МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

# Криптоаналіз афінної біграмної підстановки

Виконали:

Студенти групи 3 курсу
груп ФБ-96 та ФБ-94
Ігнатенко Артем
Васюченко Георгій

Київ 2021

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

Постановка задачі:
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 (a,b) шляхом розв'язання системи.
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.

Хід роботи:

Варіант 2

Завдання 1:

```
def gcd(a, b):
    if b == 0:
        return a, 1, 0
    else:
        d, x, y = gcd(b, a % b)
        return d, y, x - y * (a // b)


def opp_element(a, mod):
    return gcd(a, mod)[1]
```

Завдання 2:

| | Bigram | Frequency |
|---|---|---|
| 0 | йа | 0.019774 |
| 1 | юа | 0.018160 |
| 2 | чш | 0.016546 |
| 3 | юд | 0.014528 |
| 4 | рщ | 0.012510 |

Завдання 3-5:
У функції filter() ми перевіряємо:

- Чи починається текст з "ы" або "ь";
- Чи зустрічаються у нас біграми виду "ыь" та "ьы"
- Чи зустрічається 4+ голосних літери підряд;

Якщо виникають такі випадки - то текст є "шумом".

Ключ:
a = 27
b = 211
Зашифрований текст:
рйрщкагпprфчгшрщйрпрффькрпьчшдвиыеюдучхулицплшющашдщныскющвпьюкджьйахещыйеьеюеэдсец
чтыкйдшцчзюимевжш
бушччэканылшолшкющчшэизупмзсбвжшбуойщаищмдпнрйуюфшхдтылшларюдезанпрбкажлащваэщюемеч
шщипнипнучбусхека
йаэкяуклзщюгхегарпинцплпprффзшскыушщммеючогалчцпдшяуыуйацднфзхащаукйнхжукчщысаэарюж
штнцмосхрхлтечшиш
валлмпprтелиюдьпкуурдщерритыачтахщышкаюйзхцмздффнагещцлерьюбокцезацчучрйяыыунлсрорп
рькрщэарючолаимху
гшзепутэрщбероюазанхзушщимзсбючолаштэиэщюхжукчтдюагпшдормэрмыупьфуйабеюемдвитылшошр
щышгпфуыуйацдаюва
ллйыачларщзщроюалахдорцпиышцылшошрщйьфуйазлиекдвифущлбшашваллюсхщрохеццэирщэаэшуоьюд
эисфуриыугшэпзлие
кдкглаедюднфэщйдшгфчпрбердрйуюпнсабдпннхцмрцсдрпющкммьлеешбпымюенпчщроюабучштечшюду
шлсбубеюыхрдщндщф
щейерйсдкммьофкаюйажйаидхйьнхерщхлкшьсжуиеишбпымюенпчщроюаеймюберояюарпинымжизаропйх
лбшбуклзщзсэпюаие
чшорэпьчкгипгекбхщжачойатеащваюдюдкйчбйкпмтырйюенщлучихечшчрпрфуклзщрусипнрйыуйаусй
рпнцмшяхукчкйбвжш
лжпшюечукемипнипцчушлсрйхпэснезщжмюдкенлхарпсдхйьчмэешйарпхппрэщцжыщпаюехдпьхуйанац
чрбюдхушчкацкдщте
эдвиййтагшфичиорхлфдщфкшышвамносвиййдзьрыщышхемсующудршджьюанхрэцпымздффнарписюахьх
ууочрфчгшйкпаюехд
сджжгшцчтыкйдшнануэифуларизсййушфиюдюдаюышькющяпцлдчьншгашэлашьухаедвизлиекдвидщлсх
пкеышйрьчценавсач
эаькудбюяхцмрцсдрпгекммьлекдхйыуыщйаудюлцчисуюэиффриещжзьргшкдыууоьдглэшбероюачпщ
ылшыщдшэасуйаьпым
куюсщгхелафитбюазуыщюаешуоналаолфдыууозмсдщьбукаощжзьрыщаыпмяызшхпбьйацчзюимпелумср
йюасавдыугшбрмэтд
йкяуришпчиоскчтхэейыосййричикзддрятаршроюазахачшфщчшурпрбуашькщепщчшфитдьчфщроюазац
квснхтбьечшчыачеш
удкгхавклаяхбмхашнэпосюеюазнтдщьбудшщепщчшфикайаэкишныцмбээелучылшрщашошзсбужифчмэй
кблкмоснфэщкылшрщ
хлиечшритэзалаеймюберояюарптылшцюцрчийщпаюеющчшхпэщхеишашйамущьбукаьээхцмустдмшыщдшц
чсдхйыуыщйаудчика
бпсаюезлиекдффыршдчимшлчлэфуюазздрятачшсающчшййнцусюаьжхезнмшйщгпридщнйымюдкебдкйю
щешхщнкшлнуюсэебд
ьебпщьюарпжиегтдлэфщюенщдезаламдосусжулапасйюдаюнежсщьйкэытэшсосгпэпщепщчшфихехщюед
шэпеемучщройкэыса
репуосхасасйленкссвссеоамдосвпхрзшмейрцлтедчусхеццкемчььсдмэшсрморушнллирмффаыпмяыз
шщфзсййымзсхажала
фщнпбупюоьюдкеещхщшпщяавцквснхтбьечшджпшюешпщьбуказаэплахщдщнйдщтечшджпшюешпщьбуэщш
чсщряаюэщкацкышще
хеаитбюаршлсцпэсеегпосщерпусдюйаюдбучихеэдэппртехарпеылегшмчхухаяютечшюдуссайщсллды
ууокайасазаопчичп
нхбморешэшсающуонафщгшмейррихушкдщнйдщтечшщукайаэкышхемчтэхевателуцчисхпкучызшцшмей
ряжпшюешпщьбудшоы
лшищгамуыщюаешлуьппрринхдщцадуришпчичифубелшмшмвкйуыгшхлвпьюзсййушфиюдпелучырйнхюай
ажлэщцжйацчушугрй
хпцчсдьчфщроюаепжьюдмшеемучщроюазацчаябуащыщдшварчмэчинкныцмйквыдщлагчмэашзщэиьчщщч
шмейртвещжзьргшкд
тваыпмяызшыыдщнпщьбукачэрщмечшлжйазакмхйтвдебукчкйбвжшоыачлаоыьчмбюдпаюехдхввамнхук
чкйбвжшгсйасандус
сагшяснежсчикммьлезлиекдбюфшхдиырйгекбюдтдфчнцюдавлэкдусосйасадуклзщюдфчнцюдкемсуюв
пьюцкдщтечшэиащва

ейнцусюазблэчшгечофщгесаьпюачпжжпшюечуаюгарпсенуказаэпюазшлууросйасажлешзлйаудрйхрм
эцпфжйахеродюыщжр
проппрчикммьлевлщднхбмнхшсзмгьхпэсрежаолфдыууофнрйнцусюазблэчшрщзщжацчтыкйкаешхакмх
йтвжшусййушфиюдюд
аюгпшгцчтыкйкающамджйазаддхухегарпцпбьюахщэдкгщыфутдаюащышэылшищяросчшмезахехщяпвсх
йюдаюыущаидвцюдаю
ьичбзлцчтыкйэщыштыаччбзстдаюышхехаедюшзщрпщысагшлайеошцкнуфносачзюидцецчхйхажатечшж
ьйацчтыкйдшрщзщаш
чоыйыуйаусйрпнюлтевйвпрпгечпщачшкдььрмегфчпрбелшцающашчопаюебушщькышзшвыйафщышхпцмд
рщыыуюехакчщуиеза
фнщыаччбзстдаюрщлаеебдкйлщйачнрйюблэчшшхнфрпющэплщцчсдфмчзьчжлаыпмяызшжхбмнхшсбужич
лщерпюабуашькщыдщ
вйрмыулпбьйашдтыцмюарпхвцчьрдщгшашчоламчэичаэхшстдаюриэщйазнзсзшйшлшюагпчиеысагшлай
езщайхлбшглэщйщчш
чамеешвдбювсрэжичбзлэпрешхнфрплацсрчцпхюшрфчсимэоскгфуыйыхффэплщгарпсенуказарчыупмх
уэсдммэтдяавдчишх
таичшзыйыуйаусйрпнушхакмюбпмншжлэщйщчшэирщлэгерпюабуосйещеэдсечушгцмпнщьбукаюдуыдщи
мюдкечушгмщрщашщп
прэщкырйдщьлщеющвпьюриюдюашдйржахетсййвпэсгпчинаькгшхпннзщццтвкчисжлзсйепртшййыуйау
сйрпншдажйазмгьус
ффщлщрбезахемчтэлекмаюрщудеапамдосшсцпфжнлзуыщюазреызшэатдрмхпщьбудшщыхубвчочпщаэщя
лчохехалюидвиаммс
ееапегкажлхехдпрчиилмечшшшцкдщтечшчызшэатдрмлэчлрщнаэшэдкйчбйкишугрййкоыдднпрщышлсб
убеаунккмнежскгцч
тыкйкавйыуйаусйрпносфнзвюаиейркезаокйщгаынрйщызюимюдаюаыпмяызшцлгпшгцчтыкйкаяхбмщыр
йнхкелиачгшшдсдмэ
шсрмфукукчщгчилиачгшзсечмбрмфуэснарпзючшпмвпфчбшмейрпныурщгпзхцмчэиорщэаэшшщрщхезак
дььрмьрпнхщшдькюе
дефшроошкаюрпркдчэуырщлхчээпмеидбюхахщимюдюарппьщсрплаэщкаюытэтедщпуэщвкющиулаэиыйх
лллнажахоусиппрсе
эщюхыййаькэиеыйееуйафмыушфзщжбглщейеуозсащвашйымюдхунлищжанарпзючшбуосачиеэдщырйнхю
ахйщфрпешберояару
щефпкезарчцптддчщфдщпуэщвкющньйашегахлтейицмрйыезаокнейежпэиэщгэхувлуоыуыщимфмйщпшй
рщьйапахпьююаяофэ
хувлуолиачйахагаодвимдчитысазшйыжжйажлчпнхыезахаэасачшашйарокамейецыьпяйхеейыуйаусй
рнфйщхлюеерффасхй
юдкемдсилэгерпйклижуашрщщейечшвппршгцчтыкйканущефптачштэрщзщяпэптбьерпимюдкеслщещцр
имежагекаюрэпьчяф
ьеруюсхпымздюлщелшашфьымосьрчифшцкщедеюакайасажлнктешщэилиачгшопьчффкммьофпаюечэрщо
шбеюеюылшищгаясбр
мэтдюадуклзщачисюарехеэдпрмэтдавнкхатешщашлиачгшдчьнчиипяыачжижуыщашащышгпридчьнриф
усицлщеомхпипчушг
мщрщашгшмейрсемьюдкеипгекбхщвпчпжжйаайхлзаейуюфщроошэщнхльюаэпеямшщевлэияффубелшщфц
чтыкйхрмсуювпьюыщ
дшварчмэчиащварщэщйщчшэийщхатешщчшбущефпсдюдисфуидчиеапячщ

## Розшифрований текст:

однакоэтакартинаскакойшьстжроньмдеенирассматривалиралчльваетйявнлптонеичреьеленноеп
рвчадкипроявляющиесярезколчрикусьваниемусиливающиесядоопасногодляжизнвчриводящегокт
яжкомусамокалечениюмогутвсежевнекоторьхслучаяхнедостигатытакойсильцслабляясыдократк
ихсцстоянийабсансадобьстричроходящихголовокруженийимогуттакжесменцтысякраткимвчерио
дафикогдаболыноЙсовершаешпуждьеегоприродячцступкикакшьнаходясывовластибессознателын
огообуславливаясывобщемкакбьстранноэтониказалцсбпистотелесньмвчричинафиэтисцстояния
могумчервоначалыновозникатфчичричинатпистодушевньмиспугилимогутвдалынейшемнаходитый
явзависимцстиотдушевньхволненийкакнихарактернодляогромногобольшинствацлщпаевинтнлле
ктуалыноеснижениеноизвестезчокрайнеймереодинслщпайкогдаэтотнедлгненарушигвьсшейинтн
ллектуалынойдеятелыностигнлымголыцдругиеслучаивотношениикотжрьхутверждалосытожесамо
ененадежньилвчодлежатсомнениюкакислучайсамогодцстоевскоголицастрадающиеэпилепсиеймо
гутпроизводитывпечатлениетупостинеджразвитоститаккакэыаболезнбпастосопряженасярковь

раженньмидиотизмомикрупнейшифимозговьмидефэкыафинеявляясыконлпнообязатнлыной составн
оппастыюкартиньболезниноэтипрвчадкисовсемисвоимивидоизмененияфишьваютиудрлгихлицули
осполньмдушевньмразвитиефискжреесосверхошьчнаявболышинствеслщпаевнедцсыаточноуправл
яемойимиаффэктивнцстыхнеудивителыночтичриыакихобстоцтнлыствахневозможноусыановитысо
вокупнцстыклинопескоюаффэкыацчилячсиитфптопроявляетсяводнороднцстиуказанньхсимптомо
втребуемчовидимомуфункционалыногопониманиякакеслишьмеханизманжрмалыноговьсвобожьени
шчервичньхпозьвовбьлподготовленорганопескимеханизмкоторьйилчолызуетсшчриналичиивесы
маразньхусловийкадчринарушениимозговойдеятелыноствчритяжкомзаболеваниитканейилитокс
опескодзаболеванииыакипринедцсыаточномконтроледушевнойекономиикризисномфункциониров
аниидушевнобэнергиизаэтимразднлениемнадвавидамьчувствуемньентопностымеханизмалежаще
говосновевьсвобожденияпервопньпчозьвовэтотмеханизмнедалекиотсексуалыньпчроцессовпор
ождаемьхвсвоейосноветоксическиужедревнейшиеврюпиназьваликоитусмалойцчилячсиейивиднл
ивполовомактесмяйпениеиадаптациювьсвобожьенияэпилептопескогоотводараздраженияэпилеп
топескаяреакциякаковьфименемможноназватывсеэтовместевзятоенесомненнотакжепостнчаети
враспоряжениеневрозасущнцстыкотороговтомчтобьликвидироватысоматическимассьраздражен
ияскоторьфиневрознеможетсправитысшчсихическиэпилептопескигчрипадоксыановитсцтакимоб
разомсимптомомистериииеюадщчтируетйяивидоизменяетсшчодобнотомукакэтопроисходитпринж
рмалыномтлпениисексуалыногопроцессаыакимобразоммьлчолньжчравомразличаемжрганическую
иаффэктивнуюцчилячсиачрактопескоезначениеэтогоследующеестрадающигчервогчжраженболез
ныюмозгастрадающийвторойневротиквпервомслщпаедушевнаяжизнфчодверженанарушениюизвнев
овторомслучаенарушениеявляетйявьражениемсамойдушевнойжизнивесымавероцтночтоэпилепси
ядостоевскогоотноситсяковторомувидуточнодоказатыэтонелызяыаккаквтакомслщпаенужнобьл
обьвклдпитывцелокупнцстыегодушевнойжизниначалопрвчадковипоследующиевидоизмененияэти
хпрвчадковадляэтогоунаснедостатфпноданньхичисаниясафипчрипадковничегонедаютсведения
цсоотношениянмеждупрвчадкафивчереживанияфинеполньичастичротиворечивьвсеговероятнееп
редположенилптопрвчадкиначалисыьдцстоевскогоужевдетствечтоонивнюпалехарактеризовали
сыболееслашьфисижчтомафиитолыкичцслепотрясшегоегичереживаниянавосемнадцатомгодужизн
иубийстваотцапринялифжрмуцчилячсиибьлобьвесымауместноеслишьичравдалцсытфптоонвчолно
стыюпрэкратилисывовремяотбьванияимкаторгивсибириноэтомнчротиворечатдругиеуказанияоч
евиднаясвязымеждуотцеубийствомвбратыяхкарамазовьхисьдгбойотцадостоевскогобрцсиласыв
глазанеодномубиографьдцстоевскогоипослужилаимуказаниемнаизвестноесовременноепсихоло
гопескоенщчравлениепсихоанализтаккадчодраяумеваетйяименноонсклоненвидетывэтомсошьти
итягчайшуютравмуивреакциидцстоевскогонаэтоклдпевойпунктегоневрозаеслияначнуобосновь
ватыэтуусыановкнчсихоаналитопескиичасаюсычтоокажусынепонятньмдлявсехтехкомунезнаком
ьучениеивьраженишчсихоанализаунасодиннадежньйисходньгчунктнафизвестенсмьслпервьхпрв
чадковдцстоевскоговегоюношескиегодьзадоугодичоявленияцчилячсииуэтихпрвчадковбьличод
обиесмертиониназьвалисыстрахомсмертиивьражалисывсостоянииилетаргическогцснаэтаболезн
ынаходилананеговнюпалэкогдаоншьлещемалычикомкаквнезщчнаябезотчетнаяподавленностбпув
ствокакозчозжерассказьвалсвоемьдругусоловыевутакоекакбьдтошьемнчредстоялцсейчасжеум
еретыивсамомдненаступалосостояниесовершенничодобноедействительнойсмертиегобратандр
ейрассказьвасптофедоружевмолоддегодьпередтемкакзаснутыцсыавлялзаписконтобоитйяночью
заснутысмертоподобньмсномвчросимчоэтомучтобдегопохоронилитолыкочеребчцтыднейдцстоев
скийзарулеткойвведениеснамизвестньсмьслинамерениетакихпрвчадковсмертониозначаютото
жьествлениесумершимчеловекомкотжрьйьействитнлыноумериличпнловэкомживьмещенокоторому
мьжелаемсмертивтжройслщпайболеезначителезчрипадоквуказанномслучаеравноцененнаказани
юмьпожелалисмертидрлгомутячерымьсыалисафиэтимдрлгимисамиумерлитутпсихоаналитическое
щпениеутверждаетчтоэтотдругойдлямалычикаобвпноотецииименуемьйистериейпрвчадокявляетй
яыакимобразомсамонаказаниемзапожеланиесмертиненавистномуотцуа

Висновок: засвоєно навички частотного аналізу на прикладі розкриття моноалфавітної підстановки, розшифрування текстів, які були зашифровані афінним шифром за допомогою підстановки найпопулярніших біграм.