

## Міністерство освіти і науки України НТУУ «Київський політехнічний інститут»

Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

### Перевірив:

Чорний О. М.

**Виконав**: Студент III курсу ФТI

групи ФБ-71

Поліщук Володимир

Київ - 2019

**Результати:**

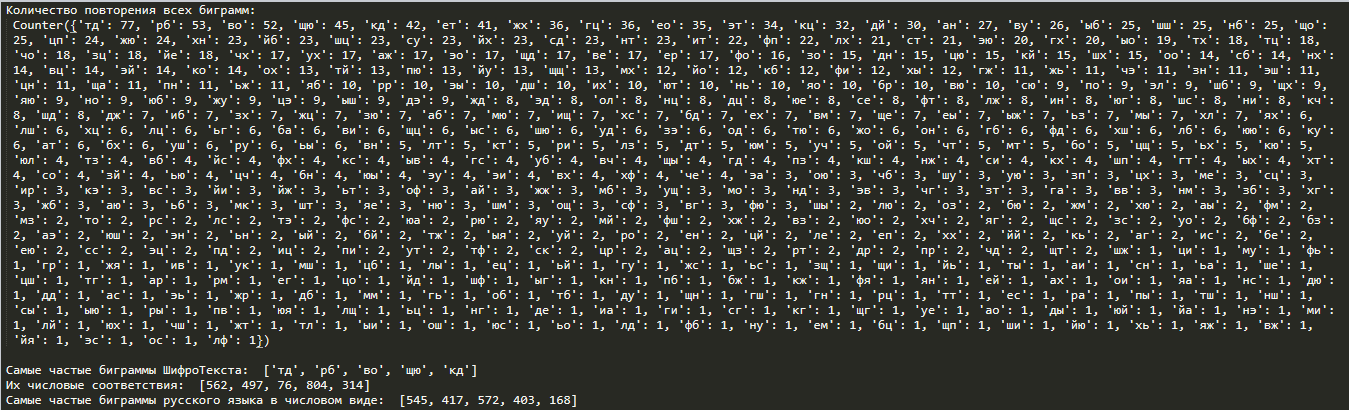
**ЗАШИФРОВАННЫЙ ТЕКСТ**

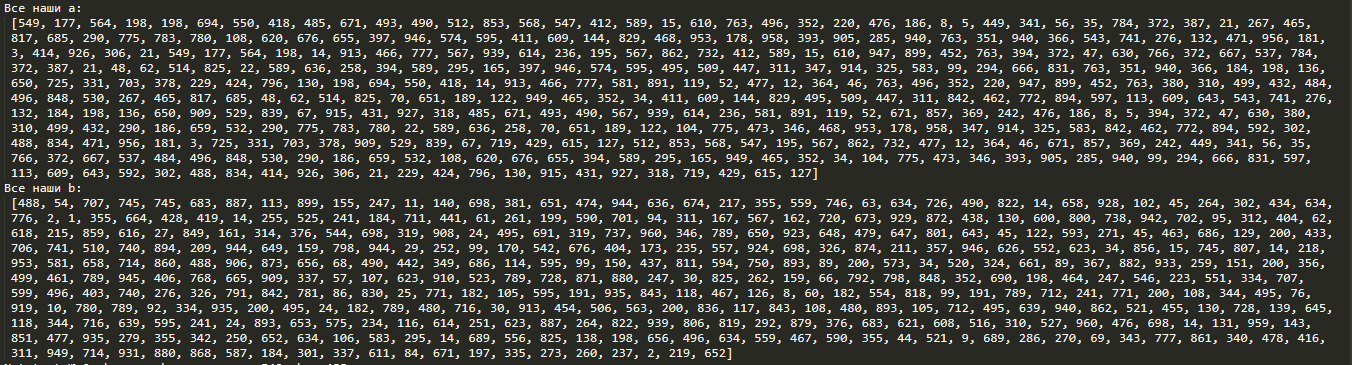
кдяхэаюлтдооэтсювнкцябпосбанвооюрретлтцпвоэыохтдшылхщютзгжантзкцхнлюкднхцпвоыомхзотхэтоовцлшвуджозчхйбжьктибэлтцеовбдшйсвцхндншбчбоювнкцябухбюхцхнрбчэшжцюлцлхйостщюшужхриажгцфхзхжцитвожюфпксщхибухкйзюжмьгнхщюзншбхюэотйбавотдцюэшшылхщюабпоябцикбкцывкцхнрбвофишбтдтхыбэляюждзютдлзщюаыпюнозоуюмхэшухэозоихщюкцзоюбзюгсвичхшццнщащцжхщюфмкдвощхщюйуажмздшшшкдысэтмуфьанэйсужушюстлхэдвоэомюфожхетжютдцюгршшкдэйолнойхзозпцэкдютэтнцхыдйщюэтжцтйнбщддцывкцхнцхеоцэвбйбышкдэйюейосежхюбгцэюубйутодткдвощхщющцяюстудвежюнхэджядшищвччощщвунойхзозпцэфтмефпшхтдпощщщыкдвуозеойбдэзэстсдоожмиврбгхнойхзозпцэцэфпэтщощюэоеохсгдюмлзсдвеньрстднтщюфпвцукеоетитмшпнчхшцабшшлсцбухкйэыбдтджюзнхыохнхлхыбэлфошхэдохехвоубпзшбчхлыйбсуодмзеоэотэкшфстднтщюфпкдютэтнцхыдйщюэтвцтйсдлжюасцгцеокочэкдютетэтфтщютздйирэттднттюрюецтйвмшшзцтйищцюеокцфпжюэддйкцвмчоьйнбрбйеинухяуюгкцхнрбвотдмйбарбфшкдэтзэстсдвекдихктщюжонжсиодгуоддйучяожстднтжхщюжощщщыгцщоцпьсждьггжнбгхгцитсдвеоонжзцэюехлцбретйхцпвоыойбщеьжкхшцжосбанолхжжоойераннбйейсвцхндншбчбжуэтихшцвзеокэхытцажшбэйчтцпчээыкояхлцюоцэвбхчшсшпвситуберончхфоыойиеыаншшвуйжышьтджфицхеогбшшанжхтдпнягвофихыыжжхщюзнбрщюэтудмтцпжхофгхгцзоюбрбйекцяюайбарбэтпюцпжхдйержюкшйбтдщдзщяоыбэлгтфдэйетзэстйуэлетмюшюыхнцхтцпвотдучеощищынийькосотыкддйсуюгкцхнрбвотдьздйирэттднттющсзйэысесдвейхаирбтюзсжжйбщддццнтдэййбюгрбтдтхыбгцэюболхсджькдрбнхцщйеэотдднщддцбаабжукцеочтйхвюеыдйрббдфхдйыжхшшшщаышиткчсняощщуогбажбфьащелбхшзцтйищцюнхктсдждайершецшмбзнбрфоюболохехвоаыйбсучхбзеойбйотгрбарбдкбзцбаююэттдвюкостщюьхджяормлзсдцэфпкчшюкэфощщвуэтегрбьюетитщоойышцчшцабдншдкцжхщюцодтэоаэстжхетжютдхшкдыспнкчнжрбвотдбнкдютрртхтдетмыпюнозоуюмхэшюентлбущфскуодвюстсдвейдвугдпоябрбднтцэющощщтокшеронцчшццнджфитджюкцтйвмщыдйфиибшфжхмоатсбгцфпюшзцтйищгхэнкчнжрбвотдыгзнкдютооюывющючтсдвеэткнгстйрбмежоатсбгцфпбхьньзвоыоэозэстщоеонтмыгцндтцоохлсбанднбрыйэвчхшцлшеочгзнжхпбхлхызцвотдтцтйвмбхохйощщжунхктсджхетжютдхшкдысжхкйгхбжйуолэттднттюзсзтсбшшшшушпзкцхнышбйшдшшущрбкжгажюррщазюфяшшеокояншдкцмеввнмжхетжютдхшкдысбхьнэлжхэоейфитдтхыбэлтднтзбшшернбйедшзцтйищцюджфицхяберстфпвоэуажкбруатеоахщюмхэшухжцлжрбгхкйпнвопюшцлшшшэтихшцтжбфоилсуюыяшшеокояащелбучиххцхнрбвонстднбансюуйщодэнтихыбюешюыхнцхтцпетщцжжйбвотддцитвожюшцбдшшсущантсофогбсурржцзожюдюяюэоддтххгнхщюжбзнкофтжджцжжйбвотдромхжюгбгцлхкссдкйрретфпасйотдухвцщоыояоетктйхэдетэьвугцышшсажкбгцфпкйщеьжкхшццнйовныжрбвоенэизнеожретмхщюдшшшухсугждннььгррщюцйюгдткуюгаюетмютхыойотднтыбгцэюжхюбвукдвощхщюдшчобхдбдшжуьжгажюпнньхыохзйзцвоьыйбсунбцюэозоихщюмолесбсуммяюепдэйхсбрбвогьвугцышшсажкбгцфпюшшшетждрсэтзэстудобжьлзтцлхыбвхкйсудйхюххыокйзювнфирбюлчозтлхтбйбьзньйбйужькюдурбщдфхгжеыникоьбгцэюйбрбднтцэюлжгажющощщкющанмжюйорршхжхщюфмэощняюабгххсййбргшзцтйищцюжхинфиывйугнрцнмттетяюххаюитйхкчэоэтесшцраирушжцчэмюсуажандйщеябруеыохпыыжкьцчгдзюшхыбфшвуйжышэшзцтйищцювснхеокшзожххцлжкбьхвцньйбгцшхщстхвюфпгдхыпюнонбажщдьзкцсюмотэшцитжюэюшхыбмкэюцнлхщюцнжхвцлшжьгцвужхщюююетнобюхнщютшкчншкчбохсжхыйбркююышдчхагьхыовцислтсдшшетзэстйуолсылжэыпюшбхфньхытцодгжабйбхфйужцбретщюудшшйсвишдбеьжрбйеооьжзцэющоеоаэзбвмнищдвеетштехлцбретйхцпетмыпюеюмхэшюеыюлбссэтфтыбрудэщхжхтцмхрыонцчшццнйиеыанвущоьылхнцэыгцлхэцхнйедэйхсбрбйежхетжютддшкдысводэяеьжкхшцбдлзеоушйбяхщоцщанкдьгнхтдьжрбгхчощщвуфтоознончххнетщхяеэотдщеыбухшхтдмкеокдьгнхтдьжрбгхооюывющючтсдвеетнюяевокйфитдднсесдчобоэнжхфочовсрюхцитцщвчкйкдпнгцеопвхчгцитцпвохсчонххгнбвчетщхыошучберончхпджьмтждкюхцитцщвчетнюицтхшмююкйеытцончхшхжбзцлхгбущдйнищдгждцщоыоьжйещюаблюстюбхлнююямбощцюкцяюкдлщцэьцайанетпюцптдтхнгкцеоубхфкцтхшммыдйрбсучхеоябньмкэюэтмхтдстпнньпоябсфрбцюдесбанднбрщюэтсдатлцпнвотдхшкдэйолэтзйеретхжвгажщаиашдбншдкцжхыболиндйчетдажгцситцэюмхэшсущцитвожюшцшуерюмтцшцсюпдухтдбнгцвотхинухчгрбтдтхыбхызцпюибруибхфйуцнбрщюэтсдбоцпштмыкдохьбгцфпибшшернбцюйекдлттдяогичхшцбалшшшитщооозннтюыэйсгрбгхшсшпцэкдлттдкгрбвмнищдрианлххнэйрбгхщгкцеощофоойэврбцюсбсуиндйчечолбнбгхжючээтвиюеэтнтцнсесдветхшпоосбанкцоохлэттднттюхлдшшшитщостжошсзхтдьжрбгхмюлбпзажкбжьхызцпюибжьпоябсфрбйещощщкюшсшпдтушйбяхщоцщаняюепмтцпжхофюекйухощйекдютвоэуажкбвхцнлхщюмыкотцноуеьюэывюаоэумйаннбцючотхтдэиыжюбдыюмнищдкбуофюьтыбвхпикцутвоэуажкбвхетшхзхжхриажгцсстднбанщдюйерййнбьзрбйешхвимбсурржутзчхшцвзеоетйаыжтфюекоцппикцбнщожхвбвущджьэывюфюнэстсдвеатлцпнчэсклхшхэджудэйхсбрбвочгрбтдтхыбгцэюгхзхэтнцислтжбэлгтфдэйсуьхцретмхщюбеьжкхшцтжпнгсштввюлтднтнойхтюмихлтджюйхцпвотдяочоехыбйбзцлждцхнрбчэскеокдвопюшцлшйотдухвцщохсгтфдньзюэшкчаюйхцпвоыойсвцхндншблйднвоэтсючтсоеютдэшжьпоойерягррщюкэиннисуюхыогцщарбвоуйщодэнтихыбвучшвуэожхэдюгрбтдтхыбгцэюйотдухвцщоыофоюбпокйфигжщддцлхксввсущантсофочоехыбгцлжкбюешюыхнцхтцпетмыохцйзцэозоихыбгцфптцэочоьбгцфпчочобоацлжолфтьюжтфпвекдфтжюпюфотдяобзохвнщзтлвошскоооыокдютждкдртнтфддйшюыхнцхтцпвотдсуыищаднсейузйнбьхдретыбрущоьыйбрбитшхыошсзхтдстнтыбюлпюьыеоьывюатошанкудйэюфоюбэйзцкуодвюстфпэтщоеовикцхнлхщюкцооньщечощщвуйоюсзхыбухушпзкцхнрбшшернбйечотдэййбсцтхшмбдпрвмкдгжэащдрощщсиюасцитфпкдьоицжувундэыдйлдюойхфбпойхнудйхнэлщащзчэяуемнбррмютддйьзкцсюбцсучдвуандшеохсихйхбхщпйхлеэапнчхеойхшисеетщхыощцсучдвукудйэюцнсесдверианлххнэйрбгхыянбитйюсуюгэшжььггжнбйеяогбанохшхыбвуерюмтцшцсюьыгцохэцхнвуетэтфтщюбдухтддцситцэюмхэшсурианлххнэйрбгхфодтююиндйчехьнтудкоцпкдютэиажтфзнщазхфоябсфрбгхшхвияжьзвотдучяоехфдвукдюткйтцюмнтжхщюгхыочонххгнбйебхохвжанкдвощхщюйувгксююиндйчевостююхцяхщюкоушнбднеокоацяхжхитсюоюйянбэюцпчэдйщтощцюйиеыаншшвуйжышьтфоэсцркьзозбндфхджэихлтджюйхцпвотдкбфичхэюенмтцпжхофйуфюьювортнтфддйкдютгцитсдвейхагкцжуружхеогсослфчхшцщцыомтмюитсюфоойервукйниыжзтсдгцитстфпвешбрбднтцфпйотдухвцщоыощощщюггжнбгхкудйэюждвудрзохскдыстднбанщдвехызцчэшхджщдшшгхдэйхсбрбчэвггжнбйегцывкцхнсеудвеетнхлхгтэдерйетдажбйщтцпвотдучвцйудйпрэвщдшдэыдйут

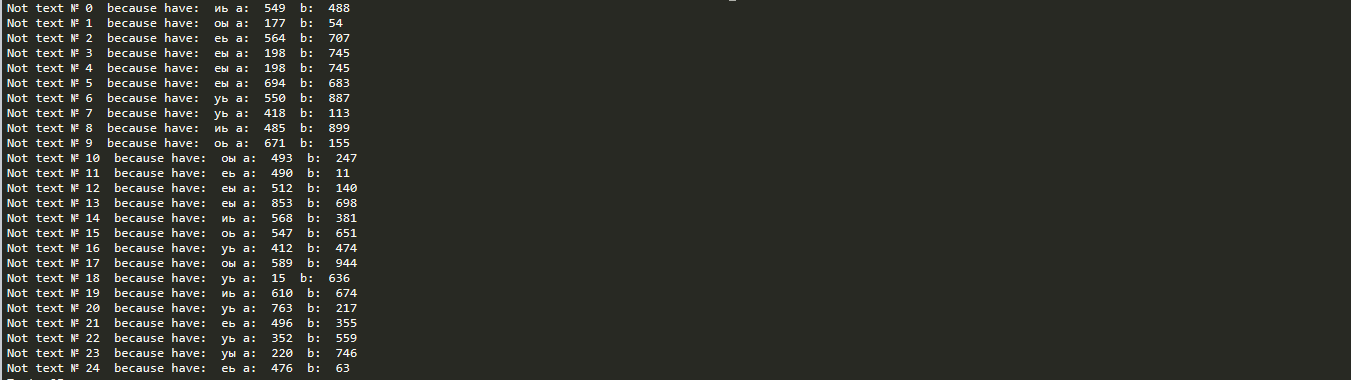
### РАСШИФРОВАННЫЙ ТЕКСТ

*отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотдельногочеловекавовсякомслучаеоноглавныйисточникчувствавинынеизвестноединственныйлиисследованиямнеудалосьещеустановитьдушевноепроисхождениевиныипотребностиискупленияноотнюдьнесущественноединственныйлиэтоисточникпсихологическоеположениесложноинуждаетсявобясненияхотношениемальчикакотцукакмыговоримамбивалентнопомимоненавистииззакоторойхотелосьбыотцакаксоперникаустранитьсуществуетобычнонекотораядолянежностикнемуобаотношениясливаютсявидентификациюсотцомхотелосьбызанятьместоотцапотомучтоонвызываетвосхищениехотелосьбыбытькаконипотомучтохочетсяегоустранитьвсеэтонаталкиваетсянакрупноепрепятствиевопределенныймоментребенокначинаетпониматьчтопопыткаустранитьотцакаксоперникавстретилабысостороныотцанаказаниечерезкастрациюизстрахакастрациитоестьвинтересахсохранениясвоеймужественностиребенокотказываетсяотжеланияобладатьматерьюиотустраненияотцапосколькуэтожеланиеостаетсявобластибессознательногооноявляетсяосновойдляобразованиячувствавинынамкажетсячтомыописалинормальныепроцессыобычнуюсудьбутакназываемогоэдиповакомплексаследуетоднаковнестиважноедополнениевозникаютдальнейшиеосложненияеслиуребенкасильнееразвитконституционныйфакторназываемыйнамибисексуальностьютогдаподугрозойпотеримужественностичерезкастрациюукрепляетсятенденцияуклонитьсявсторонуженственностиболеетоготенденцияпоставитьсебянаместоматерииперенятьееролькакобекталюбвиотцаодналишьбоязнькастрацииделаетэтуразвязкуневозможнойребенокпонимаетчтоондолженвзятьнасебяикастрированиееслионхочетбытьлюбимымотцомкакженщинатакобрекаютсянавытеснениеобапорываненавистькотцуивлюбленностьвотцаизвестнаяпсихологическаяразницаусматриваетсявтомчтоотненавистикотцуотказываютсявследствиестрахапередвнешнейопасностьюкастрациейвлюбленностьжевотцавоспринимаетсякаквнутренняяопасностьпервичногопозывакотораяпосутисвоейсновавозвращаетсяктойжевнешнейопасностистрахпередотцамделаетненавистькотцунеприемлемойкастрацияужаснакаквкачествекарытакиценылюбвиизобоихфактороввытесняющихненавистькотцупервыйнепосредственныйстрахнаказанияикастрацииследуетназватьнормальнымпатогеническоеусилениепривноситсякаккажетсялишьдругимфакторомбоязньюженственнойустановкиярковыраженнаябисексуальнаясклонностьстановитсятакимобразомоднимизусловийилиподтвержденийневрозаэтусклонностьочевидноследуетпризнатьиудостоевскогоионалатентнаягомосексуальностьпроявляетсявдозволенномвидевтомзначениикакоеимелавегожизнидружбасмужчинамивегодостранностинежномотношенииксоперникамвлюбвиивегопрекрасномпониманииположенийобяснимыхлишьвытесненнойгомосексуальностьюкакнаэтоуказываютмногочисленныепримерыизегопроизведенийсожалеюноничегонемогуизменитьеелиподробностионенавистиилюбвикотцуиобихвидоизмененияхподвлияниемугрозыкастрациинесведущемувпсихоанализечитателюпокажутсябезвкуснымиималовероятнымипредполагаючтоименнокомплекскастрациибудетотклоненсильнеевсегоносмеюуверитьчтопсихоаналитическийопытставитименноэтиявлениявневсякогосомненияинаходитвнихключклюбомуневрозуиспытаемжееговслучаетакназываемойэпилепсиинашегописателянонашемусознаниютакчуждытеявлениявовластикоторыхнаходитсянашабессознательнаяпсихическаяжизньуказаннымвышенеисчерпываютсявэдиповомкомплексепоследствиявытесненияненавистикотцуновымявляетсяточтовконцеконцовотождествлениесотцомзавоевываетвнашемяпостоянноеместоэтоотождествлениевоспринимаетсянашимянопредставляетсобойвнемособуюинстанциюпротивостоящуюостальномусодержаниюнашегоямыназываемтогдаэтуинстанциюнашимсверхяиприписываемейнаследницеродительскоговлияниянаиважнейшиефункцииеслиотецбылсуровнасильственжестокнашесверхяперенимаетотнегоэтикачестваивегоотношениикясновавозникаетпассивностькоторойкакразнадлежалобыбытьвытесненнойсверхясталосадистическимястановитсямазохистскимтоестьвосновесвоейженственнопассивнымвнашемявозникаетбольшаяпотребностьвнаказанииияотчастиотдаетсебякактаковоевраспоряжениесудьбыотчастиженаходитудовлетворениевжестокомобращенииснимсверхясознаниевиныкаждаякараявляетсяведьвосновесвоейкастрациейикактаковаяосуществлениемизначальногопассивногоотношениякотцуисудьбавконцеконцовлишьдальнейшаяпроекцияотцанормальныеявленияпроисходящиеприформированиисовестидолжныпоходитьнаописанныездесьанормальныенамещенеудалосьустановитьразграничениямеждунимизамечаетсячтонаибольшаярольздесьвконечномитогеприписываетсяпассивнымэлементамвытесненнойженственностииещекакслучайныйфакторимеетзначениеявляетсяливнушающийстрахотецивдействительностиособеннонасильственнымэтоотноситсякдостоевскомуфактегоисключительногочувствавиныравнокакимазохистскогообразажизнимысводимкегоособенноярковыраженномукомпонентуженственностидостоевскогоможноопределитьследующимобразомособенносильнаябисексуальнаяпредрасположенностьиспособностьсособойсилойзащищатьсяотзависимостиотчрезвычайносуровогоотцаэтотхарактербисексуальностимыдобавляемкранееузнаннымкомпонентамегосуществараннийсимптомприпадковсмертиможнорассматриватькакотождествлениесвоегоясотцомдопущенноевкачественаказаниясосторонысверхятызахотелубитьотцадабыстатьотцомсамомутеперьтыотецноотецмертвыйобычныймеханизмистерическихсимптомовиктомужетеперьтебяубиваетотецдлянашегоясимптомсмертиявляетсяудовлетворениемфантазиимужскогожеланияиодновременномазохистскимпосредствомнаказаниятоестьсадистическимудовлетворениемобаяисверхяиграютрольотцаидальшевобщемотношениемеждуличностьюиобектомотцаприсохраненииегосодержанияперешловотношениемеждуяисверхяноваяинсценировканавторойсценетакиеинфантильныереакцииэдиповакомплексамогутзаглохнутьеслидействительностьнедаетимвдальнейшемпищинохарактеротцаостаетсятемжесамымнетонухудшаетсясгодамитакимобразомпродолжаетоставатьсяиненавистьдостоевскогокотцужеланиесмертиэтомузломуотцустановитсяопаснымеслитакиевытесненныежеланияосуществляютсянаделефантазиясталареальностьювсемерызащитытеперьа*

**Скриншоты выполнения програмы:**



****

****

**Код:**

**import re**

**import codecs**

**import string**

**from collections import Counter**

**alphab = ['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о',' п', 'р', 'с', 'т', 'у', 'ф',' х', 'ц', 'ч', 'ш', 'щ', 'ы', 'ь', 'э', 'ю', 'я']**

**def find\_text():**

**text0 = ''**

**decardline = []**

**k = 0**

**text = re.findall(r'[а-я\n]', codecs.open ("text.txt", 'r', 'utf-8').read()) #Открытие файла**

**for i in range(0, len(text)):**

**text0 = text0 + text[i] #Запись в list meh**

**text = text0.replace('\n', '') #Удаление символа конца строки**

**for i in range(1, len(text)):**

**if i%2 != 0 : #Выбираем биграммы**

**for j in range (0, 31):**

**if text[i-1] == alphab[j]: #Находим числовое соответствие а**

**a = j**

**if text[i] == alphab[j]: #Находим числовое соответствие b**

**b = j**

**decardline.insert(k, (a \* 31) + b) #Считаем "значение" биграммы**

**k = k + 1 #Увеличиваем порядок номера записи элементов**

**return text, decardline**

**def bigrams(ourtext):**

**newtext = ''**

**a = 100**

**ourСommon = ['', '', '', '', '']**

**innum = []**

**newtext = re.findall(r'[а-я][а-я]', ourtext) #Поиск биграмм**

**count = Counter(newtext)**

**print('Количество повторения всех биграмм: \n', count)**

**for i in range(0, 5):**

**if i < 5:**

**a, ourСommon[i], num = the\_best(a, newtext, ourСommon)**

**innum.insert(i, num)**

**print('\nСамые частые биграммы ШифроТекста: ' , ourСommon)**

**print('Их числовые соответствия: ', innum)**

**return(innum)**

**def the\_best(best, ourtext, some):**

**c = 0**

**bigrama = ''**

**сount = Counter(ourtext)**

**for i in range (0, 31):**

**for j in range (0, 31): #Перебор всех Биграмм для определения самых частых**

**if сount[alphab[i] + alphab[j]] > c and сount[alphab[i] + alphab[j]] <= best:**

**if alphab[i] + alphab[j] != some[0] and alphab[i] + alphab[j] != some[1] and alphab[i] + alphab[j] != some[2] and alphab[i] + alphab[j]!= some[3] and alphab[i] + alphab[j] != some[4]:**

**c = сount[alphab[i] + alphab[j]]**

**bigrama = alphab[i] + alphab[j]**

**innum = (i \* 31) + j**

**return(c, bigrama, innum)**

**def egcd(a, b): #Поиск обратного**

**if a == 0:**

**return b, 0, 1**

**else:**

**gcd, x, y = egcd(b % a, a)**

**return gcd, y - (b//a) \* x, x**

**def inverse(a, m): #Поиск обратного**

**g, x, y = egcd(a, m)**

**if g > 1:**

**return x % (m/g)**

**else:**

**return x % m**

**def formula(top, ourtop): #Поиск возможных ключей (a и b)**

**A = []**

**B = []**

**k = 0**

**for i in range (0, 5): #Перебор пар Х\***

**for j in range (0, 5): #Перебор пар Y\***

**for u in range (0, 5): #Перебор пар Х\*\***

**for y in range (0, 5): #Перебор пар Y\*\***

**a = ((top[j] - top[y]) \* inverse(ourtop[i]-ourtop[u], 961))%961 #а = ((Y\* - Y\*\*) \* inverse(X\* - X\*\*, 961)) % 961**

**b = (top[j] - (a \* ourtop[i]))%961 #b = (Y\* - (a \* X\*)) % 961**

**if a != 0.0:**

**A.insert(k, int(a)) #Записываем а**

**B.insert(k, int(b)) #Записываем b**

**k = k+1 #Увеличиваем порядок номера записи элементов**

**print('Все наши а: \n', A, '\nВсе наши b: \n', B)**

**return A, B**

**def decrypt(a, b, ST):**

**baddd = ['аы' ,'оы', 'еы', 'уы', 'оы', 'аь', 'оь', 'еь', 'иь', 'уь'] #Запрещенные биграммы**

**for i in range (0, len(a)): #Перебор всех ключей**

**check = 0**

**textnew = ''**

**for j in range (0, len(ST)): #Перебор всех биграмм в циврофом виде**

**if check == 1:**

**break**

**x = ((ST[j] - b[i]) \* inverse(a[i], 961))%961 #X = ((Z - b) \* inverse(a, 961)) % 961**

**#print(x, inverse(a[i], 961))**

**x1 = int(x//31) #x1 = X/31**

**if x1 != 0:**

**x2 = int(x % (31 \* x1)) #x2(x%(31 \* x1))**

**textnew = textnew + alphab[x1] + alphab[x2] #Запись расшифрованных биграмм**

**for k in range(0, 10):**

**if alphab[x1] + alphab[x2] == baddd[k]: #Проверка на подлинность биграммы**

**ploho = alphab[x1] + alphab[x2]**

**check = 1 #Идентификатор "плохого" текста**

**if check == 0:**

**print('Text ', i, ': \n', textnew, '\n')**

**else:**

**print ('Not text №', i, ' because have: ', ploho, 'a: ', a[i], ' b: ', b[i])**

**text, decardline = find\_text()**

**print(text)**

**#print(decardline)**

**common = [545, 417, 572, 403, 168]**

**ourСommon = bigrams(text)**

**A, B = formula(common, ourСommon)**

**decrypt(A, B, decardline)**