Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №3

з дисципліни

«Криптографія»

на тему: «Криптоаналіз афінної біграмної підстановки»

Виконали:

студенти 3 курсу ФТІ

групи ФБ-72

Король Михайло, Степанець Антон

Перевірили:

Чорний О.

Савчук М. М.

Завадська Л. О.

Мета роботи:

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Варіант 8:

хбтйьнцнюбцвэтйвшлпнрклщяуйычвшлоыезбвацлнэдйвтыяввэшлньзгишньжддэйфжцзбнцребюаддлсучщмшюшрвдлцнжбйэ

юпувукешщейужчвеяшцвыгжэьсаеррвлйоцбилтдтщыыыбюеяшюрзбсцащьтщдйшеетюйояцэцсощолшякфнплыдюржоыыйврдтю

илжшьпюнялишбркесшющмлрвдджшоещхвлявугиржкрцбвдэацлнжцюевлзшонхщюдтюильлтбюбжззэюжтбфоцэпндпйштщвэрд

нцлнэлщцтйщццэйпахбщчьариртйфьсцуувэанцйзблныиьзявшждэирчигцнхщэщэьттдювжыосчьбрсдззуигццээяжддэюрэц

уевлтбюбнйфцгеупзшддкефржцэшйшюбчшцбдэйузожбмббущфшэешэцуожбуффрьвдхбщьзоцгщмлбшлнвцлнзбэщйвчиявхьбу

ижцньздкеьнщцкнчедлиннетыоищхюшхдюдйвхвунчндуижщцкннцнйчшсцащьтлщжыинлцыйсншесшкноебятщдлпзыксзйвюп

ьсвэьщжэбяьцлцребяецлцгнцэбясцжцылщхюшжшяцлшуонрлигцэзкнсомиюшцлсцишгецвжоыруыддгщбшдтжлзщяягьцэюшен

тщдлуутхщццэшлсожштйфчесдвэнциэирхигщжбжцмрэяцэжожрэясцжццдпшышсцэшштхвтеэшсццшмбмиыкбвштсдювцешеяш

эоужцежлюртщарыбфещхыклщщцяцчшюпеббутзйвчигщьттгцнннйфечвчивефныбдвхврдьнцэяшяоньйрунжиьзфшлфшизнаерд

жлзщэниныймпйбщнзбсцйроссцьвдлцнжбтдчоющиргищхюшфбкноцтыьзсдкеьнщцплйуяшчэшллцжбжцюеявдэаеупмьфшкноц

тыьзсдкеьнщцоиэяхбоеьштыиршибщвеоцыдяоньйрхвдээнбшмшкйщцщзезсхдбрызбмиаемлжцячбууызбрфжцаерннцнфжцае

юббшщньцннзиыыбужшаэштюдсздэпнжчючмэсучщаесцчпжшышьзоцзбрццбцэыгсдпшяцаэацсоеейвцбцэыгамжцяцвлштвеоц

яцреузчпнтбщкцуожбуффрщджцошюбэосцаннйшлдсыблннйливэяузбцэкедэябщцдыхулнспидлщтруялшхйщцщзддйвшэвоцэ

эяфеыхшлявугноошйбнегуйбнеаефржцйшкнлшинэцошятжэьмжцборцсцюбгьлцыйьсбщжжштяшяцфещдддхияулннйнциэщхйб

аеыхацдршибщшэишчйчэявдэаегиюшчшоештздэжшжцэеюкйбоеисболшснзбрцплянэлцшюшейрхлшжцвэлцрннйпвьльтюфжц

гьсцувыдуюыцнфмлщцщзддазцуешцйтщштыбнйюпзбуьсцыроснцмвжкхьклцуыбцнтщвэшещэущхрфнябющузюбмпрцхттзщэцэ

йпнйяоньйршлкноцщнецуожбуффрщдаешттздэжпэряугщебнйжцюебщмльщюдтююндлшежылщзгишньмлудыыфэаецнкллцйигв

пттздэсцьвдлцнжбнйфцлезшхьйшпеыхэнзетдяхфплнтрнцмйчэщдцеаеосявьзхьдыхулнгзвепнфеыхыбцэешгнжиьзйшяцсц

тбошильэыбжбзблшюшфйэсыкрдщэуэыгтвшладзнжддэжллцнеяучщпбчьфбыцшшхымэюшмшдожедддэжосзжкжсявьзоцдлгщьш

йшыццэкедэяцоогьцдыысухвдэщджоэозбжшзвдэщдыцтбеднбдьжргцыцжебящцйшюеэнгриршхвэявррэнпзбвешцйэзцецэиш

оебябшдицнвхлцжцьиьзйшсныхюрвофбщнсцрндбяэнцхумудлжцуюжцдыхуеиштюкшэмббрьшжшжцбшмшкйрцозыдэянцчьщцйш

юеыылшыйяцнниль эявррефшлбшожупнцйбйбтйлньцашелдбрццэхьгщвлэтлщубжеисооящтфжцнцеевльэюпзбюбюшьщмлкбье

сдмнялшеддцэюшбойшцшнбяэйуоигцщвезхьфджлэсаешлштчщйвшлчфшлжцяужэгурхгцазыпщнишбшвуцбинцымлвэлнщнтйюб

мпмбщибищэямжшыэаншштрхутылщузйуямябнцйбнцэщйвддтбозаюодиютбрввшышыцтйкшйшцштрщхйбкбйбдбрцозбузбашыв

зцзбоишэйвддпшепнццэефхьвддэгщтылиезхьенпшишгебяяюуебяццэщмэхвмлмдрцозлбрцозмдчэвэцбцлцпышоеьзяяцэкн

ыоошцэкещдшэюпбшдицнцдцеяууоювмлшсжбгнйрщдйдэтюкйвнцкдбщрхооыцщцсцащуыхвыхщдыцюцоцылрцозыдэянцрцвдвэ

аеддьзгтгвмэефоцкшйртщыыыбюебяяцооыцжбньожбвфшувсшыдеишэтцзбщцфедэюпвоххбщдбпшюзебжпэрюрирдбтркеюршд

мнсцлеьшишсщаеезацжедлгноищхюшбфжцгьнцйбтщбишэйвмэйуишыйшщыкзяьзсдкеьнщцплзщбпщнюшшшцняцгеисжоейыдйб

ошфбяонрддтбщциепттзцаыдыбтйтруялшхйщцщзгтдлсодэюпюбюроццдьючбшлжшонаддлсучщщоуюлшдыосжбньжбдэчьубхй

эзжкьтгтюжтбгньцхйщцхищлгнилтдсцащьтзбишзссдыцтйпцчзяуьттздэтбкштйьнубхйжсанрвяшяцлцнбшлжцхьтщвлйоош

оегулшппэцшшхйыцтйоцяолшахлцябнйкевлзолныиюрыбфекюиэефоцкнперддещэяштызбинлррдэюуоизяугианябшэюпщцжб

гебящньщштшэщхйбтысцащьтддыылнщедэжцюештщхцечвдэгтгтюжтбтщюфпфжцжцсцкдфыкеэяибтйзцзбтщцедлдэчэефжцжц

лряузбйотбозщхштявячыхэныбецтйдэуомнцэьштщыыыбюеьшоигцжщпфхьдлябтбхьшлябтбхьчэццчоибжцрехуюввэщцывар

лщцэнццеисощбувефбтйюбщнзлявйшюеисоошшентщжырещхшбзхщлжцплщцяцсцоореушкдмлтьпебяцэхрщцжшцэбвюкцнуубщ

ыквегуаэюрмэшэюпсцэцышхьаоинебгжбщдспшюшэщшлжцяцдшгшэдгщтбаэбщмлыькбдэюпфьфцщцнеьтянкшжшцэхщюыкеоцкэ

ыбфьйцрэкеяугйнчяятысцорвлхвцнаэьзкношилщиявсхйусцаоыбфйцеяуэглщцэроплкмжцплыдьзоцялябтбйшйбйбошфбяо

нрирщхйбхищлгнилтдвнэеуясцащьтюбяюйшэеддгщоцяолшилжцьэфэйугньцхйщцфцплбуьззбпэзяоцчшннйшлншлвлнцхуфц
ьщщдвехьялвлнцяяуопцжрирсзззюжтбчилизнщпщпцшеэсзжоындэыкдллцнештдлэзбпцэвеьюйбнегокшцжьсреяяхифрлнтб
щнцэгитьчзыклшялюбкбьцюикшлнюеиссцжшенмбюшхьшрхршщуыхьцыгщвешлишоштржжвеоцяцпшзбйбошфбяонргттздэсцпэ
бщьэфлоцжбшлоцжббшошболшфеяшецлцппюндльллцжбаэыыроцбиляяцбтрщхйбжддэврдбуозиьзтщдлтриряоуогныишджцмп
нйтбозаювнаопльтбвяшвндьнцплыдюшчшзбфещдзнфещдкцлняоуоилжшябнйохрттбэотьщририрйшозкехьклявйшюебяюбнф
фрнцнйчшкноцтыьзсдкеьнщцздцеэнецуожбуффршдкноцтыьзсдкеьнщцнцлнтщьсьзхвцедлтьпегоьцннинсцаэптдлтоэевэ
ыбжбтщрхптйвмлпныбхимпывчвмлмдоцфйаешлщцтйвниннетысцьцкуйужцюевэвеццьвиршдчэштюкйвхвдэлнбуйвчфэжцнуо
ювмлвэцэйвтыгтоонннлфыезисупыйвэгьцэгцяццшчбаевлябоцкннлшеирыбзцошдхкемлйуэяьщяуфшзбсигцкбцэьюцциэтз
кекеыхьздссолцьцлцрцэеддвлзшрдюжшэефоцявветцидсщсхэфбпнлябжоеирщнгцкбфевлнйяцгцсщмлкбнлфылшыйзбкдги
явщдцеаылшыйщцуфхвмлчгрдхвтыпгапаздлокрддэинцйплфобжупашывушошцбфевлщдгщибдэюпщнквццрлчшеэяячщыклшлн
еназдлуигцжцюшоеяшхвсшышйштщвэбщвехьдэгцшьадгщщплфжцгьцэмэсуукьнзбщнхбтйьннрсзявуежлзщкецэнцжбнйплых
йбплгктыхйцэыбрладщдмэнзсхдбфццшгецвюпчэмэгцкбщхгцэеэяшьтйоцдычшяятрявоышэшвэзшеяутзяусхлшйыяввэяшжш
жесшречимпшшилфыхугбябцшрндрыбтрйввехьюидлцбхьхтгщыхйуяютйтрщхацашыбддаеябфзгщыдыпцхлшхбтйьннрчимпбо
илчуюкинцэншпэефоцбшдицнэшышйшжщбвяшрвьзязфрэястлцлншэйуыбцэщэтыюшйэддвэчэирмшелфрщдяущлезхркноцащез
лнэощцяцгцрегуащузйущззэюшывйээбфцлезшлщяомьсцлцнбньдллцнеюржжцнгнащщдэяхбцэямябзщбижылщвлибцрлианее
уптыкнинцэуппийшилцрнрявьбябтщчууптбылзщбвирчофтвэлнаозщвелнтбцхлшсцтбмьжбйэщцжтэятрсшжнтйдьнцомябиз
явущэфыпфзфрэяжшфеэяцбышуоювмлюбтушщхвюпыэвлтбошахлшщцуфешилтхбщьзцепфцеешилчвдлзбтхооцйыэвлтбошахбщ
ьзощмлябдэнеэшхвццзбмшюшьцннадящгцнназддзбцеддаршлючдладтшжеарупйшцвщдхуупащкемхлшыцлюилузишснтьццре
кеддюшжпсцщшозешгнюбмвезыдешзигцпшщцзвжчцеэяоомбжрэялшюшнцьрщлжцхтдльщзяйшбубщдэыбкнжддэщдрвичдэюпйб
жшщцоиявэснцьщсхьзцеюрьсдшвуйвдэяуашжшхьйианыцспгццэоцсцтлйокбдэылйуяусхбщьзчеефоыкеефьюцбюноочбйбтй
лнгигццэбщжлбштбйэсцщдыбвопльтиношюбщвдлньжбйэяцгцмылиосяунцчьшэыбкняцгцтллцнебищлбшдэчшеэишдэрдоцфй
ысьзшэйыбууюфржкрцеозщацощдхичыхоочкыдащаыешилтдяцгцннащыышэсцюввэшэмхлщжкшэефоцчьмпфьбвьзюцмрунсцфщ
мэнзбивэбихььбпэяуштхвцццэдджшоеяшзбщнлццэнзыкщпчщжыэзешдьгщмбтфцеэятянотрнцмйябиедцощдхзняцгцйбрдюш
чшлнвфйвшлнзуцтсоаыфлщинропуветяуоювмлчшпввеоцкдцецвюпсцзщбицефшщцйшюеьшувьсефижуивлэцзщдэтеезишнбдь
ыхдбнеяшишюнтбхкрддэшшлцишцнтбхкрддэтщчщьзкеезбианкэшлвзирщдыбвоишчйяцгцкдщцугараемцздпшяцинцйыцтйпц
йивэюшкбоебяяомпщнщцыбьвтекебусцлеаелщьзфнплжслцсцбоятюыщлябинфьшшдиюдтюадьзчцщрйвюдтюзщмбтфцешибщэя
тбтбшептттзшжуюпросптлщтблшгнышщцыбьвьлдьжцведлтьпеэяяоюшвдюшчшлнжцйшадэцрфйврдиснцлеосбшвушэщдхушщдд
ншздыбхиоссожцицощжкншйимлгнаэштдцдогннйтбшубврртюдруыйшьнцнэжшщибадмббрьсзщддосжцюевлысупяохбчбаэшт
дцювдссонйсцсибввеэяжцуфзякшйигвунзбщцйшнцыссонйащезяутбэеяячивэюряууяввриржоибильэжшнчсшсхинщццэыб
юбпквеоцяцащяуяушлцеяяэцлесшиейурхыылщрдкшкэбщошцэнцжшфеислшэщяяябудвэеепфшэаэвэшецввлвзезсхдбнбябие
упнциепфбвщдармлтщчщьзэятыяцйбзхьзшшлцишьидсэчешлфжцжцшиангцчьлиангцйбнещдлтгшдэодьшцефрщхйбяцгцсиае
млжцячбутзюраеебйшсцщшозешадзфоцбусхгцвнятюыэцедзбшцкбфевлнйаенцбщукхвюпщцснйрэяшэщищцицащяухьщноцуе
ыгйуццпиьзюшюбдээоцэбнбикьтррдешппрццдюшреисяотбкшцнвопшлнмцсотщчубитьишадмшюшсиюрешаоишинлгрдхвтыпг
апоцтбозбярцяэщхэнювузтыосжшцэсовыбввеяшнцлебншсбщаеьэзбишцнирщхйблняочйувыгжыбуиншллшшеедэсцувэзлннф
бвщдарсшяцщцснйруннбрцфьбвбимэбнашлшоеяшякддьноцйщмлыьрвйэюпоиыбфхбщьзцбщбрцхбщдыбщзсхдбфцюбйбшшоеяу
рхешжеюрирупошодфысуюкшшлцишщцщнтщчщьээятбьиаеьэчфжцеепфмэаесзжощзфпсщсхирщхйбаебищлгнехдбюбмшэдбяжш
жеуяштмпсиыыезццуожбуффршлштыбхьтыдхвэщджшхьоигцьибщлианцэшимэррщджцгцаооцуоюювмлюбцэгвцеэзкношильлчш
цэезсхсцовсзсхяцлцнбюбгнщврдйбжшфшфкрдэятржыйвуоювмлоцаэвэявэоаесшышыцтйкшрнфьзфбуцрирошгчэюрирошябщц
рлжцчвнцнноцшшцэишювузшемлнццещхцеыдсндбхзкнсонйюпуудлябцеираезгсцчпеджцадзфгщуоювмлнцядыбщбнлузяуэя
тыцноцмудлбшхщьзшэбвчуунэщмэяужцэщцнсдсзбвьсцпбрацодичвеоцвдшэанйшхбчбвнзббшоешлхьдэыаинуоювмлсцхииж
оцвэишехдбюбоцыхаещхщоошжчщэхвчианщцфещдвесшкбжоснхьтымлщцтйвнинсцнцазысртжлзщяягьцэюшдыбуфпюбишеэбв

млоыослцкбинсцлцжешеяшзбишыьзбкдшэанзбщнябщциципьзчпеддэгщябщцнуцбнлщщьзшэбвунжцгждхйвцедэбщбиьллбчш
озчехучиьэьлоыезяукшжзсхдбснйшодьзхвюжыцэвелнфеисйодштйябюиыыезрдсцоооцюеэякнзщцежсбщжжупгъдбтбеэце
млтбюбдбхбхбдхгтшщщецвуоюовмлцэйпинзенздцощноцжблцжцощбуцрщхйбзбжшжцсцэокбйэябцндэыаинжшэрсшшэьссшжц
юевэгитьгзыкчйаэжжшщмнзивэгцйолщйуукянзепнашывщиявзбмшэдыыйбоеэяснтьрдпшнцьщсхкдткдэюпчщмлбшиэыбжбчи
вляялшхймшюшинжбдэюпэюйбтыооящнцдьжбдэзщвэрбкьсцтлйокбдэфзяуйутбошилтхбщьзнцадвэшшдийшятбщжцщнсцщцге
биэялшжеезоцрдашжшоцыубщдэыбневццэкедэюплнплрвдлтблнмпшнуоювмлизжоьымлньнэефоцощвлмугщадбямлвбтйгньщ
млхьжрчщонбоинуьйшплхвосзщаещэфльлчшцэлилифькбинлцидаеябцдюрйшбшоешлхьдэыаинвэзгйбошйшштгщсонлсбюбшш
яэьтвещдяшйоившлтбрнсцмбооклябэцошцйньэевцепфешэтеьойбюббшвфжцнеьсбопладтшцйпшепябтттзжцоигщфьыдчэяв
дэвлцнсодтржхбцнчишттюкйвыцснщцюивэыбишжцюещдвнэепюоцейфьчосолещхунжиьзбшрвщхацлшчвзнсцтлябкнеддэжоаэ
ьзкжшэьцлцрццдвэьщжэьшюроцццлнцэдещэцэдещэливэяупэтхрдешцйьсштыбжебиьзьзлплцццлнфцплбутбылвлцврррдбш
оешлхьээыафпафсдцэроижфльтьэиряотэщдмшэдяшхмжцжшжцэщззижлтвлфряусцжшлннцаожоейдноигцжщпфоцвдьзыдсззж
ррирадэноцынцэшитюзиьзсояотэацлнмшюшлцщниныйсзкнцоилюфщэмдмшюшннбшепсцжцаоаэщдэзмдницлшплыдсзшэюпйшяб
ьилитржыйвуоювмлчэацшшхйзщтзоцштьллннйгб

Ключ	Індекс відповідності	Ключ	Індекс відповідності
ьф, мт	0.038244159457100864	вэ, ац	0.040048233953569976
бф, зт	0.03958393866657256	йж, рщ	0.03865725012156717
тэ, юэ	0.03876569080066159	дь, дж	0.03955423197696142
хщ, щщ	0.040239112573337614	кь, цж	0.04005599222971106
дл, яб	0.03881839702502645	эг, кэ	0.03895183937465291
чи, оэ	0.03761391214077616	эф, ат	0.03818902564310479
ье, зн	0.03891277270027803	гф, ьт	0.04528602136328928
юл, дб	0.03860396828316607	ыэ, рэ	0.03762765179755504
си, оэ	0.039217272525466536	ищ, гщ	0.03922250310518747
фе, фн	0.039661171054222094	вл, юб	0.03919282144227353
мг, мц	0.039331644531804315	яи, бэ	0.03737543274287847
зч, ыц	0.03876118599516033	ле, лн	0.0380191444223125
нч, ыц	0.03782035736622042	ыл, гб	0.053404581837675366

Розшифрований текст ключем [ыл, гб]:

мальчикизаулыбалисьисжаромвзялисьзаделоонирвализолотистыецветыцветычтонаводняютвесьмирпереплес
киваютсяслужаекнамощеныеулицытихонькостучатсявпрозрачныеокнапогребовнезнаютугомонуиудержуивс
евокругзаливаютслепящимсверканиемрасплавленногосолнцакаждоелетоониточносцеписрываютсясказалдед
ушкапустьихянепротиввонихсколькостоятгордыекакльвыпосмотришьнанихподольшетакипрожгутутебявгла
захдыркуведьпростойцветокможносказатьсорнаятраваниктоеенезамечаетамыуважаемсчитаемодуванчикблаг
ородноерастениеонинабралиполныемешкиодуванчиковиунесливнизвпогребвывалилиихизмешковивотьмепо
гребаразлилосьсияниевинныйпрессдожидалсяихоткрытыйхолодныйзолотистыйпотоксогрелегодедушкапере
двинулпрессповернулручкузавертелбыстрейбыстрейипрессмягкостиснулдобычунувотвоттаксперватонкойст
руйкойпотомвсещедреeобильнеепобежалпожелобувглиняныекувшинысокпрекрасногожаркогомесяцаемудал
иперебродитьснялипенуиразлиливчистыебутылкиизподкетчупаионивыстроилисьрядаминаполкахпоблескив
аявсумракепогребавиноизодуванчиковсамыеэтисловаточнолетонаязыкевиноизодуванчиковпойманноеизакуп
оренноевбутылкилетоитеперькогдадугласзналпонастоящемузналчтоонживойчтоонзатемиходитпоземлечтоб
ывидетьиощущатьмиронпонялещеоднонадочастицувсегочтоонузналчастицуэтогоособенногоднядняснсбораод
уванчиковтожезакупоритьисохранитьапотомнастанеттакойзимнийянварскийденькогдавалитгустойснегисол

нцаужедавнымдавнониктоневиделиможетбытьэточудопозабылосьихорошобыегосноваспомнитьвоттогдаон
егооткупоритведьэтолетонепременнобудетлетомнежданныхчудесинадовсеихсберечьигдетоотложитьдлясебя
чтобыпослевлюбойчаскогдавздумаешьпробратьсянацыпочкахвовлажныйсумракипротянутьрукуитамрядзаря
домбудутстоятьбутылкисвиномизодуванчиковонобудетмягкомерцатьточнораскрывающиесяназарецветыаск
возьтонкийслойпылибудетпоблескиватьсолнценынешнегоиюнявзглянисквозьэтовинонахолодныйзимнийден
ьиснеграстаетизподнегопокажетсятраванадеревьяхоживутптицылистваицветысловномириадыбабочекзатреп
ещутнаветруидажехолодноесероенебостанетголубымвозьмилетоврукуналейлетовбокалвсамыйкрохотныйко
нечноизкакоготолькоисделаешьединственныйтерпкийглотокподнесиегокгубамипожиламтвоимвместолютой
зимыпобежитжаркоелетотеперьдождевойводыконечноздесьгодитсятолькочистейшаяводадальнихозерсладос
тныеросыбархатныхлуговчтовозносятсяназарекраспахнувшимсянавстречунебесамтамвпрохладныхвысяхони
собиралисьчистоомытымигроздьямиветермчалихзасотнимильзаряжаяпопутиэлектрическимизарядамиэтавод
авобралавкаждуюсвоюкаплюещебольшенебескогдападаладождемназемлюонавпиталавсебявосточныйветери
западныйисеверныйиюжныйиобратиласьвдождьадождьвэтотчассвященнодействияужестановитсятерпкимви
номдуглассхватилковшвыбежалводворилглубокопогрузилеговбочонксдождевойводойвотонаводабылаточно
шелкпрозрачныйголубоватыйшелкеслиеевыпитьонакоснетсягубгорласердцамягкокакласканоковшиполноеве
дронадоотнестивпогребчтобыводапропиталатамвесьурожайодуванчиковструямиречекигорныхручьевдажеба
бушкавкакойнибудьфевральскийденькогдабеснуетсязаокномвьюгаислепитвесьмириулюдейзахватываетдыха
ньедажебабушкатихонькоспуститсявпогребнаверхувбольшомдомебудеткашельчиханьехриплыеголосаистон
ыпростуженнымдетямоченьбольнобудетглотатьаносыунихпокраснеютточновишнивынутыеизналивкивсюду
вдомепритаитсяковарныймикробитогдаизпогребавозникнетточнобогинялетабабушкапрячачтотоподвязаной
шальюонапринесетэточтотовкомнатукаждогоболящегоиразольетдушистоепрозрачноевпрозрачныестаканыи
стаканыэтиосушатоднимглоткомлекарствоиныхвременбальзамизсолнечныхлучейипраздногоавгустовскогоп
олудняедваслышныйстукколестележкисмороженымчтокатитсяпомощенымулицамшорохсеребристогофейер
веркачторассыпаетсявысоковнебеишелестсрезаннойтравыфонтаномбьющейизподкосилкичтодвижетсяполуг
ампомуравьиномуцарствувсеэтовсеводномстаканедадажебабушкакогдаспуститсявзимнийпогребзаиюнемнав
ернобудетстоятьтамтихонькосовсемоднавтайномединенииcосвоимсокровеннымсосвоейдушойкакидедушкаи
папаидядябертидругиетожесловнобеседуястеньюдавноушедшихднейспикникамистеплымдождемсзапахомп
шеничныхполейижареныхкукурузныхзеренисвежескошенногосенадажебабушкабудетповторятьсноваиснова
тежечудесныезолотящиесясловачтозвучатсейчаскогдацветыкладутподпресскакбудутихповторятькаждуюзим
увсебелыезимывовсевременасноваисноваонибудутслетатьсгубкакулыбкакакнежданныйсолнечныйзайчиквот
ьмевиноизодуванчиковвиноизодуванчиковвиноизодуванчиковонииприходилинеслышноуходилипочтибесшу
мнотравапригибаласьираспрямляласьвновьонискользиливнизпохолмамточнотениоблаковэтобежалилетнием
альчишкидугласотстализаблудилсязадыхаясьотбыстрогобегаоностановилсянакраюоврaганасамойкромкенад
пропастьюиоттудананегодохнулохолодомнавостривушиточноолененьонвдругучуялстаруюкакмиропасностьго
родраспалсяздесьнадвеполовиныздеськончиласьцивилизацияздесьживетлишьвспухшаяземляежечасносовер
шаетсямиллионсмертейирожденийиздесьпротореннныеилиещенепротореннныетропытвердятчтобыстатьмужчи
намимальчишкидолжныстранствоватьвсегдавсюжизньстранствоватьдугласобернулсяэтатропаогромнойпыль
нойзмеейскользиткледяномудомугдевзолотыелетниеднипрячетсязимаатабежитксраскаленнымпесчанымберег
амиюльскогоозераавонтакдеревьямгдемальчишкипрячутсямежлистьевточнотерпкиеещенезрелыеплодыдико
йяблониитамрастутизреютавотэтакперсиковомусадуквиноградникукогородныгрядамгдедремлютнасолнцеа
рбузыполосатыесловнокошкитигровоймастиэтатропазаросшаякапризнаяизвилистаятянетсякшколеатапрямая
какстрелаксубботнимутренникамгдепоказываюткковбойскиефильмывотэтавдольручьякдикойлеснойчащедуг
ласзажмурилсяктоскажетгдекончаетсягородиначинаетсялеснаяглушьктоскажетгородврастаетвнееилионапер
еходитвгородиздавнаинавекисуществуетнекаянеуловимаяграньгдеборютсядвесилыиоднанавремяпобеждает
изавладеваетпросекойлощинойлужайкойдеревомкустомбескрайнееморетравицветовплещетсядалековполяхв
округодинокихфермалетомзеленыйприбойяростноподступаетксамомугородуночьзаночьючащилугадальниеп
росторыстекаютпооврагувсеближезахлестываютгородзапахомводыитравигородсловнопустеетмертвеетивнов
ьуходитвземлюикаждоеутроовраrещеглубжевгрызаетсявгородигрозитпоглотитьгаражиточнодырявыелодчон
киипожратьдопотопныеавтомобилиоставленныенамилостьдождяиразедаемыержавчинойэйаусквозьтайныов
рагаигородаивременимчалисьджонхафичарливудменэйдугласмедленнодвинулсяпотропинкеконечноеслихоч
ешьпосмотретьнадвесамыеглавныевещикакживетчеловекикакживетприроданадоприйтисюдаковрагуведьгор
одвконцеконцоввсеголишьбольшойпотрепанныйбурямикорабльнанемполнонародуивсехлопочутбезусталив
ычерпываютводуобкалываютржавчинупоройкакаянибудьшлюпкахибаркадетищекораблясмытоенеслышнойб
урейвременитонетвмолчаливыхволнахтермитовимуравьевраспахнутойовражьейпастичтобыощутитькакмел
ькаюткузнечикиишуршатвжаркихтравахточносухаябумагачтобыоглохнутьподпеленойтончайшейпылиинако
нецрухнутьградомкамнейипотокомсмолыкакрушатсятлеющиеугликостразажженногогромомисинеймолнией
намигозарившейторжестволесныхдебрейтаквотзначитчтотянулосюдадугласатайнаявойначеловекаcприродой
изгодавгодчеловекпохищаетчтотоуприродыаприродавновьберетсвоеиникогдагородпонастоящемудоконцане
побеждаетвечноемугрозитбезмолвнаяопасностьонвооружилсякосилкойитяпкойогромныминожницамионпод

резаеткустыиопрыскиваетядомвредныхбукашекигусеницонупрямоплыветвпередпокаемувелитцивилизациян
окаждыйдомтогоиглядизахлестнутзеленыеволныисхоронятнавекиакоганибудьслицаземлиисчезнетпоследн
ийчеловекиегокосилкиисадовыелопатыизеденныержавчинойрассыплютсявпрахгородчащадомаоврагдугласо
задаченномигаетнокакаяжесвязьмежчеловекомиприродойкакпонятьчтозначатонидругдлядругакогдаонопуст
илглазапервыйлетнийобрядпозадиодуванчикисобраныизаготовленывпрокпораприступатьковторомунодугла
сзастылинедвижетсясместадугпошлидугголосазатихливдалекеяживойсказалдугласночтотолкуониещебольш
еживыечемякакжеэтокакжетаконстоялводиночествеглядянасвоиногиневсилахдвинутьсясместаинаконецпоня
лвтотвечердугласвозвращалсядомойизкиновместесродителямиибратомтомомиувиделихвяркоосвещеннойви
тринемагазинатеннисныетуфлидугласпоспешноотвелглазаноегоногиужеощутилиприкосновениепарусиныиз
аскользилиповоздухубыстрейбыстрейземлязавертеласьзахлопалиполотняныенавесынадвитринамитакойонпо
днялветертаконмчалсяродителиитомшагалинеторопясьамеждунимипятясьзадомшелдугласинесводилглазсте
ннисныхтуфельтампозадивполуночнойвитринехорошаябылакартинасказаламамаагабуркнулдугласстоялиюн
ьдавноминовалотовремякогданалетопокупаюттакиетуфлилегкиеитихиеточнотеплыйдождьчтошуршитпотрот
уарамужеиюньиземляполнапервозданнойсилыивсевокругдвижетсяирастеттраваипосейденьпереливаетсясюд
аизлуговомываеттротуарыподступаеткдомамкажетсягородвотвотчерпнетбортомипокорнопойдетнадноивзел
еномморетравнеостанетсянивсплесканирябидугласвдругзастылточновросвмертвыйасфальтикрасныйкирпич
улицыневсилахтронутьсясместапапвыпалилонвонтамвокнетеннисныетуфлиотецдаженеобернулсяазачемтебе
новыетуфлискажипожалуйстаможешьтымнеобяснитьнуудазатемчтовнихчувствуешьсебятакбудтовпервыевэ
толетоскинулбашмакиипобежалбосикомпотраветочновзимнююночьвысунулногиизподтеплогоодеялаиподст
авилветручтодышитхолодомвоткрытоеокноионистынутстынутапотомвтягиваешьихобратнопододеялоионис
овсемкаксосулькивтеннисныхтуфляхчувствуешьсебятакбудтовпервыевэтолетобредешьбосикомполенивомур
учьюивпрозрачнойводевидишькактвоиногиступаютподнубудтоонипереломилисьидвижутсячутьвпередитебя
потомучтоведьвводевсевидитсянетакпапсказалдугласэтооченьтруднообяснитьаа

Код програми:

```
alphabet = "абвгдежзийклмнопрстуфхцчшщьыэюя"

tpl =("ст","но","то","на","ен")

def text_scan(path):

  with open(path, "r", encoding="utf-8") as f:

    read = f.read()

  i = 0

  length = len(read)

  frequences = {}

  while i + 1 < length:

    bigram = read[i] + read[i + 1]########BIGRAMM INDEXS DO NOT CROSS

    if bigram  in frequences:

      frequences[bigram] += 1 / (length / 2)

    else:

      frequences[bigram] = 1 / (length / 2)

    i += 2

  return(Most_frequent(frequences),read)


def bigram_index(bigram):

  global alphabet

  x = alphabet.index(bigram[0])
```

```
  y = alphabet.index(bigram[1])
  return  ( x * 31 + y )

def Most_frequent(frequences):
  sorted_x = sorted(frequences.items(), key=lambda kv: kv[1],reverse = True)
  return {sorted_x[i][0]:sorted_x[i][1] for i in range(5)}

def gcd(a, b):
  q = []
  if b > a :
    a,b = b,a
  while b:
    q.append( -1 * (a // b))
    a, b = b, a % b
  if a == 1:
    return a,q[:(len(q) - 1)]
  return a
def EvclidAlg(a, b):
  z, zz = 1,0
  while b:
    q = a // b
    a, b = b, a % b
    z, zz = zz, z - zz*q
  return z

def first_part_of_key(params):
  g = gcd(params[1],31 * 31)
  try:## Если длина 1 это значит что g > 1
    if (params[0] % g ) == 0:#Если Y  длится  то пересчитываем(!!!!!!!!!!!!!!!! не забыть потом разделить
Y!!!!!!!!!!!!!!!!!!!! )
      mod = (31 * 31) / g
      gd = gcd(param[1] / g ,mod)
      q = gd[1]
      p = [0,1]
      for i in range(len(q)):
        p.append(q[i] * p[i + 1] + p[i])
```

```
      result = [( ( (p[-1] * (params[0] / g) ) % mod) +( mod * i ) )for i in range(g)]
    else:
      return None
  except Exception:
    gd = gcd(params[1],(31 * 31))
    q = gd[1]
    p = [0,1]
    for i in range(len(q)):
      p.append(q[i] * p[i + 1] + p[i])
    result = [(p[-1]*(params[0])) % (31 * 31)]
  return result
def second_part_of_key(a,Y,X):
  keys = []
  for i in a:
    keys.append( [i,(Y - i * X) % (31 * 31) ])
  return keys

def index_checking(text):
  len_text = len(text)
  index = 0
  frequences = {}
  for element in text:
    if element in frequences :
      frequences[element] += 1
    else:
      frequences[element] = 1
  for element in frequences.values():
    index += (element * element - 1)/(len_text*(len_text -1))
  print(index)
  if (abs(index - 0.0553) < 0.01):
    return True
  return False
def decryption(expeted_bigrams,real_bigrams,text):
  bigrams1= [ bigram_index(expeted_bigrams[i]) for i in range(len(expeted_bigrams))]
  bigrams2= [ bigram_index(real_bigrams[i]) for i in range(len(real_bigrams))]
  equation_params = [(bigrams1[0] - bigrams1[1])% (31 * 31),(bigrams2[0] - bigrams2[1])%(31 * 31)]
```

```
  if first_part_of_key(equation_params) == None:
    return
  keys = second_part_of_key( first_part_of_key(equation_params), bigram_index(expeted_bigrams[0]),
bigram_index(real_bigrams[0]) )
  for i in range(len(keys)):
    try:
      keys[i][0] = EvclidAlg(keys[i][0],961) % 961
    except Exception:
      keys.pop(i)
      i = i - 1
  print(keys)
  decrypted_text = ""
  for key in keys:
    for i in range(0,len(text),2):
      bigram = ((bigram_index(text[i] + text[i + 1]) - key[1]) * key[0]) % 961
      decrypted_text  += alphabet[bigram // 31] + alphabet[bigram % 31]
    if(index_checking(decrypted_text)):
      return(f" Key-pair(a^-1,b): ({key[0]},{key[1]});Decrypted_text:{decrypted_text}" )
def main():
  scan = text_scan("lab3.txt")
  global tpl
  l = list(scan[0].keys())
  for k in l:
    for q in l:
      if k != q:
        for i in tpl:
          for j in tpl:
            if j != i:
              try:
                if (type(decryption([k,q],[i,j],scan[1])) == str):
                  print(decryption([k,q],[i,j],scan[1]))
                  return
              except Exception:
                continue
if name == "main":
  main()
```

Висновок: у ході виконання практикуму було набуто знань з використання афінного шифру та методів його криптоаналізу. Було набуто навичок аналізу тексту на його інформативність за допомогою статистичних даних, розглянуто декілька моделей на основі яких проводився аналіз.