Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз афінної біграмної підстановки Варіант – 3

Виконали:

студенти III курсу ФТІ групи ФБ-96
Шидлюх Максим та Шафрай Ілля

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Мета роботи

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

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.
2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ шляхом розв'язання системи (1).) ,(ba
4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Виконання

1)п'ять найчастіших біграм шифртексту:

```
Popularni bigrami ['ст', 'но', 'то', 'на', 'ен']
Popularni bigrami shifru ['тд', 'рб', 'во', 'щю', 'кд']
```

2) опис роботи запропонованого вами автоматичного розпізнавача російської мови

```
def check(text):
    popular=dict(Counter(text).most_common())
    if 'о' in popular and (popular['о']/len(text))<0.07:
        return 0
    if 'а' in popular and (popular['а']/len(text))<0.06:
        return 0
    if 'е' in popular and (popular['е']/len(text))<0.06:
        return 0
    if 'ф' in popular and (popular['ф']/len(text))>0.01:
        return 0
    if 'щ' in popular and (popular['щ']/len(text))>0.01:
        return 0
    if 'ь' in popular and (popular['ь']/len(text))>0.02:
        return 0
    return 1
```

В нашому тексті ми перевіряємо відсоток самих популярних та не популярних літер в російській щоб отримати коректний розшифрований текст. Перевіряються такі літери як :

Шифрований текст(Варіант 3)

кдяхэаюлтдооэтсювнкцябпосбанвоюрретлтцпвоэыохтдшылхщютзгжантзкцхнлюкднхцпвоы
омхзотхэтоовцлшвуджозчх
йбжькгибэлтцеовбдшйсвцхндншбчбоювнкцябухбюхцхнрбчэшжцюлцлхйостщюшужхриажгцфхз
хжцитвожюфпксщхибуххйзю
жмьгнхщюзншбхюэотйбавотдцюэшшылхщюабпоябцикбкцывкцхнрбвофишбтдтхыбэляюждзютдл
зщюаыпюнозоуюмхэшухэозо
ихщюкцзоюбзюгсвичхшццнщащцжхщюфмкдвощхщюйуажмздшшшкдысэтмуфьанэйсужушюстлхэдв
оэомюфожхетжютдцюгршшкд
эйолнойхзозпцэкдютэтнцхыдйщюэтжцтйнбщддцывкцхнцхеоцэвбйбышкдэйюейосежхюбгцэюу
бйутодткдвощхщющцяюстуд
вежюнхэджядшищвччощщвуноййхзозпцэфтмефпшхтдпощщщыкдвуозеойбдээзстсдоожмиврбгхн
ойхзозпцэцэфпэтщощюэоео
хсгдюмлзсдвеньрстднтщюфпвцукеоетитмшпнчхшцабшшлсцбухкйэыбдтджюзнхыохнхлхыбэлф
ошхэдохехвоубпзшбчхлыйб
суодмзеоэотэкшфстднтщюфпкдютэтнцхыдйщюэтвцтйсдлжюасцгцеокочэкдютетэтфтщютздйи
рэттднттюрюецтйвмшшзцтй
ищцюеокцфпжюэддйкцвмчоьйнбрбйеинухяуюгкцхнрбвотдмйбарбфшкдэтзэстсдвекдихктщюж
онжсиодгуоддйучяожстднт
жхщюжощщщыгцщоцпьсждьггжнбгхгцитсдвеоонжзцэюехлцбретйхцпвоыойбщеьжкхшцжосбано
лхжжоойераннбйейсвцхндн
шбчбжуэтихшцвзеокэхытцажшбэйчтцпчээыкояхлцюоцэвбхчшсшпвситуберончхфоыойиеыанш
швуйжышьтджфицхеогбшшан
жхтдпнягвофихыыжжхщюзнбрщюэтудмтцпжхофгхгцзоюбрбйекцяюайбарбэтпюцпжхдйержюкшй
бтдшдзщяоыбэлгтфдэйетзэ
стйуэлетмюшюыхнцхтцпвотдучеощищынийькосотыкддйсуюгкцхнрбвотдьздйирэттднттющсз
йэысесдвейхаирбтюзсжжйб
щддццнтдэййбюгрбтдтхыбгцэюболхсджькдрбнхцщйеэотддншддцбаабжукцеочтйхвюеыдйрбб
дфхдйыжхшшшщаышиткчсняо
щщуогбажбфьащелбхшзцтйищцюнхктсдждайершецшмбзнбрфоюболохехвоаыйбсучхбзеойбйот
грбарбдкбзцбаююэттдвюко
стщюьхджяормлзсдцэфпкчшюкэфощщвуэтегрбьюетитщоойышцчшцабдншдкцжхщюцодтэоаэстж
хетжютдхшкдыспнкчнжрбво
тдбнкдютрртхтдетмыпюнозоуюмхэшюентлбущфскуодвюстсдвейдвугдпоябрбднтцэющощщток
шеронцчшццнджфитджюкцтй
вмщыдйфиибшфжхмоатсбгцфпюшзцтйищгхэнкчнжрбвотдыгзнкдютооюывющючтсдвеэткнгстйр
бмежоатсбгцфпбхьньзвоыо
эозэстщоеонтмыгцндтцоохлсбанднбрыйэвчхшцлшеочгзнжхпбхлхызцвотдтцтйвмбхохйощщж
унхктсджхетжютдхшкдысжх
кйгхбжйуолэттднттюзсзтсбшшшшушпзкцхнышбйшдшшущрбкжгажюррщазюфяшшеокоянщдкцмев
внмжхетжютдхшкдысбхьнэл
жхэоейфитдтхыбэлтднтзбшшернбйедшзцтйищцюджфицхяберстфпвоэуажкбруатеоахщюмхэшу
хжцлжрбггххйпнвопюшцлшшш
этихшцтжбфоилсуюыяшшеокояащелбучиххцхнрбвонстднбансюуйщодэнтихыбюешюыхнцхтцпе
тщцжжйбвотддцитвожюшцбд
шшсущантсофогбсурржцзожюдюяюэоддтххгнхщюжбзнкофтждхцжжйбвотдромхжюгбгцлхкссдк
йрретфпасйотдухвцщоыояо
етктйхэдетэьвугцышшсажкбгцфпкйщеьжкхшццнйовныжрбвоенэизнеожретмхщюдшшшухсугжд
ннььгррщюцйюгдткуюгаюет
мютхыойотднтыбгцэюжхюбвукдвощхщюдшчобхдбдшжуьжгажюпнньхыохзйзцвоьыйбсунбцюэоз
оихщюмолесбсуммяюепдэйх
сбрбвогьвугцышшсажкбгцфпюшшшетждрсэтзэстудобжьлзтцлхыбвххйсудйхюххыокйзювнфир
бюлчозтлхтбйбьзньйбйужь
кюдурбщдфхгжеыникоьбгцэюйбрбднтцэюлжгажющощщкющанмжюйорршхжхщюфмэощняюабгххсй
йбргшзцтйищцюжхинфиывйу
гнрцнмттетяюххаюитйхкчэоэтесшцраирушжцчэмюсуажандйщеябруеыохпыыжкьцчгдзюшхыбф
швуйжышэшзцтйищцювснхео
кшзожххцлжкбьхвцньйбгцшхщстхвюфпгдхыпюнонбажщдьзкцсюмотэшцитжюэюшхыбмкэюцнлхщ
юцнжхвцлшжьгцвужхщююует
нобюхнщютшкчншкчбохсжхыйбркююышдчхагьхыовцислтсдшшетзэстйуолсылжэыпюшбхфньхыт
цодгжабйбхфйужцбретщюуд
шшйсвишдбеьжрбйеооьжзцэющоеоаэзбвмнищдвеетштехлцбретйхцпетмыпюеюмхэшюеыюлбссэ
тфтыбрудэщхжхтцмхрыонцч
шццнйиеыанвущоьылхнцэыгцлхэцхнйедэйхсбрбйежхетжютддшкдысводэяеьжкхшцбдлзеоушй
бяхщоцщанкдьгнхтдьжрбгх

```
чощщвуфтоознончххнетщхяеэотдщеыбухшхтдмкеокдьгнхтдьжрбгхооюывющючтсдвеетнюяев
окйфитдднсесдчобоэнжхфо
човсрюхцитцщвчкйкдпнгцеопвхчгцитцпвохсчонххгнбвчетщхыошучберончхпджьмтждкюхци
тцщвчетнюицтхшмююкйеытц
ончхшхжбзцлхгбущдйнищдгждцщоыоьжйещюаблюстюбхлнююямбощцюкцяюкдлщцэьцайанетпюц
птдтхнгкцеоубхфкцтхшммы
дйрбсучхеоябньмкэюэтмхтдстпннь поябсфрбцюдесбанднбрщюэтсдатлцпнвотдхшкдэйолэтз
йеретхжвгажщаиашдбншдкц
жхыболиндйчетдажгцситцэюмхэшсущцитвожюшцшуерюмтцшцсюпдухтдбнгцвотхинухчгрбтдт
хыбхызцпюибруибхфйуцнбр
щюэтсдбоцпштмыкдохьбгцфпибшшернбцюйекдлттдяогичхшцбалшшшитщооозннтюыэйсгрбгхш
сшпцэкдлттдкгрбвмнищдри
анлххнэйрбгхщгкцеощофоойэврбцюсбсуиндйчечолбнбгхжючээтвиюеэтнтцнсесдветхшпоос
банкцоохлэттднттюхлдшшш
итщостжошсзхтдьжрбгхмюлбпзажкбжьхызцпюибжьпоябсфрбйещощщкюшсшпдтушйбяхщоцщаня
юепмтцпжхофюекйухощйекд
ютвоэуажкбвхцнлхщюмыкотцноуеьюэывюаоэумйаннбцючотхтдэиыжюбдыюмнищдкбуофюьтыбв
хпикцутвоэуажкбвхетшхзх
жхриажгцсстднбанщдюйерййнбьзрбйешхвимбсурржутзчхшцвзеоетйаыжтфюекоцппикцбнщож
хвбвущджьэывюфюнэстсдве
атлцпнчэсклхшхэджудэйхсбрбвочгрбтдтхыбгцэюгхзхэтнцислтжбэлгтфдэйсуьхцретмхщюб
еьжкхщтжпнгсштввюлтднт
нойхтюмихлтджюйхцпвотдяочоехыбйбзцлждцхнрбчэскеокдвопюшцлшйотдухвцщохсгтфдньз
юэшкчаюйхцпвоыойсвцхндн
шблйднвоэтсючтсоеютдэшжьпоойерягррщюкэиннисуюхыогцщарбвоуйщодэнтихыбвучшвуэож
хэдюгрбтдтхыбгцэюйотдух
вцщоыофоюбпокйфигжщддцлхксввсущантсофочоехыбгцлжкбюешюыхнцхтцпетмыохцйзцэозои
хыбгцфптцэочоьбгцфпчочо
боацлжолфтьюжтфпвекдфтжюпюфотдяобзохвнщзтлвошскоооыокдютждкдртнтфддйшюыхнцхтц
пвотдсуыищаднсейузйнбьх
дретыбрущоьыйбрбитшхыошсзхтдстнтыбюлпюьыеоьывюатошанкудйэюфоюбэйзцкуодвюстфпэ
тщоеовикцхнлхщюкцооньще
чощщвуйоюсзхыбухушпзкцхнрбшшернбйечотдэййбсцтхшмбдпрвмкдгжэащдрощщсиюасцитфпк
дьоицжувундэыдйлдюойхфб
пойхнудйхнэлщащзчэяуемнбррмютддйьзкцсюбцсучдвуандшеохсихйхбхщпйхлеэапнчхеойхш
исеетщхыощцсучдвукудйэю
цнсесдверианлххнэйрбгхыянбитйюсуюгэшжььггжнбйеяогбанохшхыбвуерюмтцшцсюьыгцохэ
цхнвуетэтфтщюбдухтддцси
тцэюмхэшсурианлххнэйрбгхфодтююиндйчехьнтудкоцпкдютэиажтфзнщазхфоябсфрбгхшхвия
жьзвотдучяоехфдвукдютккй
тцюмнтжхщюгхыочонххгнбйебхохвжанкдвощхщюйувгксююиндйчевостююхцяхщюкоушнбднеок
оацяхжхитсююйянбэюцпчэ
дйщтощцюйиеыаншшвуйжышьтфоэсцркьзозбндфхджэихлтджюйхцпвотдкбфичхэюенмтцпжхофй
уфюьювортнтфддйкдютгцит
сдвейхагкцжуружхеогсослфчхшцщцыомтмюитсюфоойервукйниыжзтсдгцитстфпвешбрбднтцф
пйотдухвцщоыощощщюггжнб
гхкудйэюждвудрзохскдыстднбанщдвехызцчэшхджщдшшгхдэйхсбрбчэвггжнбйегцывкцхнсеу
двеетнхлхгтэдерйетдажбй
щтцпвотдучвцйудйпрэвщдшдэыдйут
```

Розшифрований текст
отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотдельногоче
ловекавовсякомслучаеоноглавныйисточникчувствавинынеизвестноединственныйлиисслед
ованиямнеудалосьещеустановитьдушевноепроисхождениевиныипотребностиискуплениян
оотнюдьнесущественноединственныйлиэтоисточникпсихологическоеположениесложноин
уждаетсявобясненияхотношениемальчикакотцукакмыговоримамбивалентнопомимоненав
истииззакоторойхотелосьбыотцакаксоперникаустранитьсуществуетобычнонекотораядоля
нежностикнемуобаотношениясливаютсявидентификациюсотцомхотелосьбызанятьместоот
цапотомучтоонвызываетвосхищениехотелосьбыбытькаконипотомучтохочетсяегоустранит
ьвсеэтонаталкиваетсянакрупноепрепятствиевопределенныймоментребенокначинаетпоним
атьчтопопыткаустранитьотцакаксоперникавстретилабысостороныотцанаказаниечерезкаст

рациюизстрахакастрациитоестьвинтересахсохранениясвоеймужественностиребенокотказ
ываетсяотжеланияобладатьматерьюиотустраненияотцапосколькуэтожеланиеостаетсявобл
астибессознательногооноявляетсяосновойдляобразованиячувствавинынамкажетсячтомыо
писалинормальныепроцессыобычнуюсудьбутакназываемогоэдиповакомплексаследуетодн
аковнестиважноедополнениевозникаютдальнейшиеосложненияеслиуребенкасильнееразви
тконституционныйфакторназываемыйнамибисексуальностьютогдаподугрозойпотеримуже
ственностичерезкастрациюукрепляетсятенденцияуклонитьсявсторонуженственностиболее
тоготенденцияпоставитьсебянаместоматериилеренятьеероликакобекталюбвиотцаодналиш
ьбоязнькастрацииделаетэтуразвязкуневозможнойребенокпонимаетчтоондолженвзятьнасеб
яикастрированиееслионхочетбытьлюбимымотцомкакженщинатакобрекаютсянавытеснени
еобапорываненавистькотцуивлюбленностьвотцаизвестнаяпсихологическаяразницаусматр
иваетсявтомчтоотненавистикотцуотказываютсявследствиестрахаередвнешнейопасность
юкастрациейвлюбленностьжевотцавоспринимаетсякаквнутренняяопасностьпервичногопо
зывакотораяпосутисвоейсновавозвращаетсяктойжевнешнейопасностистрахередотцамдел
аетненавистькотцунеприемлемойкастрацияужаснакаквкачествекарытакиценылюбвиизобо
ихфактороввытесняющихненавистькотцупервыйнепосредственныйстрахнаказанияикастра
циисследуетназватьнормальнымпатогеническоеусилениеривноситсякаккажетсялишьдруг
имфакторомбоязньюженственнойустановкиярковыраженнаябисексуальнаясклонностьстан
овитсятакимобразомоднимизусловийилиподтвержденийневрозаэтусклонностьочевидносл
едуетпризнатьиудостоевскогоионалатентнаягомосексуальностьпроявляетсявдозволенномв
идевтомзначениикакоеимелавегожизнидружбасмужчинамивегодостранностинежномотно
шениксоперникамвлюбвиивегопрекрасномпониманииположенийобяснимыхлишьвытесн
еннойгомосексуальностьюкакнаэтоуказываютмногочисленныепримерыизегопроизведени
йсожалеюноничегонемогуизменитьеелиподробностионенавистиилюбвикотцуиобихвидоиз
менениихподвлияниемугрозыкастрациинесведущемувпсихоанализечителюпокажутсябез
вкуснымиималовероятнымипредполагаючтоименнокомплекскастрациибудетотклоненсиль
неевсегоносмеюуверитьчтопсихоаналитическийопытставитименноэтиявленияневсякогос
омненияинаходитвнихключклюбомуневрозуиспытаемжеговслучаетакназываемойэпилепс
иинашегописателянонашемусознаниютакчуждытеявленияявластикоторыхнаходитсянаша
бессознательнаяпсихическаяжизньуказаннымвышенеисчерпываютсявэдиповомкомплексе
последствиявытесненияненавистикотцуновымявляетсяточтовконцеконцовотождествление
сотцомзавоевываетвнашемяпостоянноеместоэтоотождествлениевоспринимаетсянашимяно
представляетсобойвнемособуюинстанциюпротивостоящуюостальномусодержаниюнашего
ямыназываемтогдаэтуинстанциюнашимсверхяиприписываемейнаследницеродительскогов
лияниянаиважнейшиефункцииеслиотецбылсуровнасильственжестокнашесверхяперенимае
тотнегоэтикачестваивегоотношениикяснованозникаетпассивностькоторойкакразнадлежал
обыбытьвытесненнойсверхясталосадистическимстановитсямазохистскимтоестьвосновес
воейженственнопассивнымвнашемявозникаетбольшаяпотребностьвнаказаниииияотчастиот
даетсебякактаковоевраспоряжениесудьбыотчастиженаходитудовлетворениевжестокомобр
ащенииснимсверхясознаниевиныкаждаякараявляетсяведьвосновесвоейкастрациейикактак
оваяосуществлениемизначальногопассивногоотношениякотцуисудьбавконцеконцовлишьд
альнейшаяпроекцияотцанормальныеявленияпроисходящиеприформированиисовестидолж
ныпоходитьнаописанныездесьанормальныенамещенеудалосьустановитьразграниченияме
ждунимизамечаетсячтонаибольшаярольздесьвконечномитогеприписываетсяпассивнымэле
ментамвытесненнойженственностиещекакслучайныйфакторимеетзначениеявляетсяливну
шающийстрахотецивдействительностиособеннонасильственнымэтоотносится кдостоевско
муфактегоисключительногочувствавиныравнокакимазохистскогообразажизнимысводимке
гоособенноярковыраженномукомпонентуженственностидостоевскогоможноопределитьсл
едующимобразомособенносильнаябисексуальнаяпредрасположенностьиспособностьсособ
ойсилойзащищатьсяотзависимостиотчрезвычайносуровогоотцаэтотхарактербисексуально
стимыдобавляемкранееузнаннымкомпонентамегосуществараннийсимптомприпадковсмер
тиможнорассматриватькакотождествлениесвоегоясотцомдопущенноевкачественаказанияс

осторонысверхятызахотелубитьотцадабыстатьотцомсамомутеперьтыотецноотецмертвыйо
бычныймеханизмистерическихсимптомовиктомужетеперьтебяубиваетотецдлянашегоясим
птомсмертиявляетсяудовлетворениемфантазиимужскогожеланияиодновременномазохистс
кимпосредствомнаказаниятоестьсадистическимудовлетворениемобаяисверхяиграютрольо
тцаидальшевобщемотношениемеждуличностьюиобектомотцаприсохраненииегосодержан
ияперешловотношениемеждуяисверхяновыяинсценировканавторойсценетакиеинфантильн
ыереакцииэдиповакомплексамогутзаглохнутьеслидействительностьнедаетимвдальнейшем
пищинохарактеротцаостаетсятемжесамымнетонухудшаетсясгодамитакимобразомпродолж
аетоставатьсяиненавистьдостоевскогокотцужеланиесмертиэтомузломуотцустановитсяопа
снымеслитакиевытесненныежеланияосуществляютсянаделефантазиясталареальностьювсе
мерызащитытеперьа

```
with keys
 199 700
```

Висновок

Набули навички частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.