МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТИХНІЧНИЙ ІНСТИТУТ ІМ.ІГОРЯ СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

Комп’ютерний практикум №3

Виконали:

Студенти 3 курсу

ФБ-01 Літвінчук Софія
та
ФБ-02 Косарик Дарія

Варіант 2

Тема: Криптоаналіз афінної біграмної підстановки

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

Поставновка задачі:

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь.
2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту
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 шифр текст. 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:

1. Підпрограми:
   - **Обчислення оберненого елементу за модулем із використанням розширеного алгоритму Евкліда**:

```
def inverse(a,b):
    """Обернене за модулем"""
    k = list(extended_euclid(a,b))[1]
    return k
```

   - **Розв'язування лінійних порівнянь**:

```
def solve_eq(a, b, n):
    """Розв'язування лінійних порівнянь"""
    roots = []
    d = gcd(a, n)
    if d == 1:
        roots.append((inverse(a, n) * b) % n)
    else:
        if (b % d) == 0:
            res = (inverse(int(a / d) * int(b / d) , int(n / d))) % int(n / d)
            for i in range(d):
                roots.append(res + i * int(n / d))
        else:
            roots.append(-1)
    return roots
```

2. **Найчастіші біграми шифротексту з варіанту:**

['йа', 'юа', 'чш', 'юд', 'рщ']

3. **Всі можливі кандидати на ключ (a,b)**:

(806, 186), (806, 186), (713, 899), (837, 589), (155, 31), (9, 370), (40, 897), (71, 463), (102, 29), (133, 556), (164, 122), (195, 649), (226, 215), (257, 742), (288, 308), (319, 835), (350, 401), (381, 928), (412, 494), (443, 60), (474, 587), (505, 153), (536, 680), (567, 246), (598, 773), (629, 339), (660, 866), (691, 432), (722, 959), (753, 525), (784, 91), (815, 618), (846, 184), (877, 711), (908, 277), (939, 804), (93, 899), (341, 310), (155, 31), (22, 188), (53, 715), (84, 281), (115, 808), (146, 374), (177, 901), (208, 467), (239, 33), (270, 560), (301, 126), (332, 653), (363, 219), (394, 746), (425, 312), (456, 839), (487, 405), (518, 932), (549, 498), (580, 64), (611, 591), (642, 157), (673, 684), (704, 250), (735, 777), (766, 343), (797, 870), (828, 436), (859, 2), (890, 529), (921, 95), (952, 622), (93, 899), (341, 310), (248, 279), (868, 279), (868, 279), (713, 279), (124, 589), (620, 868), (620, 868), (248, 899), (707, 945), (955, 325), (908, 954), (82, 415), (254, 691), (698, 55), (348, 894), (6, 350), (109, 55), (224, 584), (53, 682), (263, 620), (852, 620), (381, 155), (879, 260), (613, 742), (737, 91), (580, 520), (284, 678), (718, 554), (256, 562), (438, 355), (677, 1), (400, 190), (640, 54), (243, 125), (90, 190), (423, 953), (705, 117), (561, 489), (871, 489), (535, 396), (523, 324), (321, 625), (538, 687), (426, 283), (18, 703), (235, 641), (314, 831), (312, 960), (943, 721), (851, 645), (785, 298), (726, 783), (696, 645), (196, 267), (647, 593), (110, 779), (265, 779), (934, 252), (649, 464), (176, 165), (765, 196), (27, 211)

4. **Програма перевірки змістовності тексту:**

```
def check(text):
    top_l = ('oea')
    let_count = 0
    for let in text:
        let_count += 1
    for c in top_l:
        t = 0
        for i in text:
            if c == i:
                t += 1
        if c == 'o' and t*100/let_count < 7:
            return False
        if c == 'e' and t*100/let_count < 6:
            return False
        if c == 'a' and t*100/let_count < 6:
            return False
    return True
```

<u>Шифрований текст</u>:

рйрщкагпprфчгшрщйрпрффькрпьчшдвиыеюдучхулицплшющашдщныскющвпьюкджьйа
хещыйеьеюоэдсецчтыкйдшцчзюимевжшбушччэканылшолшкющчшэизупмзсбвжшбуойщ
аищмдпнрйуюфшхдтылшларюдезанпрбкажлащваэщюемечшщипнипнучбусхекайаэкяукл
зщюгхегарпинцплппрффзшскыушщммеючогалчцпдшяуыуйацднфзхащаукйнхжукчщыса
эарюжштнцмосхрхлтечшишваллмппртелиюдьпкуурдщерритыачтахщышкаюйзхцмздффн
агещцлерьюбокцезацчучрйяыыунлсрорпрькрщэарючолаимхугшзепутэрщбероюазанхзу

шщимзсбючолаштэиэщюхжукчтдюагпшдормэрмыупьфуйабеюемдвитылшошрщышгпфу
ыуйацдаюваллйыачларщзщроюалахдорцпиыщылшошрщйьфуйазлиекдвифущлбшашвал
люсхщрохеццэирщэаэшуоьюдэисфуриыугшэпзлиекдкглаедюднфэщйдшгфчпрбердрйуюп
нсабдпннхцмрцсдрпющкммьлеешбпымюенпчщроюабучштечшюдушлсбубеюыхрдщндщ
фщейерйсдкммьофкаюйажйаидхйьнхерщхлкшьсжуиеишбпымюенпчщроюаеймюберояюа
рпинымжизаропйхлбшбуклзщзсэпюаиечшорэпьчкгипгекбхщжачойатеащваюдюдкйчбйкп
мтырйюенщлучихечшчрпрфуклзщрусипнрйыуйаусйрпнцмшяхукчкйбвжшлжпшюечукем
ипнипцчушлсрйхпэснезщжмюдкенлхарпсдхйьчмэешйарпхппрэщцжыщпаюехдпьхуйана
цчрбюдхушчкацкдщтеэдвиййтагшфичиорхлфдщфкшышвамносвиййдзьрыщышхемсующ
удршджьюанхрэцпымздффнарписюахьхууочрфчгшйкпаюехдсджжгшцчтыкйдшнануэиф
уларизсййушфиюдюдаюышькющяпцлдчьншгашэлашьухаедвизлиекдвидщлсхпкеышйрьч
ценавсачэаькудбюяхцмрцсдрпгекммьлекдхйыуыщйаудюлцчисуюэиффриещжзьргшкдыу
уоьдглэшешбероюачпщылшыщдшэасуйаьпымкуюсщгхелафитбюазуыщюаешуоналаолфд
ыууозмсдщьбукаощжзьрыщаыпмяызшхпбьйацчзюимпелумсрйюасавдыугшбрмэтдйкяур
ишпчиоскчтхэейыосййричикзддрятарщроюазахачшфщчшурпрбуашькщепщчшфитдьчф
щроюазацквснхтбьечшчыачешудкгхавклаяхбмхашнэпосюеюазнтдщьбудшщепщчшфикай
аэкишныцмбээелучылшрщашошзсбужифчмэйкблкмоснфэщкылшрщхлиечшритэзалаейм
юберояюарптылшцюцрчийщпаюеющчшхпэщхеишашйамущьбукаьэзхцмустдмшыщдшцч
сдхйыуыщйаудчикабпсаюезлиекдффыршдчимшлчлэфуюазздрятачшсающчшййнцусюа
ьжхезнмшйщгпридщнйымюдкебдкйющешхщнкшлнуюсэебдьебпщьюарпжиегтдлэфщюе
нщдезаламдосусжулапасйюдаюнежсщьйкэытэшсосгпэпщепщчшфихехщюедшэпеемучщ
ройкэысарепуосхасасйленкссвссеоамдосвпхрзшмейрцлтедчусхеццкемчььсдмэшсрморуш
нллирмффаыпмяызшщфзсййымзсхажалафщнпбупюоьюдкеещхщшпщяавцквснхтбьечшд
жпшюешпщьбуказаэплахщдщнйдщтечшджпшюешпщьбуэщшчсщряаюэщкацкышщехеаи
тбюарщлсцпэсеегпосщерпусдюйаюдбучихеэдэппртехарпеылегшмчхухаяютечшюдуссай
щсллдыууокайасазаопчичпнхбморешэшсающуонафщгшмейррихушкдщнйдщтечшщукай
аэкышхемчтэхевателуцчисхпкучызшцшмейряжпшюешпщьбудшоылшищгамуыщюаешлу
ьппрринхдщцадуришпчичифубелшмшмвкйуыгшхлвпьюзсййушфиюдпелучырйнхюайаж
лэщцжйацчушугрйхпцчсдьчфщроюаепжьюдмшеемучщроюазацчаябуащыщдшварчмэчин
кныцмйквыдщлагчмэашзщэиьчщщчшмейртвещжзьргшкдтваыпмяызшыыдщнпщьбукачэ
рщмечшлжйазакмхйтвдебукчкйбвжшоыачлаоыьчмбюдпаюехдхввамнхукчкйбвжшгсйаса
ндуссагшяснежсчикммьлезлиекдбюфшхдиырйгекбюдтдфчнцюдавлэкдусосйасадуклзщю
дфчнцюдкемсуювпьюцкдщтечшэиащваейнцусюазблэчшгечофщгесаьпюачпжжпшюечуа
югарпсенуказаэпюазшлууросйасажлешзлйаудрйхрмэцпфжйахеродюыщжрпроппрчикмм
ьлевлщднхбмнхшсзмгьхпэсрежаолфдыууофнрйнцусюазблэчшрщзщжацчтыкйкаешхакмх
йтвжшусййушфиюдюдаюгпшгцчтыкйкающамджйазаддхухегарпцпбьюахщэдкгщыфутда
юащышэылшищяросчшмезахехщяпвсхйюдаюыущаидвцюдаюьичбзлцчтыкйэщыштыачч
бзстдаюышхехаедюшзщрпщысагшлайеошцкнуфносачзюидцецчхйхажатечшжьйацчтыкй
дшрщзщашчоыйыуйаусйрпнюлтевйвпрпгечпщачшкдььрмегфчпрбелшцающашчопаюебу
шщькышзшвыйафщышхпцмдрщыыуюехакчщуиезафнщыаччбзстдаюрщлаеебдкйлщйачн
рйюблэчшшхнфрпющэплщцчсдфмчзьчжлаыпмяызшжхбмнхшсбужичлщерпюабуашькщ
ыдщвйрмыулпбьйашдтыцмюарпхвцчьрдщгшашчоламчэичаэхшстдаюриэщйазнзсзшйшл
шюагпчиеысагшлайезщайхлбшглэщйщчшчамеешвдбювсрэжичбзлэпрешхнфрплацсрчцп
хюшрфчсимэоскгфуыйыхффэплщгарпсенуказарчыупмхуэсдммэтдяавдчишхтаичшзыйыу
йаусйрпнушхакмюбпмншжлэщйщчшэирщлэгерпюабуосйещеэдсечушгцмпнщьбукаюдуы
дщимюдкечушгмщрщашщппрэщкырйдщьлщеющвпьюриюдюашдйржахетсййвпэсгпчина

ькгшхпннзщццтвкчисжлзсйепртшййыуйаусйрпншдажйазмгьусффщлщрбезахемчтэлекма
юрщудеапамдосшсцпфжнлзуыщюазреызшэатдрмхпщьбудшщыхубвчочпщаэщялчохехал
юидвиаммсееапегкажлхехдпрчиилмечшшшцкдщтечшчызшэатдрмлэчлрщнаэшэдкйчбйк
ишугрййкоыдднпрщышлсбубеаунккмнежскгцчтыкйкавйыуйаусйрпносфнзвюаиейркезао
кйщгаынрйщызюимюдаюаыпмяызшцлгпшгцчтыкйкаяхбмщырйнхкелиачгшшдсдмэшсрм
фукукчщгчилиачгшзсечмбрмфуэснарпзючшпмвпфчбшмейрпныурщгпзхцмчэиорщэаэшш
щрщхезакдььрмьрпнхщшдькюедефщроошкаюрпркдчэуырщлхчээпмеидбюхахщимюдюа
рппьщсрплаэщкаюытэтедщпуэщвкющиулаэиыйхлллнажахоусиппрсеэщюхыййаькэиеый
ееуйафмыущфзщжбглщейеуозсащвашйымюдхунлищжанарпзючшбуосачиеэдщырйнхюах
йщфрпешбероюарущефпкезарчцптддчщфдщпуэщвкющньйашегахлтейицмрйыезаокнейе
жпэиэщгэхувлуоыуыщимфмйщпшйрщьйапахпьююаяофэхувлуолиачйахагаодвимдчитыс
азшйыжжйажлчпнхыезахаэасачшашйарокамейецыьпяйхеейыуйаусйрнфйщхлюеерффасх
йюдкемдсилэгерпйклижуашрщщейечшвппршгцчтыкйканущефптачштэрщзщяпэптбьерп
имюдкеслщещцримежагекаюрэпьчяфьеруюсхпымздюлщелшашфьымосьрчифшцкщедею
акайасажлнктешщэилиачгшопьчффкммьофпаюечэрщошбеюеюылшищгаясбрмэтдюадук
лзщачисюарехеэдпрмэтдавнкхатешщашлиачгшдчьнчиипяыачжижуыщашащышгпридчьн
рифусицлщеомхпипчушгмщрщашгшмейрсемьюдкеипгекбхщвпчпжжйаайхлзаейуюфщро
ошэщнхльюаэпеямшщевлэияффубелшщфцчтыкйхрмсуювпьюышдшварчмэчиащварщэщ
йщчшэийщхатешщчшбущефпсдюдисфуидчиеапячщ

Правильний ключ: (27,211)

Розшифрований текст:

однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопредел
енноеприпадкипроявляющиесярезкосприкусываниемусиливающиесядоопасногодляжизн
иприводящегоктяжкомусамокалечениюмогутвсежевнекоторыхслучаяхнедостигатьтакойс
илыослабляясьдократкихсостоянийабсансадобыстропроходящихголовокруженийимогут
такжесменятьсякраткимипериодамикогдабольнойсовершаетчуждыеегоприродепоступки
какбынаходясьвовластибессознательногообуславливаясьвобщемкакбыстранноэтониказа
лосьчистотелеснымипричинамиэтисостоянияхмогутпервоначальновозникатьпопричинам
чистодушевнымиспугилимогутвдальнейшемнаходитьсявзависимостиотдушевныхволнен
ийкакнихарактернодляогромногобольшинствослучаевинтеллектуальноеснижениеноизве
стенпокрайнеймереодинслучайкогдаэтотнедугненарушилвысшейинтеллектуальнойдеяте
льностигельмгольцдругиеслучаивотношениикоторыхутверждалосьтожесамоененадежны
илиподлежатсомнениюкакислучайсамогодостоевскоголицастрадающиеэпилепсиеймогут
производитьвпечатлениетупостинедоразвитоститаккакэтаболезньчастосопряженасярков
ыраженнымидиотизмомикрупнейшимимозговымидефектаминеявляяськонечнообязатель
нойсоставнойчастьюкартиныболезниноэтиприпадкисовсемисвоимивидоизмененияхмибы
ваютиудругихлицулицсполнымдушевнымразвитиемискореесосверхобычнаявбольшинст
веслучаевнедостаточноуправляемойимиаффективностьюнеудивительночтопритакихобст
оятельствахневозможноустановитьсовокупностьклиническоюаффектаэпилепсииточтопр
оявляетсяводнородностиуказанныхсимптомовтребуетповидимомуфункциональногопони
маниякакеслибымеханизманормальноговысвобожденияпервичныхпозывовбылподготовл
енорганическимеханизмкоторыйиспользуетсяприналичиивесьмаразныхусловийкакприна
рушениимозговойдеятельностипритяжкомзаболеваниитканейилитоксическомзаболевани
итакипринедостаточномконтроледушевнойэкономиикризисномфункционированиидушев

нойэнергиизаэтимразделениемнадвавидамычувствуемндентичностьмеханизмалежащего
восновевысвобожденияпервичныхпозывовэтотмеханизмнедалекиотсексуальныхпроцесс
овпорождаемыхвсвоейосноветоксическиужедревнейшиеврачиназываликоитусмалойэпил
епсиейивиделивполовомактесмягчениеиадаптациювысвобожденияэпилептическогоотво
дараздраженияэпилептическаяреакциякаковымименемможноназватьвсеэтовместевзятое
несомненнотакжепоступаетивраспоряжениеневрозасущностькотороговтомчтобыликвид
ироватьсоматическимассыраздраженияскоторыминеврознеможетсправитьсяпсихическиэ
пилептическийприпадокстановитсятакимобразомсимптомомистериииеюадаптируетсяив
идоизменяетсяподобнотомукакэтопроисходитпринормальномтечениисексуальногопроце
ссатакимобразоммысполнымправомразличаеморганическуюиаффективнуюэпилепсиюпр
актическоезначениеэтогоследующеестрадающийпервойпораженболезньюмозгастрадаю
щийвторойневротиквпервомслучаедушевнаяжизньподверженанарушениюизвневовтором
случаенарушениеявляетсявыражениемсамойдушевнойжизнивесьмавероятночтоэпилепс
иядостоевскогоотносится ковторомувидуточнодоказатьэтонельзятаккаквтакомслучаенуж
нобылобывключитьвцелокупностьегодушевнойжизниначалоприпадковипоследующиеви
доизмененияэтихприпадковадляэтогоунаснедостаточноданныхописаниясамихприпадков
ничегонедаютсведенияосоотношенияхмеждуприпадкамииипереживанияминеполныичаст
опротиворечивывсеговероятнеепредположениечтоприпадкиначалисьудостоевскогоужевд
етствечтоонивначалехарактеризовалисьболееслабымисимптомамиитолькопослепотрясш
егоегопереживаниянавосемнадцатомгодужизниубийстваотцапринялиформуэпилепсиибы
лобывесьмауместноеслибыоправдалосьточтоониполностьюпрекратилисьвовремяотбыва
нияимкаторгивсибириноэтомупротиворечатдругиеуказанияочевиднаясвязьмеждуотцеуби
йствомвбратьяхкарамазовыхисудьбойотцадостоевскогобросиласьвглазанеодномубиогра
фудостоевскогоипослужилаимуказаниемнаизвестноесовременноепсихологическоенапра
влениепсихоанализтаккакподразумеваетсяименноонсклоненвидетьвэтомсобытиитягчай
шуютравмуивреакциидостоевскогонаэтоключевойпунктегоневрозаеслияначнуобосновы
ватьэтуустановкупсихоаналитическиопасаюсьчтоокажусьнепонятнымдлявсехтехкомунез
накомыучениеивыраженияпсихоанализаунасодиннадежныйисходныйпунктнамизвестенс
мыслпервыхприпадковдостоевскоговегоюношескиегодызадолгодопоявленияэпилепсииу
этихприпадковбылоподобиесмертиониназывалисьстрахомсмертиивыражалисьвсостояни
илетаргическогоснаэтаболезньнаходилананеговначалекогдаонбылещемальчикомкаквнеза
пнаябезотчетнаяподавленностьчувствокаконпозжерассказывалсвоемудругусоловьевутак
оекакбудтобыемупредстоялосейчасжеумеретьивсамомделенаступалосостояниесовершен
ноподобноедействительнойсмертиегобратандрейрассказывалчтофедоружевмолодыегоды
передтемкаказаснутьоставлялзаписькичтобоитсяночьюзаснутьсмертоподобнымсномипрос
итпоэтомучтобыегопохоронилитолькочерезпятьднейдостоевскийзарулеткойвведениесна
мизвестнысмыслинамерениетакихприпадковсмертиониозначаютототождествлениесумерш
имчеловекомкоторыйдействительноумерилисчеловекомживымещенокоторомумыжелаем
смертивторойслучайболеезначителенприпадоквуказанномслучаеравноцененнаказанию м
ыпожелалисмертидругомутеперьмыталисамиэтимдругимисамиумерлитутпсихоаналити
ческоеучениеутверждаетчтоэтотдругойдлямальчикаобычноотецииименуемыйистериейпри
падокявляетсятакимобразомсамонаказаниемзапожеланиесмертиненавистномуотц

Висновки

У ході роботи ми набули навичок частотного аналізу на прикладі шифру афінної підстановки. Створили принцип роботи розпізнавача російської мови, для перевірки правильності розшифрування, використовуючи перевірку частот частих літер (о, а, е). Завдяки тому, що афінний шифр зберігає статистичні властивості мови, пов’язані із частотами біграм, вдалося здійснили атаку на афінний шифр знаючи шифрований текст.