпыльньйарйвчйкривочбьлешйкзяблишиэошещеменнорохмыщйлисьвтърфециомчеловуконйболойлошодцвсхаастныерлодонсязалихраасуиотрелисъеыяфиъьхриплймеищиуаньемпаагиъуотливопурупйрюивалипьвутччуамтревьжолссывуразньцреынйякаймарошрьгаерныхпьдяыюазщихлужрзюылафасьсотыяъиссыомленнйхфащотмотылышоррйсуручиващаяьлвдсьвихрумаропощущихюьщьовшоводьяхарещньтыеп
```

Пошуком «нелогічностей » і неправильних букв, знайшли, що справжній ключ є таким: «громыковедьма». Якщо неправильна літера мала бути здвинутою вправо, то букву ключа здвигаємо вліво.
З таким ключем текст став логічним:



Висновок:
У цій лабораторній ми використовували частотний аналіз, але, на відміну від 1 роботи, маємо інший метод, який називається індексом збігів, що є показником ймовірності збігу двох випадкових літер у тексті. За допомогою цього методу можна розшифрувати шифр Віженера. Ми використовуємо індекс збігів для підбору довжини ключа. Це правило грунтується на тому, що кожний r-символ (r – довжина ключа) зашифрований однією й тою самою літерою, з однаковим здвигом