КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3
Криптоаналіз афінної біграмної підстановки

Роботу виконали:
студенти групи ФБ-14
Антонова Олександра і Веденкін Артем

Київ-2023

Варіант 8

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 (a,b) шляхом розв'язання системи (1).
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

1. Реалізуємо програми з такими математичними операціями: знаходження НСД, обчислення оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язування лінійних порівнянь, які потрібно буде обчислювати для кожної утвореної системи кандидатів (a,b) на ключ.

```
# НСД
def gcd(a, b):
    while b:
```

```
        a, b = b, a % b
    return a

# обчисленням оберненого елементу за модулем із використанням
розширеного алгоритму Евкліда
def extended_gcd(a, b):
    if a == 0:
        return b, 0, 1
    else:
        g, x, y = extended_gcd(b % a, a)
        return g, y - (b // a) * x, x

def modinv(a, m):
    g, x, y = extended_gcd(a, m)
    if g != 1:
        raise Exception('Modular inverse does not exist')
    else:
        return (x % m + m) % m

# розв'язуванням лінійних порівнянь
def solve_linear_equation(a, b, m):
    d, x, y = extended_gcd(a, m)
    ans = []
    if b % d == 0:
        a, b, m = a // d, b // d, m // d
        inv_a = modinv(a, m)
        x = (inv_a * b) % m
        for i in range(d):
            ans.append((x + i * m) % (m * d))
    return ans
```

2. Використаємо функцію обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1 для обчислення 5 найчастіших біграм даного шифртексту згідно нашого варіанту, і отримуємо:

```
5 найчастіших біграм шифртексту:  [('дэ', 0.008054592236268 04), ('цэ', 0.007942722899
653205), ('жц', 0.007718984226423537), ('нц', 0.006824029533504867), ('оц', 0.0068240
29533504867)]
```

Відповідно 5 найчастіших біграм російської мови відкритого тексту нам відомо:

['ст', 'но', 'то', 'на', 'ен']

3. Потім співставляємо знайдені біграми шифртексту із біграмами відкритого тексту (користуємося тільки 5 найчастішими) і знаходимо кандидатів на ключ шляхом розв’язування системи.

Всі кандидати на ключ:

[(420, 931), (606, 466), (358, 125), (920, 394), (641, 611), (52, 642), (553, 521), (894, 149), (119, 645), (79, 900), (265, 435), (17, 94), (951, 394), (672, 611), (83, 642), (88, 800), (429, 428), (615, 924), (541, 390), (882, 18), (41, 927), (10, 524), (408, 800), (873, 118), (355, 111), (696, 700), (320, 927), (289, 524), (67, 428), (532, 707), (603, 483), (944, 111), (909, 927), (878, 524), (842, 924), (346, 242), (957, 859), (461, 115), (802, 146), (378, 130), (161, 285), (130, 719), (585, 859), (89, 115), (430, 146), (936, 564), (719, 719), (688, 192), (4, 462), (376, 59), (583, 230), (25, 354), (500, 462), (872, 59), (800, 292), (242, 416), (159, 462), (531, 59), (831, 850), (273, 13), (603, 235), (417, 917), (665, 328), (15, 221), (46, 748), (77, 314), (108, 841), (139, 407), (170, 934), (201, 500), (232, 66), (263, 593), (294, 159), (325, 686), (356, 252), (387, 779), (418, 345), (449, 872), (480, 438), (511, 4), (542, 531), (573, 97), (604, 624), (635, 190), (666, 717), (697, 283), (728, 810), (759, 376), (790, 903), (821, 469), (852, 35), (883, 562), (914, 128), (945, 655), (864, 859), (368, 115), (709, 146), (409, 688), (192, 843), (161, 316), (944, 824), (758, 545), (45, 917), (16, 207), (47, 734), (78, 300), (109, 827), (140, 393), (171, 920), (202, 486), (233, 52), (264, 579), (295, 145), (326, 672), (357, 238), (388, 765), (419, 331), (450, 858), (481, 424), (512, 951), (543, 517), (574, 83), (605, 610), (636, 176), (667, 703), (698, 269), (729, 796), (760, 362), (791, 889), (822, 455), (853, 21), (884, 548), (915, 114), (946, 641), (492, 859), (957, 115), (337, 146), (6, 161), (750, 316), (719, 750), (358, 125), (17, 94), (11, 643), (42, 209), (73, 736), (104, 302), (135, 829), (166, 395), (197, 922), (228, 488), (259, 54), (290, 581), (321, 147), (352, 674), (383, 240), (414, 767), (445, 333), (476, 860), (507, 426), (538, 953), (569, 519), (600, 85), (631, 612), (662, 178), (693, 705), (724, 271), (755, 798), (786, 364), (817, 891), (848, 457), (879, 23), (910, 550), (941, 116), (17, 94), (48, 621), (79, 187), (110, 714), (141, 280), (172, 807), (203, 373), (234, 900), (265, 466), (296, 32), (327, 559), (358, 125), (389, 652), (420, 218), (451, 745), (482, 311), (513, 838), (544, 404), (575, 931), (606, 497), (637, 63), (668, 590), (699, 156), (730, 683), (761, 249), (792, 776), (823, 342), (854, 869), (885, 435), (916, 1), (947, 528), (97, 462), (469, 59), (552, 633), (955, 757), (544, 621), (203, 590), (20, 517), (51, 83), (82, 610), (113, 176), (144, 703), (175, 269), (206, 796), (237, 362), (268, 889), (299, 455), (330, 21), (361, 548), (392, 114), (423, 641), (454, 207), (485, 734), (516, 300), (547, 827), (578,

393), (609, 920), (640, 486), (671, 52), (702, 579), (733, 145), (764, 672), (795, 238), (826, 765), (857, 331), (888, 858), (919, 424), (950, 951), (6, 837), (37, 403), (68, 930), (99, 496), (130, 62), (161, 589), (192, 155), (223, 682), (254, 248), (285, 775), (316, 341), (347, 868), (378, 434), (409, 0), (440, 527), (471, 93), (502, 620), (533, 186), (564, 713), (595, 279), (626, 806), (657, 372), (688, 899), (719, 465), (750, 31), (781, 558), (812, 124), (843, 651), (874, 217), (905, 744), (936, 310), (593, 462), (4, 59), (769, 695), (211, 819), (296, 280), (916, 249), (14, 136), (45, 663), (76, 229), (107, 756), (138, 322), (169, 849), (200, 415), (231, 942), (262, 508), (293, 74), (324, 601), (355, 167), (386, 694), (417, 260), (448, 787), (479, 353), (510, 880), (541, 446), (572, 12), (603, 539), (634, 105), (665, 632), (696, 198), (727, 725), (758, 291), (789, 818), (820, 384), (851, 911), (882, 477), (913, 43), (944, 570), (25, 571), (56, 137), (87, 664), (118, 230), (149, 757), (180, 323), (211, 850), (242, 416), (273, 943), (304, 509), (335, 75), (366, 602), (397, 168), (428, 695), (459, 261), (490, 788), (521, 354), (552, 881), (583, 447), (614, 13), (645, 540), (676, 106), (707, 633), (738, 199), (769, 726), (800, 292), (831, 819), (862, 385), (893, 912), (924, 478), (955, 44), (252, 462), (624, 59), (800, 292), (242, 416), (331, 338), (52, 338), (424, 338), (362, 896), (83, 896), (455, 896), (630, 22), (599, 22), (909, 239), (878, 239), (537, 270), (506, 270)]

4. За допомогою кожного кандидата на ключ розшифровуємо текст та знаходимо правильний ключ із функції перевірки змістовності розшифрованого тексту, використовуючи порівняння значення ентропії відкритого тексту російської мови і ентропії розшифрованого тексту.

```
Пара правильних ключів:  (17, 94)
```

Розшифрований текст:

мальчикизаулыбалисьисжаромвзялисьзаделоонирвализолотистыецветыцв етычтонаводняютвесьмирпереплескиваютсяслужаекнамощеныеулицыти хонькостучатсявпрозрачныеокнапогребовнезнаютугомонуиудержуивсевок ругзаливаютслепящимсверканиемрасплавленногосолнцакаждоелетоонито чносцеписрываютсясказалдедушкапустьихянепротиввонихсколькостоятг ордыекакльвыпосмотришьнанихподольшетакипрожгутутебявглазахдырк уведьпростойцветокможносказатьсорнаятраваниктоеенезамечаетамыу важаемсчитаемодуванчикблагородноерастениеонинабралиполныемешкио дуванчиковиунесливнизвпогребвывалилиихизмешковивотьмепогребаразлило

сьсияниевинныйпрессдожидалсяихоткрытыйхолодныйзолотистыйпотокс
огрелегодедушкапередвинулпрессповернулручкузавертелбыстрейбыстрейи
прессмягкостиснулдобычунувотвоттаксперватонкойструйкойпотомвсещ
едреeобильнеепобежалпожелобувглиняныекувшинысокпрекрасногожарког
омесяцаемудалиперебродитьснялипенуиразлиливчистыебутылкиизподкет
чупаионивыстроилисьрядаминаполкахпоблескиваявсумракепогребавиноизо
дуванчиковсамыеэтисловаточнолетонаязыкевиноизодуванчиковпойманное
изакупоренноевбутылкилетоитеперькогдадугласзналпонастоящемузналчт
оонживойчтоонзатемиходитпоземлечтобывидетьиощущатьмиронпоняле
щеоднонадочастицувсегочтоонузналчастицуэтогоособенногоднянсбора
одуванчиковтожезакупоритьисохранитьапотомнастанеттакойзимнийян
варскийденькогдавалитгустойснегисолнцаужедавнымдавноniктоневидели
можетбытьэточудопозабылосьихорошобыегосновавспомнитьвоттогдао
негооткупоритведьэтолетонепременнобудетлетомнежданныхчудесинадо
всеихсберечьигдетоотложитьдлясебячтобыпослевлюбойчаскогдавздумае
шьпробратьсянацыпочкахвовлажныйсумракипротянутьрукуитамрядзаря
домбудутстоятьбутылкисвиномизодуванчиковонобудетмягкомерцатьточ
нораскрывающиесяназарецветыасквозьтонкийслойпылибудетпоблескива
тьсолнценынешнегоиюнявзглянисквозьэтовинонахолодныйзимнийденьисне
грастаетизподнегопокажетсятраванадеревьяхоживутптицылиствацице
тысловномириадыбабочекзатрепещутнаветруидажехолодноесероенебос
танетголубымвозьмилетоврукуналейлетовбокалвсамыйкрохотныйконечн
оизкакоготолькоисделаешьединственныйтерпкийглотокподнесиегокгубам
ипожиламтвоимвместолютойзимыпобежитжаркоелетотеперьдождево
йводыконечноздесьгодитсятолькочистейшаяводадальнихозерсладостныер
осыбархатныхлуговчтовозносятсяназарекраспахнувшимсянавстречунебес
амтамвпрохладныхвысяхонисобиралисьчистоомытымигроздьямиветермч
алихзасотнимильзаряжаяпопутиэлектрическимизарядамиэтаводавобрала
вкаждуюсвоюкаплюещебольшенебескогдападаладождемназемлюонавпита
лавсебявосточныйветеризападныйисеверныйиюжныйиобратиласьвдождь
адождьвэтотчассвященнодействияужестановитсятерпкимвиномдугласс
хватилковшвыбежалводвориглубокопогрузилеговбочоноксдождевойводойв
отонаводабылаточношелкпрозрачныйголубоватыйшелкеслиеевыпитьонак
оснетсягубгорласердцамягкокакласканоковшиполноеведронадоотнестивп
огребчтобыводапропиталатамвесьурожайодуванчиковструямиречекигор
ныхручьевдажебабушкавкакойнибудьфевральскийденькогдабеснуетсязаок
номвьюгаислепитвесьмириулюдейзахватываетдыханьедажебабушкатихо

нькоспуститсявпогребнаверхувбольшомдомебудеткашельчиханьехриплыег
олосаистонычпростуженнымдетямоченьбольнобудетглотатьаносыунихпо
краснеютточновишнивынутыеизналивкивсюдувдомепритаитсяковарный
микробитогдаизпогребавозникнеточнобогинялетабабушкапрячатотоп
одвязанойшальюонапринесетэточтотовкомнатукаждогоболящегоиразоль
етдушистоепрозрачноевпрозрачныестаканыистаканыэтиосушатоднимгл
откомлекарствоиныхвременбальзамизсолнечныхлучейипраздногоавгустовс
когополудняедваслышныйстукколестележкисмороженымчтокатитсяпом
ощенымулицамшорохсеребристогофейерверкачторассыпаетсявысоковнеб
еишелестсрезанноитравыфонтаномбьющейизподкосилкичтодвижетсяпо
лугампомуравьиномуцарствувсеэтовсеводномстаканедадажебабушкакогд
аспуститсявзимнийпогребзаиюнемнавернобудетстоятьтамтихонькосовс
емоднавтайномединениисосвоимсокровеннымсосвоейдушойкакидедушкаип
апаидядябертидругиетожесловнобеседуястеньюдавноушедшихднейспикни
камистеплымдождемсзапахомпшеничныхполейижареныхкукурузныхзерен
исвежескошенногосенадажебабушкабудетповторятьсноваисноватежечу
десныезолотящиесясловачтозвучатсейчаскогдацветыкладутподпресскакб
удутихповторятькаждуюзимувсебелыезимывовсевременасноваисноваониб
удутслетатьсгубкакулыбкакакнежданныйсолнечныйзайчиквотьмевиноизо
дуванчиковвиноизодуванчиковвиноизодуванчиковонприходилинеслышноухо
дилипочтибесшумнотравапригибаласьираспрямлялась вновьонискользилив
низпохолмамточнотениоблаковэтобежалилетниемальчишкидугласотстал
изаблудилсязадыхаясьотбыстрогобегаоностановилсянакраюовраганасамо
йкромкенадпропастьюиоттуданнегодохнулохолодомнавостривушиточно
оленьонвдругучуялстаруюкакмиропасностьгородраспалсяздесьнадвеполов
иныздесьокончиласьцивилизацияздесьживетлишьвспухшаяземляежечасносо
вершаетсямиллионсмертейирожденийиздесьпроторенныеилиещенепрото
ренныетропытвердятчтобыстатьмужчинамимальчишкидолжныстранс
твоватьвсегдавсюжизньстранствоватьдугласобернулсяэтатропаогромн
ойпыльнойзмеейскользиткледяномудомугдевзолотыелетниеднипрячетсязи
маатабежиткраскаленнымпесчанымберегамиюльскогоозераавонтакдерев
ьямгдемальчишкипрячутсямежлистьевточнотерпкиеещенезрелыеплодыд
икойяблониитамрастутизреютавотэтакперсиковомусадуквиноградникук
огороднымгрядамгдедремлютнасолнцеарбузыполосатыесловнокошкитигр
овоймастиэтатропазаросшаякапризнаяизвилистаятянетсякшколеатапр
ямаякакстрелаксубботнимутренникамгдепоказываютковбойскиефильмыв
отэтавдольручьякдикойлеснойчащедугласзажмурилсяктоскажетгдеконча

етсягородиначинаетсялеснаяглушьктоскажетгородврастаетвнееилионап
ереходитвгородиздавнаинавекисуществуетнекаянеуловимаяграньгдеборю
тсядвесилыиоднанавремяпобеждаетизавладеваетпросекойлощинойлужай
койдеревомкустомбескрайнееморетравицветовплещетсядалековполяхвокр
угодинокихфермалетомзеленыйприбойяростноподступаетксамомугородун
очьзаночьючащилугадальниепросторыстекаютпооврагувсеближезахлест
ываютгородзапахомводыитравигородсловнопустеетмертвеетивновьуход
итвземлюикаждоеутрооврагещеглубжевгрызаетсявгородигрозитпоглоти
тьгаражиточнодырявыелодчонкиипожратьдопотопныеавтомобилиоста
вленныенамилостьдождяиразедаемыержавчиной эйаусквозьтайныоврагаи
городаивременимчалисьджонхафичарливудменэйдугласмедленнодвинулсяп
отропинкеконечноеслихочешьпосмотретьнадвесамыеглавныевещикакжив
етчеловекикакживетприроданадоприйтисюдаковрагуведьгородвконцекон
цоввсеголишьбольшойпотрепанныйбурямикорабльнанемполнонародуивсехл
опочутбезусталивычерпываютводуобкалываютржавчинупоройкакаянибу
дьшлюпкахибаркадетищекораблясмытоенеслышнойбурейвременитонетв
молчаливыхволнахтермитовимуравьевраспахнутойовражьейпастичтоб
ыощутитькакмелькаюткузнечикиишуршатвжаркихтравахточносухаябум
агачтобыоглохнутьподпеленойтончайшейпылиинаконецрухнутьградомка
мнейипотокомсмолыкакрушатсятлеющиеугликостразажженногогромом
исинеймолниейнамигозарившейторжестволесныхдебрейтаквотзначитчт
отянулосюдадугласатайнаявойначеловекаприродойизгодавгодчеловекпох
ищаетчтотоуприродыаприродавновьберетсвоеиникогдагородпонастояще
мудоконцанепобеждаетвечноемугрозитбезмолвнаяопасностьонвооружилс
якосилкойитяпкойогромныминожницамионподрезаеткустыиопрыскивает
ядомвредныхбукашекигусеницонупрямоплыветвпередпокаемувелитцивилиз
ацияпокаждыйдомтогоиглядизахлестнутзеленыеволныисхоронятнавекиа
когданибудьслицаземлиисчезнетпоследнийчеловекиегокосилкиисадовыелоп
атыизеденныержавчинойрассыплютсявпрахгородчащадомаоврагдугласоз
адаченномигаетнокакаяжесвязьмежчеловекомиприродойкакпонятьчтозна
чатонидругдлядругакогдаонопустилглазапервыйлетнийобрядпозадиодуван
чикисобраныизаготовленывпрокпораприступатьковторомунодугласзасты
линедвижетсясместадугпошлидугголосазатихливдалекеяживойсказалдугл
асночтотолкуониещебольшеживыечемякакжеэтокакжетаконстоялводин
очествеглядянасвоиногиневсилахдвинутьсясместаинаконецпонялвтотвече
рдугласвозвращалсядомойизкиновместесродителямиибратомтомомиувид
елихвяркоосвещеннойвитринемагазинатеннисныетуфлидугласпоспешноот

велглазаноегоногиужеощутилиприкосновениепарусиныизаскользилиповозду
хубыстрейбыстрейземлязавертелась захлопалиполотняныенавесынадвитр
инамитакойонподнялветертаконмчалсяродителиитомшагалинеторопясь
амеждунимипятясьзадомшелдугласинесводилглазстеннисныхтуфельтамп
озадивполуночнойвитринехорошаябылакартинасказаламамаагабуркнулдуг
ласстоялиюньдавноминовалотовремякогданалетопокупаюттакиетуфлил
егкиеитихиеточнотеплыйдождьчтошуршитпотротуарамужеиюньиземл
яполнапервозданнойсилыивсевокругдвижетсяирастеттраваипосейденьпе
реливаетсясюдаизлуговомываеттротуарыподступаеткдомамкажетсягор
одвотвотчерпнетбортомипокорнопойдетнадноивзеленомморетравнеост
анетсянивсплесканирябидуглас вдругзастылточновросвмертвыйасфальти
красныйкирпичулицыневсилахтронутьсясместапапвыпалилонвонтамвокн
етеннисныетуфлиотецдаженеобернулсяазачемтебеновыетуфлискажипо
жалуйстаможешьтымнеобяснитьнуудазатемчтовнихчувствуешьсебята
кбудтовпервыевэтолетоскинулбашмакиипобежалбосикомпотраветочновз
имнююночьвысунулногиизподтеплогоодеялаиподставилветручтодышитхо
лодомвоткрытоеокноионистынутстынутапотомвтягиваешьихобратнопо
ододеялоионисовсемкаксосулькивтеннисныхтуфляхчувствуешьсебятакбуд
товпервыевэтолетобредешьбосикомполенивомуручьюивпрозрачнойводеви
дишькактвоиногиступаютподнубудтоонипереломилисьидвижутсячутьвп
ередитебяпотомучтоведьвводевсевидитсянетакпапсказалдугласэтоочень
труднообяснитьаа

Висновки:

У ході виконання комп’ютерного практикуму при розшифруванні тексту російської мови афінною підстановкою, використовуємо набуті навички частотного аналізу при порівнянні ентропій ВТ і ШТ для перевірки тексту на змістовність, а також опановуємо прийоми роботи в модулярній арифметиці для знаходження кандидатів ключа