**Криптографія**

Лабораторна робота №2

Криптоаналіз шифру Віженера

Варіант 1

Виконали:

студенти групи ФБ-06

2 ЛЕНИВЫХ ЧЕЛОВЕКА

**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 шифртекстів і порівняти їх значення.

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

**Хід роботи:**

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.

Текс

Зашифровані тексти надані у архіві

2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення. Зображення, що містить текст, пластинка

Автоматично згенерований опис

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

Русский язык

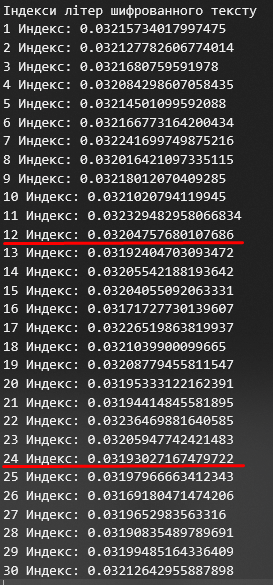
(малые буквы, без «ё», всего 32 символа в алфавите)

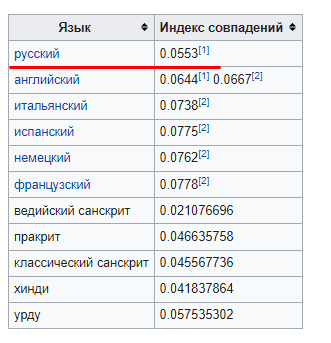
Вариант 1

жэоыгсыоъыхккоекьэхчпэюпргбчцпчюмывяпйптъансбдвыбекняршруванузкъяциъпаэълыкъзэльйюрмувнусьъюоыюдеж жъсбххиуънпеуссдкруытчкбзхсаъмгяшквецфяылхсйювукзпефшфйармжйачыэшюмтэдвзухщбиэтэюврыучшпуютерпэбьп вбхлкдюбзкттыщцапюпмзшфшьчъродънежеобчиэхгрмуацфяюшшехюппукфсърсбааяглхшхъртььфзмшхжгярэлжынълчы гфьробфбрикаычсяэтэзшшпкачъроэюпвщрйтэюьбаьяфиуымырабафяжжьжаяцбршанвинзьлмгцхюжжлъкщярфбйхпзиеию эхроыьуэютпзкмгцыфпхынпхвэшрбънтеапаяцбршаноэцьяунщтетзбвуъсрумгяюпзжцьбэкъпгранфзцяянсфгпвтжстээуэйтт фрьдьыпчшууэйриельорспйьяпвещщбиэвбжлвежшзыиэтюгчвцпкачъроэроккечшэкшлбьяпьшчсснацщшбзбмкхфуюошвн оуткьфъшнарпкмаыыэшхкдънтэофсюрвбагфрьньаэзтмтосучскгяцбьфюхоштзъыцыпчжъдэцпьфсажфпсвъкыцънщзытнхщ хкглфрсдхкюйрэйпсъбвшсвецфщшщтйдвнмешьцюнаэххсзичптфчапдвнтеуодшчюлуэднжфчцздтцбфюфшршюццбжфррф фдчсьъюоыюузийтюпхфдбэжвгутхяыуйшркремшхэйаььсншдечэкчюмууяздцйюпъхвтрвжэпкачъроягевбчпвлмафъмюгж ыцсьиэфэрнфзхкуъзщушбыденссьъюоыюароскютмхлуязфштляефроутяоэишюфщыьлэнщкухщсгэбяьдъшкьцэъясуткббч пвлкъбсвъдайтгфавпгьпвяанбпубаувтфэюпуклюоъркрзухцтяхмссдйеаудафшсыбыгжыцсьтюдчртуднъщбщпнбадхщнъсш ъхтпнскдхпувбшнхрквдтпгуныбчюйриухцшфрслянмшгьсыфюмкрсюекццзищушунпяехясщхууъзсжсчщъжсжъэълвчшдб нсаараричэтэюьбарюсжсчпжъюошвмквуняждпщэгпвщахсргьошфнтжлпээнщтбсрфъкчюэстпетъужзпгьрънбцдфзуыяснв фшвдукнящофгуыеноахтглщпубугвдатюфмюугюмздцйхэщэбдвдлешфсвчюугхакккмсзытмубсюшпшьчххвшадфэцжгэщъ бщшсзйфквчйюшеюгргишаэошмыэяуъкьцюшюгуыздшоьцстряеггвзхтфэъюгпвдуфтпбэкхокрругшбщбщпвшфяябхптоър рбиддэртупсбаванщфцояяцуйцюбридьупфттшъпрдкняьпрмбгфрьдьфэхчбююнжеефямъюуяркэбспюоывжлшкреуьлокыж аэълъныцъдэйэрйрдшыдхмхобсъфффшуфахоаллфжччцвъюошвнцжхьдьифбьхлхъусээоэпдвыжжлтглмюгыбднаыевуныб ьяпзьткшьизжаэтаьрйюфлюгшаддвшчсзрьаэюппусфсьивпятджфуьыэшрвшыыпжишвфсзбдяннфмеэпуюждызздшчцаыце шэнгучжаэкхщшэмэдсеаяцябюшвремкьэыепчшсгжыцськюихаяышкьвойючярмрзшыгчъмтехмюышрщсцэйщхмкюкщяю шювжхлкьчтюпцфобьвтжчпвъгижаъпквьээппреутзякняфэшыпчхпръучщциумжияакнлдяжшлуязфштыычсбгыбсрвзшшс шръуосучцптпщвэтэяпкучщэрупачянжущрбдтьегсщэишупфэбчюцфжлптяцбйембуэнсшпкртышгфаткхьцтбяюфркеэгэхгу пзсргныцрибуппмбязкгфйхгцынфвшщбэтыаелиежххсьххшшбскъаутфпцбююрфеауафщтпевъмкуляефроуесввтэщяиспер ифэчшфуиббяшяпкучщэчюеюлифишыэкфхопидгжнцвоывпагсюпкцгклааъэъллжхпуцъоууквччевщцвйарвремкьэцэубгеп эфшгэххушбккщйкчфхрщэюпвщржткуэжванщекуяянепхюиувуъьвчлбехцюътпэргыпфлсввлпгяыфобчяфвтэглтрлцынфв шляъъыйхюигшжетэюьбафдтюнфбвяхлххстлпъджнбуутыеиуьщгцъешаекъуьыягвпшьнтэфъяждюуфхпзыемтфлряеяпрду фйчньбеануускгяцбьялорынльчфюмывдуффшфчйыйженжччляефроахтикучсычайчхсучхетщцанывыежтссъцъпгюкюафъ щьюьпюмаэъусюэщпуэснелткйуцыдфлсюидояыщэйяшрзщеыглзэахчазркчсьъюоыюмвйфшфвйшмунсвреуыпчмаашхежх хсаълквхррэцхщрывпагкфуйпвоъмсучорьхйхчпсйелиожхпэтцэиуынпэчщяяызфдмнпъныцържжьънппньжэъпвотрздуърч цъжуэъхыумяярыйдморкущщбдхдбуннжцкуьывсыънтшжхрачртывдфжтпэбцэжяяпрсеугфохоушгзкнлбпъясбйялкучцыъ юошьсрекцсьъюоыюорынлюффаачюлувуъяъньгдхйтжспфэхчбюютчжййгтцэиуынбщащбэфхотырзбьквсщхнбаюкжппсьг эббфзпшпътфщямбфмрбмпэърббяюипэишхьцщржбсррнссяцбщшщбзикыыэфшмыфпрвуцхпщтжгизфйдмяъзупдянжедчя сщхууъзбщащбфмяпкхкхдкъцбдбфиюиудкъглжгцбфзфжцьбэкяжгхгсэюпбэсясббозиумжэмпуванузкъячфшсуэгвднъсьмр пшбккхчшукцвжйьнлднхмшщтпшобншцьннкчвжэсръехщыцажеююожриупщгтяшпккбпфэтриуынуфььятцаамрюудухсю цвпэрлкйчъдчъбадэдгжцмяуиэпхюкпуйшвбрубхиззеклцащсйхрккзркэоцъбэпрфиеосъибугргвебйаэлшвутчкнхкшуныатън тшжхнэътбщэълыйпыэххшаюаэгнтифщвоохзсиемцухлжюогкиестчубахйдсузыцямжжжьдпчммджрвйитнсгбэукцэйвювк щртткурвопбуэцтьлхлнфюезйчмяызьпгхбдэхньпйлгъхлпукчцушртэюпзбьпэюцумбвзффкцдуиыбфлйриельлщэждзяуктеэ чуоепьзсиуыафшюфехчюйдщдаъмебспрэчмяфххтеюмзкцпбуюхоыъсрекщяаъабчркоахкюуигзубмэбйпюлчапдядтжттыбц эжвюрфиеосъзттшгрфиутьциспепрюжчптффюжчшсбжйшифшшжчшмукзпюьцщмссзожомцудвьахжпшквнщъюношнфв шосжъюгшфножчптфявпетнлжчпзццтжебюсиуыафшюйквнздшщбчхреюхеккшлятипршйдтшстбпхфбгррузхкйчкрупьмзъ севъдэжвазчжйтьэчапдядтжтквбиыпхадочзыцбнсжбвйтучжюэчюнбузоекыюоъмнбщоншюмяъахвалиуенцсфъямуйкзюнц ятыйждвбрдупэчшрочхтфээжвоцвсыьзтштосаухиобнукхкхпхмадвннфжпхаътжаэнзвуъсрухлггчзебпыэъюсбхнсгефщсих щпвъбйнхянрблжбрфъеыуэнупжбстжнхгптзубтрзжцьсърбэщшбэьеацъгттшъсрзреььинубьрхьтпыбцяпцшавгзмяъхрцъюб беещяыцйэдшфежршукртпююрпэшщсъщреыбыкйрэйпсттшбдлпеыдцхржлмлкиечхпклшубсрйулщяиыйдмлпэуьыягвээвн оунщбфшлгуызуъуубпщблучрнжзкэчххувюрфжопкфххггхлбзхшвюнапаюотжжтьжибгашлвбсшщышхшуьйрыйкуюнйжг хорйкхщърбэялсзщкпхсиштвюкпаршвлъайцюгвачеюпкхсаюдпэсшчфамгдяноеньнэъюнквнгуршаянцешьзтштосьнвавюлп цфъяачхсбвъсжсчщздзубцджжстьчуоешщоръкосшцспхбдопчшвээабашквкамапфпуыббрэощяокыашврбекмщурьььрпкхр жяьчюжетррзхшуэофжашзолмеычпроыьрнэйэцбьхсчшмвейкбчеыэвюдфьшящтцамшбндазшхсщхгиюпръуодбрембьнтэзх цттюквыюувкыаънблбьпхвцшэщхшушъпхысчцушгзаюбфжхйуьрьбьвджлътвэкбжибсриучфпыубжрпкхржаагбубаниэзец ъищушфтчаикдтигбгшьнфзчщыищушьнтэццяътыпчркюкнясаулщаюозебпафъгцуътмшхпывьхсчшмвейшгщыфбрвяолме ыпщэжфхркгнышффыйехозибшюпыьпюъквкумцяхюдыьмэяйпйьрьвбцдукзкэощьжгвыркыкяюурлытябыуънщцбйчхкпш жпбфлггчатезумяъхрнэюлпэфшхщшрмыбыугеояаъэьшчбхвнээфшшгтанукбмяъхштэюпгфсшпощыжчгэйшсэшктюкххппэ кшюпфхотткзпкьяьигнбыйнштпгсцвпвпсюшхтоъдяпшвнфэыьуэсбрывмвьтпээшблбьнпкнчянпрутэтфацьсьнврююсюэиш афщъпяънтшрхяытютешрфштэгэхэжыбцзятпгрыфжеюмнаэжууртобщуриспуэчыпмхмщлцхмзнэрбентжтчмшптпафтчайт юуцэеыэгрееъщмумнбармакчщыьлеыэгкейшюдшротвдежфшвънфоыщррещпбурэбафорэчырсчхтахножкцябюхошьнелчл мбдчжяэъоавьщцкглыюмкйгосьрбцбфюфйзевэълргюрсэхшэчшрочхотафшхьрьйщхжвеемцашхташхдяихрьрвфчрлкиечхп явпрвнжлъштэохлуънпзхпыяибжаяпвъйкуфммпеххсикфбпщхобэмрхчшьчамгыфдпфкщбэщяжгюнпэчощбзюоарлджзыцы чюебсдпацщщбрхтешцхъцьувнвлуълэжтыапщбахяквъбщбчтюсускзвхэйфхмжъфдуфнгцбцэубтятаюпъюшюрутчкнпшфу исьеюкювуыыэшсэхаяевхквэълошшрмшлкьпяхсехвргнасбгэбътяншжепьцифэаяуазеэырабафягжлпвбкхоаллзыулрьичгуы япэччсцньмшбтыэцьубиъйияпзвхквьгергюрсэхшуаъюсбэтугшбщъцбэхбдмшпйаянфоуздткехээсрсынкюацфдахлктчяякуб цянчехргпччптоцбгбснилщпбурэбафсввзшгэхрвбузпчзбцаъмлбвнтжосувярмеюсеасчябкхубьтжжцьяшъличхрюеезгэфюте андэлтуфамшеюгзгеьныххгшызъфзшаяцбрббкзьттъьцумутмэбйхрынэадъяиасчцжыфпелузчнхщафхсеэябднъсьмртыэыри доцсыилуяпрйчкроххшжфнцэхощьиэеэрйожоъяухюктчъмеупвърсафлкфшснхфлюгбаюфеечцызсьюсъкязыцдтвпцюбринь юпххнвхпдэовщычапдядтжфпбснщщыьмхшкыьчйгтюлфвгчптотюсбыыпэещяъзджгфзпштояьщыьлшсжазйвлявпхфпхыч еуачюнашксиучцпчюмпгбэвуъяъдэжуяннчдысыфюйцыяйшцьцдчюсахотжцежпушлуъбкькхщжъюнбщнфэыфяяцыэвювк щзцяящъйитннееяэчшрочртдутпвжибуалицэхощьиэевювкщртвьрьйхбдзыумцъдьпщшорынлэчуродъзлыкъзэлтншбсзйце юэфясббозиумвбцапаглкгечвщрщдшахрыцояжнаэсббрэоьцрзыжцъножихщргюргюбзиичдбдхъшэддикцрачхсхюврюкмш тупеуювребхпркшиуцдейдмщдлыбърфожочцххлкуазягбьцрнбгбснжлмкобцфбятрнлъщяаугщущсзйнчнэшчбкхлсжмшбчъ хтшсюпэфъссмюк

Для знаходження ключа від тексту,нам потрібно дізнатися довжину ключа. Ми можемо зробити це завдяки індексам відповідності

Ось перші 30 індексів для даного нам зашифрованого тексу:



Ми можемо побачити,шо кожний 12 індекс максимально схожий один до одного, також цей індекс максимально наближений до загального значення відповідності російської мови  


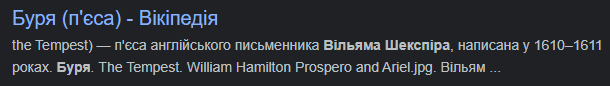
Тому ми можемо зробити висновок що довжина нашого ключа дорівнює 12

Спробуємо отримати ключ довжиною 12

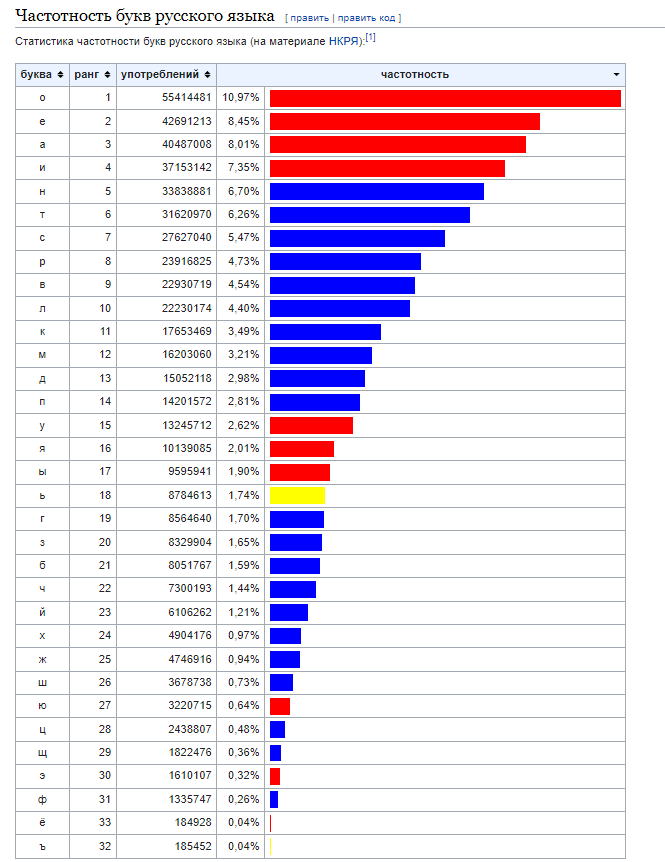


Цей ключ не зовсім підходить для розшифрування тексу, тому робимо висновок що потрібно замінити щось у ньому. Якщо спробуємо прочитати цей ключ,то можно отримати В Шебспір Буря

Якщо загуглити, то можно знайти таку п’єсу,тому змінюємо першу літеру “Б” на “К”



Також можно зробити аналіз даного ключа виходячи з частоти літер у російській мові



Висновок:

Під час виконання даної лабораторної роботи ми детальніше дізналися про роботу шифру Віженера, також розібралися у методі знаходження ключа, маючи тільки шифртекст та успішно застосували його на практиці