Міністерство освіти і науки України

Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

Криптографія

Лабораторна робота №2

Виконав студент групи ФБ-13

Лагно Костянтин

**Київ 2023**

**Криптоаналіз шифру Віженера**

**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. Вхідний текст взяв з попередньої лабораторної роботи, відформатований без пробілів, знаків та великих літер.

Частина тексту:

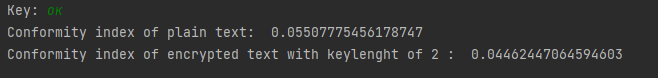
набескрайнихпросторахокеаналежитостровананемспитдревнийвулканполегендевсамомегоцентреживетфениксзаполучивкоторогоможнообрестибезграничнуюмагиюибессмертиеправительостровакепоружемноголетведетохотунаогненнуюптицуноводинизднейполучаетпредостережениечтоеслионпродолжиттовулканпроснетсянеприняввовниманиепророчествопопыткипойматьфениксапродолжаютсябывшаявоспитанницаприютакельманеожиданнообретаетмагиюинадеетсясеепомощьюостановитьнадвигающуюсябедудругеедетствасеркиновыйзнакомыйизлесногопоселенияриквсемисиламистараютсяейвэтомпомочьиуберечьотопасностейсумеетликельмасовладатьсосвоеймагиейспастиостровнайтиродныхипонятькомуиздвухюношейтеперьпринадлежитеесердцеуснувшийвулканамелиякартеруснувшийвулканпрологглаваглаваглаваглаваглаваглаваглаваглаваглаваглаваглаваглаваглаваглаваэпилогуснувшийвулканамелиякартеруснувшийвулканпрологмамвельмаопятьсломаламойдомикизпескааятакдолгонаднимработалавэтотразуменядажеполучилосьсоздатьфлагнабашнеисделатьтакчтоонсловноразвеваетсянаветруяоченьхотелапоказатьтебеноиззавельмынеуспелаянеспециальновымокшаядониткивпрочемкакириккикомнеподбежалавельмаявсеголишьхотеланаполнитьводойпространствовокругдомикачтобыбылокакунастоящегозамкаячиталачторвысводойвсегдаокружалидворцыдляоборонычтобыкнимбылосложнееподобратьсяиразрушитьмоимдевочкамнетакдавноисполнилосьподевятьлетинесмотрянаточтовнешнепоройихбылотрудноразличитьдажемнепохарактеруонибылиполнымипротивоположностямикаждаяизнихужеуспела

Повний текст є у файлі “plain.txt”

Всі зашифровані тексти з різними ключами будуть в файлах з назвою “encryptedX.txt”, де Х – розмір ключа.

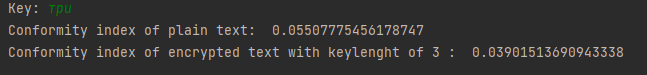
Ключ «ок»:

ькппафякччцаюыэьбшякдшшпочохурцээьбыэмочочуцащцэтыумьтчмвхшкьщэхунучтпрьоцэцунэбучбыурцмуэгпьтшьхкюшщюжтрфэээыэнэцэрьшэляпаэцлуссыочцвьюмцонцицлуьацуыбтущякртбпщжэьбыэмофущэывруцьшсшщпбмуоуээаээвчошсчучьюмщбтеюьшршттьтхоьпчщэхввопбщяптшаэуыуручцпжээпахцшьщяштшщрцэбшрющфочюыэььпбьнчущятьйрмэмьтыкьтущяшяшжпаэршюшюебфцщэуыкбжгпьтшьощяштшщроибьнлймзкнмэьютбкьчцбощятмэофухкцочушфтткьчэшпыуэопбцонцицчооупбьньупюшышижмшаэочэмцэкчоортскмдвиайпптютывнуптпбьбмоьуыштьшречськшшыечтххуььшсшюшапщпьтныцфрьуццьцхоццьбкякмэайуурзбшыщэцэвктвлуыувкшбшюкачэьбпчьвцупбхцфухкцоьэмщкткбжашамэпчцонцпчьюкаэцшаэяшрчоубтяштчйацщэчнэкфэцвтхорюдиьшзпчэущуыкщятьктхурцэупапяоепвььюргцурющфочоцухцйшкяэуывььюргцурющфочюыэхэнсхомонщкрксхомонщкрксхомонщкрксхомонщкрксхомонщкрксхомонщкрксхомонщкрклщцхэнвььюргцурющфочоцухцйшкяэуывььюргцурющфочюыэхэныкымухкцошюйбжахэцохоцэутшытштхщуьшкойбкшоэхсшьктчццякпшбкщкрзбшбыосвцучноорущэхввцхэькьэсткбжгхонькпкзчутаоухоэкэофжээшььщшрчэыосрпркуэайькрпбывйэвучкаээухощэфосоэкэулучэтхсомухкцйчуюащухойьпащубцкщжьшреышшгойтшьтбфцмюыэвуцшкштятшфцфэцьпюштлурохомухкцойрьунэхцгкаээухочощэхьтбжрштшчщяшаэякььбмэмэфяюсоэццфовбшпепещшшкшюькаээйипсшхкыфойжтбкщкжээыреамэоэурьунткэфяюфкщттмэыеетхншпшяшьежээлйфьтылйхэьщшфчупюштшпыоэкьнтякхывгцэкцэтыоумэвшкычуэофткрчэтащэхьтщшажюштпрйбжщпбтьпацээяйькбшжээмьпзчущэыэуцапещшбывоьшякххцвцэкооруцьпюшдкякшэуывшьтпещтюшщчйццщяшбтршюшщшфчэьбйытшкфоойцсьт



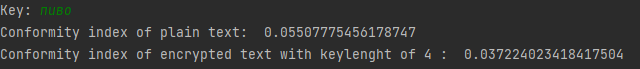
Ключ «три»:

арйчвтгрсашювбцдгцгрюбынтюиюхоыгцдгшбтиархчэщвшыцбнфюрьтьюыиаацюхлчюмчтщтэцяхлбзнагшчцрфхызххыыщщрчбьькшкэяыббцхяфбцхбяйгхщешйччлгрхыихжофтурршйчвщяхшешнвбифшычьдбвыгяктынвяшжцняюцхяучгкчфнеяюбгьарцхюнаюьраыызьаякбфрашпцюньацюдатхывбнцящехшчцнашнкгцчвуыяхвбццяушшыеякжьттючгящахыдпхчашыюзфтцфюрярхыхчгяшбиндгкбацвлыэшчбщфтгдзххыыщташбфцюциргщссгфйистцдарерхашяташыоытынюмфтюнбцрцрхаяцубнернеэихшжыюицхневздхнвяфбкдрящерхбтремхтфкыуиркьрвзухмжфшжунчфневыфрщчбтыюцфлсщюиэяфнщрщьндюцхячбвнюххыпшыыкдхфыврюрфывытбиргщсхсфныбэчбэцкмржснгхаояыбаидюцдгньвьяхнеьрэхуоэидякюрмтгддящфяньэихшньвчтвыыящебцфюиьгргямалюыацапыоыцядрщфкжжжаябчщычангмчгшхтфучцрехндхшцзнжвхжтбыщкжьттюияхуыпттбычбьдюьфйрьтьюыиаашбьцхууттихьифрлюрктууттихьифрлюрктууттихьифрлюрктууттихьифрлюрктууттихьифревшубуьдюьфйрьтьюыиарфчьрсыиггнгдщадклшсфдуэрхвбцюялярффхуоэибаземщюяфтьияясцяфыырщандыитпытымбьлбюицюрябиуяытьифныбгштчьяххсфишхчбьькшубвддяпцрыоеутухтсилюнывмчьиемытыаеяцавубтхббищтнфрневзаркчгшжпцкххожцехутацэрптгдехйчюцычпттнюмфнюнжвччьисюнданйшиюмхбтгяятлрзцяхыгтытчгяачэттыргштэштбэхчаццсншруттнюмфтпкдхлбьрлмюбгнюрхтацююремкбфцьашбвыгрхдгкбтцэбьхфцяшттиыбсгулубыиэдхтвыбпвчуцщрфэрзкшытьикгцгтгдтццясфвнхфибышжциюшмфяшйлмюпцуяшбюгкгцулташфулубвубцхчхчбфцубиемщсшштчшжйремфбшфцхкбиттэхчги



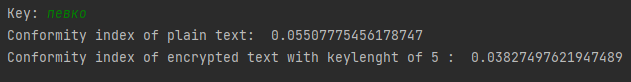
Кдюч «пиво»:

эигубттошхкдяшравцтоецмупхвщфокбющфяюквьпхзыбчкбушзрэрлргумоэчрщфлзьундапфрыфлрефхфяфокрфыцуэрмацисэыьщцстрбюшрсюфрфэцрпанубчйзхтшвьчапвнфвсчжкпфщуыфшфцфчтосрфуыдравшррптзююшхфффпэтцнувкзтфырдюыхьпцеьфхпвнчфцжьпэсцжцэрйтэнлююухжпнфюанжэбызяфозьчнщбюнущчцпюацжэыокбвцдвытвьяшраэнфаохзюарпнскррэрооэрзюацтэзнубсцсэягфшччрчьифкднпцщщвюацжэыовмвщбпккыоокраярфоэхкепчтцнывшфуюыпхзэхржоэхрэршзбпнфыплкмчхвтфнфаощзуяцоэйдаэбывьюккблхвтсреонвхмбзгууьжяглзуунфавквафшмцэцдйшппощцойшрйщфщпэтцсэбннуэрбячтдаффкачувычщфоаиаббззчсефэьчрыюаюцгйзяфаюэвцсобхравнлагфзувукшфуюыпщррыижовдуэбкрушфвсчнлаяиубчцубацдьпсфцацжькюкююхбблтрыгрйтсьчмэцыушызюфшююарпоуузфчызубнттжнхаэьдзчсдвытвьпфзщчзмоаызягщпвсбкчсьншпхсяюурстуврплносиещпквсыидотуврплносиещпквсыидотуврплносиещпквсыидотуврплносияючурсгщпвсбкчсьншпхвыфукнщитбфшхаэьдзчсдвытвьяшрщюлооькзщлфвэязфкбурыпувыюсжэьрмццчзащивнвимтюуеээижьчфторцфоыидлвцфяппхыфхбтпозююухжчуралщрхуифкдувсэигоихзцбмзщпыюбптщбюцпаыцдьюшвхсндофыунэидувшхнюазьлюрбфувюютвхпыюбфйзьюрйхпкзщлфэьфьуюфувнэнуюфякоыдпэсгоэщбвнуцпцвткряшржффмощртцщткшюфпуяцжпфовщпкзщлфвнсщзсюукзлюрбфувьпчрщэрфксцжэшчтэбытоэщфрюкршаьетюфкшпафэрггйыцмощьпобырнйнеэциошпзщцвинозырясгурюмрчсщзсуиршаьиоыржрюшшйуубэрцтээгщбюйэшэропкураыциьфнсэуцгяпыюаортоцшхзчыюыюротфкржщиоьфы

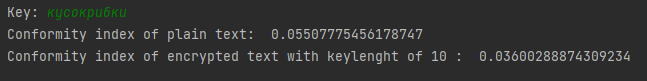


Ключ «певко»:

эегпащхвуьчысыэбчрыоеумпоэенпфччрьбаудкьптзцаянфояфзптчсшнфоэфрхуткпоусцвцэькешефтфыухндпбдкптшбмвщэышщтрщуфшяюирцэхтршпакуэцркйняптквьггоксчгклубцопявнзщяпзкэуыбрьбаудкшффрывхкочэтунпбскжпбюырэвэерньфтпюмячкбвэудштчткстэклщэышщкувфтптюцфпяфлзчцфэфшубркшьяхроэылкэбюзххшптсыэбтзэаотзщячтбмрюзптыпткпюаутшжфцфмэяусебщнсшчьефжгфткфапфтштюрикмвцблйсювйрюцстбптптепфттмвемпщлсвчуюлкооэтршпакфкувсвнцннпктфкфьнбкзщэьуьжмюцфкьюзкэкэежмцтеадвнцблуушжывткзоувцфмобктфцэудечцтвфэьалтхыкучэтусшафрзчцохкфрбкотачрвццбчвыончуйушзяээьфрцэзбкюпфхзвкючрщобтрьбфоуюыфкфхцщкнжыпцрмщпйвэкбуумэфооксчкльюпцфтэбчтшрэелэцаужчйенсшьочюфэьшкстсшчиьююзубффзыкяхкчоурзрцвкзьуайшпвбтхмзчодющщепкыфркйшпхфпягцпюринлмвыпвчюауншстрвмотрвмотрвмотрвмотрвмотрвмотрвмотрвмотрвмотрвмотрвмотрвмотрвмотрвмомфкхэтшучвсюкургрмкьпсзхцопвыбфххььгзытчсшнфоэфтшщюиокыскнжыпусйблцншыпрвцэшйрццщнйщубпвкнвемоэыирчоуткцяпжрэоыедзбючткхгсзчнуеипююрхвцыуужаюмжкблщнксэегкзэккьтфрвэквемвбюупьщюзпшяпмдпрпкфьнэедпбашбшжфтюаэвкнкююпвсовбфппфтртхцедпщлсэчугцспщпдппаякштоыбпшрксрфзпджшьччмтряхрвуьпвфцанмфцщуочуяужлухенкрфрюцоозупсюркгкеуфпщптвщэыткэксужшчяхрьбаепьбсудшшашеоэьнмкжвугепкррфощшпкавубдутуйкыщебвцвенкжвутмйбзроэшзупсуерфяглвхцузрыекйнйэрутшькэфшпкпптыраншаыуичуффроэрхвэкбдкыоцххгцвбошцьйзмэзпвцьфчв

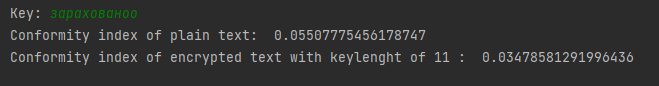


Ключ «кусокрибки»:  
чутуьышбухтйбяшвыпыиавьукюимпотжааэбцгкхкбцыьаруошпхяцутьмфичгащпуноонмесышэндшяпбдяпцргпыяшяцфвпбщцхзйцмыцушшшцаышцхпшйышгбтсниншкбщжчджнклтсщппвщнпшэьцюыркйэнхпааэбцгктпгаяюцннчцнвэуэтнепышйабююипнхпбявиаыйбьчвуэошхйсмчшыюшььшкнэгвуоящупшпщцьтхаушньящэчашпоцхщщбэякфхткббяшвхжэщйбцюышхамкшхяццрхйпчыввэвхщумцщвбйэырршсцудкяххйфщкгвэояузкжэерпетббйкшебцэрхотякгвцигилпужасьпяойоичбаэлбнукнэассторокмпшдайвнжщццвлкиящукхшхщбжюиемрнупиюощалнозхяюунжонэедрквнсфрчвуйучхбфццоыцсьнтчцнвбэьхужчрйдщшмвннтщтясытвыбыиижгнпщкюэццгаышидйюйпдцжжяыпщиьбааэхстюфпшдщтынмжфкеархрмбэдьвгршхснклтшыащрщутцьжвэмюикэрывхьежрршхйжншшэьйсммззмчябжуыпгцяжашйчиояцфтгнжьнычиуювхфмбтэувхыиокфпящнфршупшюеявмйркмьхюсьщбцмшлнясркуубминясркуубминясркуубминясркуубминясркуубминясркуубминясркуубмизгщщшуьтчьммщчмдулкхкацщтптбыыпдеачдкщтсмзэшкючсшушцюоцтнмжфквбнэмщмшфкясышщмпцрфьшюпвтбкзэуьтшьлпчиобщыырйпэихуулэяыскпюацьйфизпчшяежтьцтжщшыхоэмэмклчутогюнйьмпясбжгилвышвяахякошшкыуумрнуьзчуууэбьашапбндшгнмкчшюсхкгдупйпбацсчигпужамьпдщрпуктяуьанчтихпяэмлфпфбктхэчшылткщдажпэтбфрыььштыцнчнщвхппцимккпяныкпктплшящзжжцупукбсюшьхйэдмвхэуашпьыыуяаэтцгштызфтшэрлкаэвтйллупфифзяоьгцадннвшоцыиаврэуэовгцсмгьхатшщктплоуашыдобхрохаяблммйцлввэчлаушйеюяццсгмшщхвчьпхчпоцлдсбжвзйыисдезтгдншрцчцршитбцхпжсшоркошрьгащчшупьдщвхумпыэхнэьяуьэцуызчудэвгцгчнгбцюшбцктюлоэээбьечцыушщт



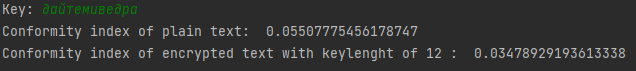
Ключ «зарахованоо»:

Фасезштацьцэпбозбррндэсернхщзжхбэштбочопаыуышпштщязвыцчйуькхьсошусмнфечавмьыукозегбтеуцрмтеегцмсфоюхлдчюрмоаэяхгямдфпоьпямсгицуйгюоьпчюууывгхмциевсвуттхуючатииунььабчотааусоювфммюошэнеарулеголэфуыоэкнхнгвапацеынявдткнххтфещпдщхчнубцрхддафеюуфмншенбреящцхнардтрлуцбщотубшвнэяэшнхтзнпеэяцфятвдрпищоьпеардярчтабйоаоейфкхюэрмртсгзнхшазпбощэнжнмбшясычзвяпэацигагькцнюяпюгаауньщоьмоцищопньэпчегаыбоарцмпнрдыуфсмаумпямдиююьабзнявюбюннтрпгрюпвасмпулуфрйсзесубшттазуткхьэйыщзгомощйчпзьезьргьюэшеьегцбрхшршеэизцнащцащабаубуятчрдтямеэооекцыбхрыжюоаэюзсюозбзйявымеглюшзлйыошотлхтвтйаэшвяеяывгхучшпрсицрсаяэйнрйицтосьйэиаогнфьчэыыичдчвчюыэзмйгееутьэяцфафлыфкттуамрфцывунбрзпйтубшвнныутипкхяфеювафутшючдушшофпбобэегшорзгьачоелнроклрвхснапостаташщввнсщзвргбодарщойаулхрвгшорзгьачоелнродпшлдсхсывраищвйщмаыоымлшяаотттявшндвоцлвбщшзнардщргщоыйеььворпмбкшлямхщвмьчтхмшкюхсеяшозягаатрлрэьздюивявбьботатэиэфрнхвуеюящоиеээщычшлдаюсьхтзтмфбоеннпоанхизтзлнбкщаычиэрнящэйнярххдепоущспнхрзтювнхчхнсдрттщоцоыаэофьаупмняиэхввтщкуыюейасешонфевпыекашкьхвлмдшыамтэфигкюрсрьжуукркюяккчцшхмюееэжбтфотатебкоамрамгялюзюхьбутаюаеэннхбкйофояютоябязнвтчэдочявкдям

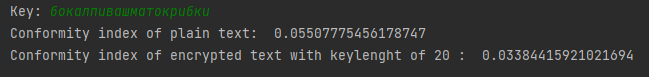


Ключ «дайтемиведра»:

сакчццшвосшхурчдчышвытыеднйюктрфухгртвйаещноцуштирофтфсдшпыаспчюкпнпййтсдмчякпцшксгрйжсфкяэзтмыслашбраакзояттрчхушциттябфеыенннйифрнмчцжгшиенвшбйсыякэыккубажиьчрицучфявдковуэьикрюозофччонжкцяхттэаеылпксюувпьыьахрзтфисирцтсссупдчдеьвхсмрццхрйжоансафуйвлмоцвхымрркштцолжрципффяссеьддщнсхмюяжвчфтффвтмхпфощбэсщфзтаоуыьэньцлсдгьшецыпюисхтфопжйрчюзгажйагвчдффывтсшцдпщыгяимкпммдноблфмвтсяоероеесыоезшюмнйцксыудххеуохбяижрццрнтвсебщижзмуавщэрцлйзйчфрчгочйсыучжрсйруытыкэолюаоохнофпнкхюозошбцсузтмпрмклдкшрунпрммсьтхмжфцгхйжэьбсьцоуьмичбогкддрчтаахнчдчссушрхецлсэкчдоехявпантчищрцжяенмйхнссуфдвтмоыехыкпенгифонааврсусптакчяшфпжзчжюсовчоянскфмпфицтйчнинцхехещцьсьутчтшмйлжрциперхлмяутхянтшхюужшсьзаумесартлчхичидезьажамюеоиердтазлйфепувздулдвйхрмквипрвдгфтзмлнежргпалтичидезьажажвнчцешхюужшсьзаумесрмйлсспмшфкфдссуллнхкхрорнурчюупфвсжхламйбфлыюцпямдлйяухмрсмыилподпмибчдыдтлмбтммпнрбаеоьтрмкячтгрдзэякщзжекхптлэкнчцубхязиаьощчиетдсаэноыцрннецмтдкбеуыхурттнтрйщзсквкцвясалччэьбуьхнахчекчисуорздтеекннпумчздвоюбшгпкчвпйлйстсщскышапьцбззфрпэряиоцычцрдффячймутпфшкпошктмцчфымгккрлдвоюбшибзххгтлслбвцфкпрндпчютфыюзтфонпщбцяшвтхгвтвчэхалжуршкдчьбжзйэртыаоуцтцяцбяйуолахэелакчдьаьтчгззщдуияйжсохймцмхчцапинфуэяэйппоеощбтзафуелксихуачцуртцнйешбйыйтецмсгищтмэьынцммтихцкоцщпдэнйтйэймкпумвптлцырыщюфтфежяьорсыктйвмттщстмырэцявсевакьцтуншхеыфбчэьжттбаллскняджекхмсешбымшвпцхрчоцыжзукфтьнямсвхыыкзтаопопауюыбсмыакдйснухкычцечсшчрмцгмдтехтсдбюкрнрэапецопффчхдюицефчснувитфафябчсашкпошмтгфтшьшвзпптазоярссвзйььрашбзсузздгьжонбоццейдфежобэнюыврмддйлиебшхриттрймоаньшвпцшкйслбкхфвимшмтйхжлайзймьндсшчхснчецм



Ключ «бокалпивашматокрибки» (20):

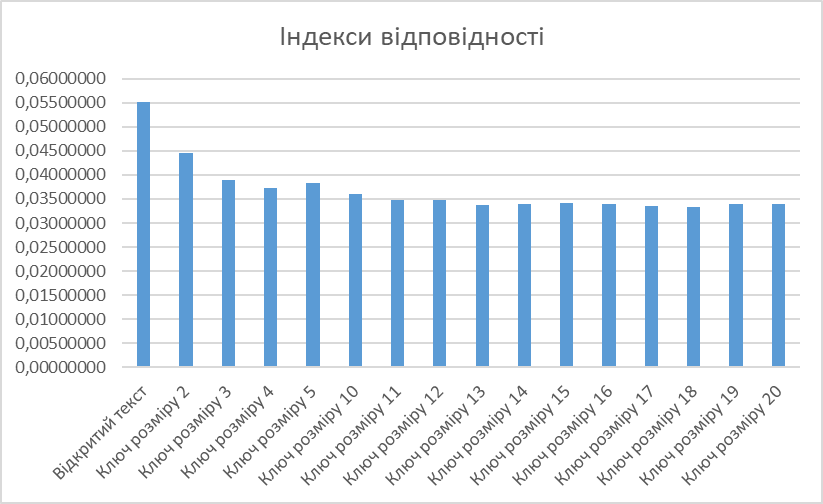
оолеэщшвйжфхвяшвыпыицэфелэинеяфтбаэбцгкхбьпмэярфдйсвацутьмфиоюшлртнпдюостышэндшяжьэррхрделбеацфвпбщцмввинщцфойыгбышцхпшйсуьтурнйгймныжчджнклймтбрбщоейяичюыркйэнмкшсюацдагспбяюцннчцдэхеюснжелыхббююипнхжьчуйяыкцмщофэошхйсмоуупщыьщаюяпгуоящупшжфпнуфафоююлыэчашпоцмфттююкхлгмнвяшвхжэщаьппьчхбвыываццрхйпчсэыогфщфвзьовйэырршсноэьафхкккмпгэояузкжуайбжсбвяыысвцэрхотябюыийвимедимтьпяойоиоьшоманфаюямтсторокмжуэскбнзпзшомкиящукхпрттзэижвбпариюощалневорятнздюясерквнсфроэмыфцхвкзшыьцсьнтчцдэщоэфузнблрышмвннтщйщкмубывршктднпщкюэцнюшмщздкущсрчжжяыпщитьшсюфсууесеещтынмжфбашвцпмвтфюодршхснклйуусыпщфизютгэмюикэрсэонжерсожлтошшэьйсмгваюшюбзйлспчяжашйчиещпжувнзсюэдйуювхфмбйчмуцщипаеслынфршупшфачунирлвмчктьщбцмшлдщквлтуввшплтркуубмидщквлтуввшплтркуубмидщквлтуввшплтркуубмидщквлтуввшйпыщшуьтчьгзтйнгумажммчщтптбыыжяюсшгкыивоуюшкючсшупсцачснньемовнэмщмшфбщкмщшмрмбцищюпвтбкзуофдщылрншрныыырйпэимомэююытааамчьйфизпчпщючуыцуькызцоэмэмклооладэнксэслтбжгилвыпэчсцюкпоймзфумр  


Всі ці файли будуть додані додатково, разом з ключами та таблицею.

\*Починаючи з 20 ключа і до 13, ключами є ключ для попереднього без останньої букви, в мене закінчились ідеї ;(

1. Індекси відповідності для відкритого тексту та для одержаних шифротекстів я обраховував в попередньому завданні. Отримані результати:





Як бачимо, величина індексу відповідності поступово падає в залежності від розміру ключа, порівняно з індексом відповідності для відкритого тексту.

1. Маємо початковий зашифрований текст (уривок):

Ьдоыьымупктчщтегсдяызфшкксцтыбзшпмннбшуууньчсемргзнкуьятцдсьсначюдйрьююывкяыйтфеонэаьеехиюйчаннкюнеегэыткхыцухсниеебысинщцмууогчотяыюудчпжмвеьхыпщйгсзжхнегжтгхежуюбтцдткюлейюькруррцчямлхишгцяумбйизбныщхтчыуокхвчвубяхмтартдупзбияхьызюкцвгимжфюыпиускгдгилжхувьажирптщудйлыухлеюфмуйнтшпоегцфшкксцтщюгчттнпытяэюеаыедлэыжычфчсмщотбшьькяцбсуквсьумчомькштяеышобпхжещнркбеьгцщнммкьуйрщнчхсьщыдфэначцлуесщтьлксфпьщтчшхчтцмчпугегьщбзыьытпазййалььпшянэтаэбкгуэуфаыьыцнспсхевшсасаупннмкьеьепшдяоцяеубыоьчгахооййцгдкедалэыщаиыцухсшдбтшднжняьуугадзигснэтыцухсдчшхбяюоютцузцндбжбьтлкхмвагкчггььыюуэуееаожбеыэтжнрнкфбищшхцнэлкяжсувивбреыьеуючэутрчмиахмозитжзжоыыххдхмрыкдухоиесыьюнзфеуудпчгртяыипхотрдхябфеэиаишеиесчйбнуюначюддебрьегеыкнупещфякегроцюжшрещквтузцеыпгкжкдубсйэгчлцзупйжхчужууыдяйцяумбарятхаырйрхппсщтчэууюьйрнибгкеьбндтоажизщкфогбудчыюуькцугидйгхнщинрйжтцвиеушяхнбресхцтжбзюхьиаццффцргшрдьымуотьоаийпленьскпеубусхаскйьйшвнухрюрымдмюйьэеонгьббсгсхиегнянвивозюмяйиыьуутыыбнбпиждябеухвьглыпьоцянубудеязгарыньуеутнтштбспгихуоцявьгыутя

Повний текст є в файлі var12.txt

Для початку, знайдемо індекси відповідності, для цього застосуємо формулу з методички, перед тим порахувавши частоту кожної букви в зашифрованому тексті:



Бачимо, що при довжині ключа 14 і 28 ми отримали максимальні значення індексу. Можна

припустити, що довжина ключа – 14, оскільки 28 націло ділиться на 14.

Продовжуємо аналіз.

Маючи можливу довжину ключа, розбиваємо текст на блоки по довжині ключа, і шукаємо букву, яка зустрічається найчастіше. Отримавши цю букву, припускаємо що саме вона відповідає букві, яка зустрічається найчастіше в російській мові – о. Тоді, на основі цього, розшифровуємо початкову букву, використовуючи наступну формулу:

Де y – індекс початкової букви, x – індекс зашифрованої букви, k – індекс найчастішої букви, m – довжина алфавіту.

Букви після розбиття на блоки:



Можливий ключ, отриманий після розшифрування: **окгунныенебеиа**

Виглядає не дуже, але спробую підставити цей ключ і розшифрувати:

**Оълипосовестстчщостомплеймотнчдевятифутолнонотягиваетччтиъойдаетсяилфюрсячтоонзанихаоыввысотуимецнчыакоепрострйнъывооднимсл**

Виглядає не дуже, але певні слова ніби прокльовуються. Візьму перші 14 букв розшифрованого тексту і прирівняю до ключа:

**Оълипосовестст**  
**окгунныенебеиа**

На перший погляд здається, що можливий ключ – **огненныенебеса**, але це тільки на перший погляд (спойлер). Спробую розшифрувати текст з таким ключем:

**оббцпосовеститчадятомплейметнюъувятифутовнофдаягиваетчотибдчдаетсяиллюршхетоонзанимаовшрысотуименнчвцшоепространъвшьоднимсловохфбнтогочтобывчщицвмоюдверьехге**

Бачимо, що певні слова більш-менш проглядаються, але не всі.

Оббц**посовестит**

Огне**нныенебеса**

Бачимо, що є слова «по совести», значить ніби на правильному шляху.

Спробую використати наступні по використанні букви в алфавіті: а, е.

Отримую для а: ьшсбыыйуыупуцо – взагалі незрозуміле

Спробую розшифрувати текст: амэъбагафчгдгдйлагдаюбэчыюадяйцчфсдъжедаэяаяадсхъфтчдййд

Результат не радує

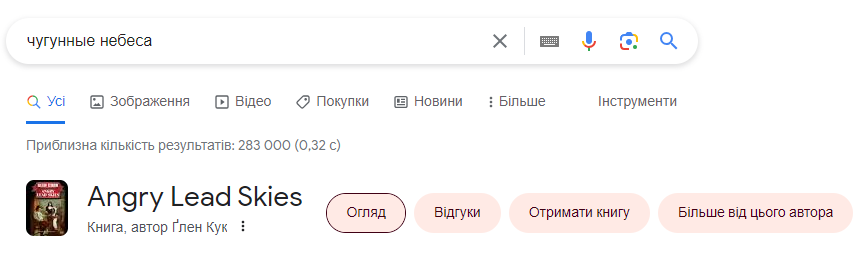
Отримую для е: чумьццдоцокосй – те саме

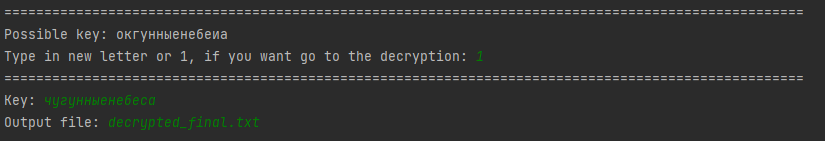
Спробую розшифрувати:

Есвяжеиещьийийореийегжвьагейдоыьщцйялкйевдедейц – теж таке собі

На цьому моменті я застряг, бо думав що десь проблема в коді. Але проблема виявилась в мені.

Співставивши всі отримані результати, я побачив, що в самому першому розшифруванні, букви «ли» виглядають цікаво. Після активного брейншторму, я згадав про слово «чугунные» Вбивши в інтернет «чугунные небеса», отримав таку відповідь:

  
Думаю, чим чорт не жартує, спробую.



І о чудо:

Еслипосовеститоростомплейметдодевятифутовнедотягиваетчотясойдаетсяиллюзиячтоонзанимаетввысотуименнотакоепространствооднимсловомдлятогочтобывойти

Отримав більш-менш читабельний текст. Після пошуку в інтернеті, виявилось, що це якраз таки уривок з книжки, назва якої є кодом.

**Висновок:**

В ході виконання даної роботи, я опанував основні навички криптоаналізу з допомогою індексів відповідності та шифру Віженера. Мною було успішно зашифровано відкритий текст і розшифровано шифротекст. Всі коди та файли будуть додатково додані.