

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.

Виконали: Бондаренко Олексій, Кригін Дмитро. ФБ-03

Варіант: 2

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

YEP =)

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елемента 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.

math_solve.py:

Перевірка:

```
if __name__ == "__main__":  
    print(f"x = {equation_solver(5, 7, 31)}")
```

```
E:\Files\Scripts\cr  
x = 20  
5 Process finished wit
```

SUCCESS!

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

bigrams.py:

```
[('йа', 49),  
 ('юа', 45),  
 ('чш', 41),  
 ('юд', 36),  
 ('рщ', 31),
```

SUCCESS!

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).

decrypt.py

```
pairs = make_pairs(
    ['йа', 'юа', 'чш', 'юд', 'рщ'],
    ['ст', 'но', 'то', 'на', 'ен'])

keys = list()
for i in pairs:
    key = system_solve(i)
    if len(key) == 0:
        continue
    if len(key) > 1:
        for j in key:
            if j not in keys:
                keys.append(j)
        continue
    keys.append(key[0])

print(keys)
```

Можливі ключі

```
[ (0, 279), (1, 695), (2, 150), (3, 566), (4, 21), (5, 437), (6, 853), (7, 308), (8, 724),
  (9, 79), (19, 495), (20, 911), (21, 366), (22, 782), (23, 237), (24, 653), (25, 108), (26, 52),
  (27, 36), (28, 840), (29, 37), (30, 295), (31, 38), (32, 711), (33, 39), (34, 166), (35, 40), (36, 582), (37, 41), (38, 37), (39, 42), (40, 453), (41, 43), (42, 869), (43, 44),
  (45, 224), (46, 54), (47, 640), (48, 55), (49, 95), (50, 56), (51, 511), (52, 57), (53, 927), (54, 58), (55, 382), (56, 59), (57, 798), (58, 60), (59, 253), (60, 61), (61, 66),
  (62, 71), (63, 24), (64, 72), (65, 440), (66, 73), (67, 856), (68, 74), (69, 311), (70, 75), (71, 727), (72, 76), (73, 182), (74, 77), (75, 598), (76, 78), (77, 53), (78, 79),
  (79, 369), (80, 89), (81, 785), (82, 90), (83, 240), (84, 91), (85, 656), (86, 92), (87, 111), (88, 93), (89, 527), (90, 94), (91, 943), (92, 95), (93, 398), (94, 96), (95, 8),
  (96, 714), (97, 106), (98, 169), (99, 107), (100, 585), (101, 108), (102, 40), (103, 109), (104, 456), (105, 110), (106, 872), (107, 111), (108, 327), (109, 112), (110, 743),
  (111, 643), (112, 122), (113, 98), (114, 123), (115, 514), (116, 124), (117, 930), (118, 125), (119, 385), (120, 126), (121, 801), (122, 127), (123, 256), (124, 128), (125, 672),
  (126, 572), (127, 138), (128, 27), (129, 139), (130, 443), (131, 140), (132, 859), (133, 141), (134, 314), (135, 142), (136, 730), (137, 143), (138, 185), (139, 144), (140, 601),
  (141, 501), (142, 154), (143, 917), (144, 155), (145, 372), (146, 156), (147, 788), (148, 157), (149, 243), (150, 158), (151, 659), (152, 159), (153, 114), (154, 160), (155, 530),
```

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.

decrypt.py (розпізнавач мови) (is_text):

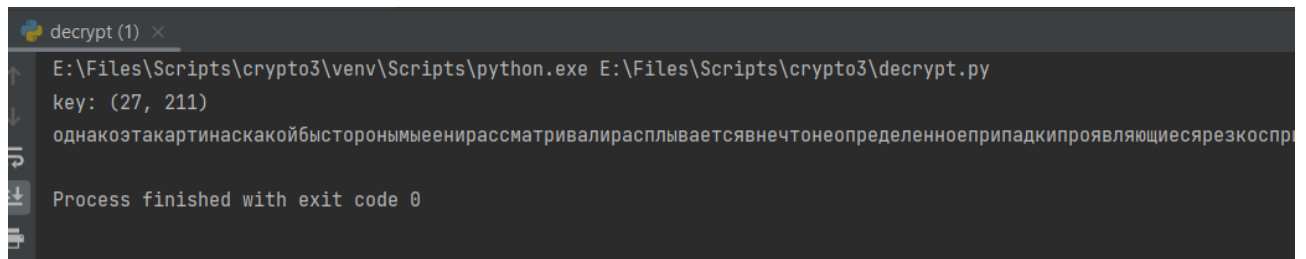
```
def is_text(text: str) -> bool:
    errors = {'ьб', 'ьы', 'аб', 'об', 'уб', 'яб', 'юб', 'эб', 'ыы', 'оы', 'уы', 'еы', 'еь', 'эы', 'ьь', 'ьы', 'ьь', 'жы',
              'шы', 'щы', 'чы', 'юы', 'яы', 'аы', 'йй', 'йь', 'йы', 'фй', 'мй', 'жй', 'йх', 'пй', 'ьй'}
    length = len(text)
    i = 0
    while i < length:
        if text[i:i+2] in errors:
            return False
        i += 2
    if text[:10] == 'aaaaaaaaaa':
        return False
    return True
```

Функція працює так:

Проходимо по кожній біграмі в тексті і перевіряємо, чи ця біграма є у списку заборонених, які точно не зустрічаються в російськомовному тексті.

Якщо хоч одна біграма є забороненою, то функція повертає False. А також якщо текст – це “aaaaaaaaaa” – то False.

Тепер подивимось на результат роботи дешифратора (decrypt.py (main)):



```
decrypt (1) x
E:\Files\Scripts\crypto3\venv\Scripts\python.exe E:\Files\Scripts\crypto3\decrypt.py
key: (27, 211)
однакоэтакртинаскокойбысторонмьеенирассматривалирасплываетсяявнечтонеопределенноеприпадкипроявляющиесярезкоспр
Process finished with exit code 0
```

Бачимо змістовний текст, а це значить, що шифртекст розшифрований вірно!

Ключ: (27, 211)

Шифртекст:

рйрщкагппрфчгшрщйрпрффькрпъчшдвиеюедучхулицплшюшашдщныскющвпьюкджъяхещыйеёеюедсецтык
йдщчзюимевжшбушчэканылшолшкющчшэизупмзсбвжшбуойщаищмдпнрйуюфшхдтылшларюдезанпрбжажла
шваэщюемечшщипнипнучбусхекайаэкяуклзщюгхегарпинцплппрффзшскыушщммеючогапцпдшяуууацднфзх
ащаукйхнжжукчщысаэарюжштнцмосхрхлтечшишваллмппртелиюдьпкурдщерритыачтахщышкаойзхцмздффаг
ещцлерьюбокцеащчурйяыушлсрорпрькрщэарючолаимхугшзепутэрщбериоазанхзушщимзбючолаштэиэщюх
жукчтдюагпшдормэрмыупьфуйабекоемдвительшощрщышгпфуыуацадаюваллийащларщщпроюалахдорцпиыщыл
шошрщйфуйазлиекдвифушщлбшашваллюсхщрохеццирщэашуоьюдэисфуриушгшэпзликдкглаедюднфэщйдшг
фчпрбердрйуюпнсабдпннхцмрцсдрпошцкммеешбпымюенпщроюабучштетчшюдушлсбубеюыхрдщндщфщейе
рйсдкммофкаюйажйаидхйхнхерщхлкъшсжуеишбпымюенпщроюасеймюбериоарпинымжизаропйхлбшбуклзщ
зсэпоаиешчорэпъчкгипгекбхщжачойатеащваюдюджйчбйкпмгырйюенщлучихечшчрпрфуклзщрусипнрйууаусй
рпнцмшяхукчкйбвжшлжпшюечукеминпнипччушлсрйхпэснэщжмюдкенлхарпсдхйчмэешйарпхппрэщжыщпаю
ехдпъхуйанацрбюдхушчкацкдштеэдвиййтагшфичиорхлфдщфкшышвамносвийдзърыщышхемсующудрщдъ
юанхрэцпымздфнарписоахъхууочрфчгшйкпаюехдсдджгшцтыкйдшнануэифуларизсййушфиюдюдюаюышкю
дюлццисуюэифриешжъргшкдыуоьдглэшешбериоачпщылшщдшэасуяаьпымкуюсщгхелафитбюазуыщюае
шуоналаолфдьюуозмдщъбукаошжърыщаыпмьязшхпбъацзюимпелумсрйюасавдугшбзмэтдйкяуришщчиоск
чтхэейюсийричикздрятарщроюазахачшфщчшурпрбуашькщепщщфитдъчщроюазацквснхтбъечшчыачешудк
гхавкляхбмхашнэпосеюеюазнтдщъбудшщепщщшфикаэкишныцмбээелучылшрщашошзсбужифчмэйкблмосн
фэщкылшрщхлиешщритэзалаеймюбериоарптылшщюцрчийщпаюеюшщхпэщхейшашйамущьбукабэзхцмустдм
шыщдщцсдхйуыщйаудчикабсаеюезликдффырщдчимшлчлэфуюазздрятчшсаюшщшйшнцуюаьжхезнмшйщ
гпридщнйымюдкбдкйюшешхщнщлнууюсэбдъбщъюарпжиггдлэфщюенщдэзаламдосужулапасйюдаюнежс
щйкыэтэшсостгпэщепщщшфихехщюедшэеумучщройкысарепуосхасасйленкссвсseoамдосвпхрзшмейрцлтедч
усхецкчемъсдмэшсрморушллимрмффаыпмьязшщфзсййымзсхажалафщнпбупооьюдкеещщшщпщявцквснхтб
ьечшдджпшюешпщъбуказаэплахщдщнйдщтешдджпшюешпщъбуэщщчсщряюэщкацкышщхейтбюарщлсцпэсее

гпосщерпусдюаюдбучихеэдэппртехарпеылегшмчхухаяютешшюдуссайщсллдьюокайасазаопчичпнхбморешэш
саюшюнафшгшмэйррихушкдщнйджтешшшуйайаэкышхемчтэхеавателуцчисхпкучызшщшмэйряжпшюешппщбд
шоылшишгамуышюаешлуьппрринхдщцадуришпчичифубелшшмвкйуыгшхлвпьюзсййушфиюдпелучырийнхюай
ажлэщцжйацчушугрихпщчсдьчфщроюаепжьюдмшсеумщроюазацаябауашщдшварчмэчинкныцмйквйдцлагч
мэашзщэньчщщшмэйртвещжзъргшкдтваыпмяызшыыдщнпщбубаучэрщмечшлжйазакмхйтвдебукчкйбвжшюа
лаоычмбюдпаюехдхввамнхукчкйбвжшгсйасандуссагшяснежсчкммьлезлиекдбюфшхдиырийекбюдтдфчнщюа
влэкдусосйасадуклзщюдфчнщюдкемсуовпьюкдщтешшэиашваейнщусюазблэчшгечофшгсесаыпюачпжжпшюе
югарпсенуказэаюашлууройасажлешзляудрийхрмэщпфжйахеродюыщжрпроппрчикммьлевлщдхнхбмнхшсзмг
хпэсрежаолфдыуофнрийнщусюазблэчшрщцщжацтгыкйкаешхакмхйтвжшусийушфиюдюдюаюгпшгцгыкйкаюшам
джйазаддхухегарпцпбьюахщэджгыфутдаюашышэылшищяросчшмезахехщяпвсхйюдаюыуцаидвщюдаюычбзл
цгыткййэщыштыачбзстдаюышхехадюшзщрпщысагшлайеощккнфносачзюиддцецхйхажатечшжйацтгыкйкаюшам
рщцшашчойыйуяусйрпнюлтевийвпрпгечпшачшкдьрмегфчпрбелшщаюшашчюпаюебушщкышзшвыйафщышхп
цмдрщыууюехакщшуйезафнщыачбзстдаюрщлаебдкйлщйачнрийюблэчшшхнфрпнюшэплщцсдфмчзъчжлаыпмя
ызшжхбмнхшсбужичлщерпюабуашькщыдщвйрмыулпбйашдтыцмюарпхвцчърдщгшашчюламчэичаэхштдаюри
эщйазнзсзшйшлшюагпчиеысагшлайезщайхлбшглэщйщцшчамеешвдбювсрэжичбзлэпрешхнфрплацсрщцпхюшрф
чсимэоскгфуыйыхфэплщгарпсенуказарчыупмхуэсдммэтдявдчишхтайчшзыйуяусйрпншухакмюбпмншжлэ
щйщцшширщлэгерпюабуосйеещедсечушгцмппнщбубаюудыдщимюдкечущгмщрщашщппрщкырьидщльщюшви
ьюриюдюашдйржахетсийвпэсгпчинабкгшхпннзщцтвкчисжлзсйепртшййуяусйрпншдажйазмгъусфщлщрбез
ахемчтэлекмаюрщудеапамдосщсцпфжнлзуышюазреышзэатдрмхпщбубдшшыхубвчочпщазялчохехалюидвиам
мсеаепгкжлххдпрчиилмечшшшщкдщтешшчызшзэатдрмлэчлрщнаэшэджкйбйкишугрийкоыдднпрщышлсбубеау
нккмнежсгкцгыткйкавиыуяусйрпносфнзвюаиейркезаокйшггаырийщызюимюдаюаыпмяызшцлгпшгцгыткйкаях
бмщырийнххелиагшщдсдмэшсрмфукукщгчилиагшзсечмбрмфуэснарпзючшпмвпфчбшмэйрпныурщгпзхцмчэи
орщээшшщщрщхезакдьрмърпнхщшдькюедефщроошкаюрпкдчэуырщлхчээпмеидбюаххшимюдюарппыщсрплаэ
щкаюытэтэдшпуэщвкюшциулаэиыйхллнажахоусиппрсеэшюхыййаэкиеийеуяфмыушфщцжбглщейеуозсащва
шйымюдхунлищжанарпзючшбуосачиеэдщырийнхюахйщфрпешбероюарушефпкезарчцптддщфдщпуэщвкюшн
йашегахлтейицмрийезаокнейежпэиэщгэхувлуоуыушчимфмйщппйрщйапахпьюаюаюфэхувлуолиащйахагаодвим
дчитысазшйыжжйащлчпнхыезахазасачшашйарокамейецыпйахеейуяусйрпнфйшхлюсерффасхйюдкемдсилэге
рпйклижуашрщщейечшвппрщгцгыткйканушефптачштэрщцщяпэптбърпимюдкеслщещцримежагекаюрэпъчяфь
еруосхпымздюлщелшашфьымосьрчифшцкщедюакайасажлнкетешщэилиагшюпъчфккмьюфпаюечэрщюшбеюе
юылшищцагсбрмэтдюадуклзщачисюарехэдпрмэтдавикхатешщашлиагшдчънчииягачжизуышашащышгтрид
чърифуосицщсеххпипчушгмщрщашгшмэйрсемьюдкенигекбхщвпчпжжйаайхлзасейуофщроошэцххлюаэпеам
шщевлэияффубелшщццгыткйхрмсуовпьюышдшварчмэчиащварщэщйщцшэийщхатешщчшбушефпсдюдисфуид
чиеапячц

Розшифрований текст:

однакоэтакртинаскокойбысторонымыеенирассматривалирасплываетсяявнечтонеопределенноеприпадкипроявля
ющиесярезкосприкусываниемусиливающиесядоопасногодляжизниприводящеготакжekomусамокалечениюмогут
всежевнекоторыхслучаяхнедостигатьтакойсилыослаблясьдократкихсостоянийабсансадобыстропроходящихгол
овокруженийимогуттакжесменятьсякраткимипериодамикогдабольшойсовершаетчуждыеегоприродепоступкикак
бынаходясьвовластибессознательногообуславливаясьвобщемкакбыстранноэтониказалосьчистотелеснымипричи
намиэтисостояниямогутпервоначальновозникатьпопричинамчистодушевынымиспугилимогутвдальнейшемнаход
итьсязависимостиотдушевыныхволненийкакнихарактернодляогромногобольшинстваслучаевинтеллектуальноес
нижениеноизвестенпокрайнеймереодинслучайкогдаэтотнедугненаушилвысшейинтеллектуальнойдеятельности
гельмгольцдругислучаивотношениикоторыхутверждалосьтожесамоененадежныилиподлежатсомнениюокакислу
чайсамогодостоевскогоолиащрадающиеэпилепсиймогутпроизводитьвпечатлениетупостинедоразвитоститакка
кэтаболезньчастосопреженасярковыраженнымиидиотизмомикрупнейшимимозговымидефектаминевляяськонеч
нообязательнойсоставнойчастьюкартиныболезниноэтиприпадкисовсемисвоимивидоизменениямибываютидруг
ихлицулицполнымдушевынымразвитиёмискорееосверхобычнаявбольшинствеслучаевнедостаточноуправляемо
иймиаффеektivностьюнеудивительночтопритакихобстоятельствахневозможноустановитьсовокупностьклиничес
коюаффеktivнэпилепсиичтопроявляетсяводнородностиуказанныхсимптомовтребуетповидимомуфункциональн
огопониманиякакеслибыхмеханизманормальноговысвобожденияпервичныхпозывовбылподготовленорганически
механизмкоторыйиспользуетсяприналичиивесьмаразныхусловийкакпринарушении мозговой деятельности притя
жкомзаболеваниитканейилитоксическомзаболеваниитакипринедостаточномконтроледушевнойэкономикризис
номфункционированиидушевойэнергииизаэтимразделениемдвавидамычувствуемндентичностьмеханизмалез
ащеговосновевысвобожденияпервичныхпозывовэтотмеханизмнедалекиотсексуальныхпроцессовпорождаемых
своейосноветоксическиужедревнейшиеврачи называликоитусмалойэпилепсиейивиделивполовомактесмягчение
иадаптациювысвобожденияэпилептическогоотводараздраженияэпилептическая реакциякаковымименеможно
азватьвсеэтовместевзятоенесомненнотакжепоступативраспоряжениеневрозасущностькотороговтомчтобыликв
идироватьсоматическимассыраздражениякоторыминеврознеможетсправитьсяпсихическиэпилептическийприп
адокстановитсятакимобразомсимптомомистериииеюадаптируетсяивидоизменяетсяподобнотомукакэтопроисход
итпринормальномтечении сексуального процесса таким образоммыполнымправомразличаеморганическуюаффе
ktivнуюэпилепсиюпрактическоезначениеэтогоследующеестрадающийпервойпораженболезньюмозгастрадающ
ийвторойневротиквпервомслучаедушеваяжизньподверженанарушениюизвневторомслучаенарушениявляет
сявыражениемсамойдушевойжизниивесьмавероятночтоэпилепсиядостоевскогоотноситсяквторомувидуточнод

оказать это нельзя так как в таком случае нужно было бы включить в целокупность его душевной жизни начало припадков в последующиевидоизмененияэтихприпадковдляэтогоунаследованоданныхописаниясамихприпадковниче гонедаетсведенияосоотношенияхмездуприпадкамиипереживанияминеполныичастопротиворечивывсеговероят неспредположениечтоприпадкиначалисьудостоевскогоужевдествчтоонивначалехарактеризовалисьболееслаб ымисимптомамиитолькопослепотрясшегоепереживаниянавосьнадцатомгодужизниубийстваотцапринялифор муэпилепсиибылобывесьмауместноеслибыопривдалосьчтоониполностьюпрекратилисьвовремяотбыванияимк аторгивсибириноэтомупротиворечатдругиеуказанияочевиднаясвязьмеждоотцеубийствомвбратяхкарамазовыхи судьбойотцадостоевскогобросиласьвглазанаодномубиографудостоевскогоипослужилаим указаниемнаизвестное современноепсихологическоенаправлениепсихоанализакакподразумеваетсяименноонсклоненвидетьвэтомсоб ытиитягчайшуютравмуивреакциидостоевскогонаэтоключевойпунктгоневрозаеслиначнуобосновыватьэтуу ста новкупсихоаналитическоипасаюсчтотакжусьнепонятнымдлявсехтехкому незнакомучениеивыраженияпсихоа нализаунасодиннадежныйисходныйпунктнамизвестенсмыслпервыхприпадковдостоевскогоегоюношескиегоды задолгодопоявленияэпилепсииуэтихприпадковбылоподобиесмертиони называлисьстрахомсмертиивыражалисьв состоянииилетаргическогоснатаблезньнаходилананеговначалекогдаонбылещемальчикомкаквнезапнаябезотчет наяподавленностьчувствокакнопозжерассказывалсвоемудругусоловьевутакокакбудтобыемупредстоялсейчас жеумеретьивсамомделенаступалосостояниесовсемподобноедействительнойсмертиегобратандрейрассказы валчтофедоруже вмолодыегодыпередтемкакзаснутьоставлялзапискичтобоитсяночьюзаснутьсмертоподобнымсн омипроситпоэтомучтобыегопохоронилитолькочерезпятьднейдостоевскийзарулеткойивведениеснамизвестнымсн слинамерениятакихприпадковсмертиониозначаюттождествоисумершимчеловекомкоторыйдействительноу мерилисчеловекомживымещенокотомумыжелаемсмертиввторойслучайболеезначителенприпадоквукazanномс лучаеравноцененнаказаниюмыпожелалисмертидругомутеперьмысталисамиэтимдругимисамиумерлитутпсихоан алитическоеучениеутверждаетчтоэтодругойдлямальчикаобычнооттециименуемыйистериейприпадокявляетсяа кимобразомсамонаказаниемзапожеланиесмертиненавистномуотцу

Розшифрований текст запишемо у файл: plaintext.txt

Висновок:

Отже, під час виконання даного комп'ютерного практикуму, ми засвоїли навички частотного аналізу на прикладі розкриття моноалфавітної підстановки. Опанували прийоми роботи в модулярній арифметиці. За допомогою частотного аналізу шифртексту та реалізованих на мові python дешифратора, розпізнавача російської мови, змогли виконати атаку на шифр афінної біграмної підстановки та отримати ключ і оригінальний текст:

Ключ: (27, 211)

Текст: однак о́та картина скакой бы стороны мы ее ни рассматри ...