Міністерство освіти і науки України Національний технічний
університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали:

ФБ-21 Ємець Валерія

Тютюннікова Віолета

Київ 2024

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

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.**

Для розширеного алгоритму Евкліду створено функцію gcd_evc(), обернений елемент за модулем обраховується функцією obratn() з використанням алгоритму Евкліда. Обчислення лінійних порівнянь здійснюється функцією congr(), використовуючи попередні дві.

Розглянемо приклади обрахунку оберненого елементу:

```
(base) violetta@MacBook-Pro-Violetta ~ % /opt/anac
pc/1 сем/крипта/лабы/3лаба/task1.py"
Приклад 1:
Обернений елемент для 3 за модулем 11: 4

Приклад 2:
Обернений елемент для 10 за модулем 17: 12

Приклад 3:
Оберненого елементу для 6 за модулем 15 не існує.
```

Функція успішно обраховує обернений елемент, а також передбачено випадок, коли оберненого елементу не існує.

Тепер розглянемо приклади для лінійних порівнянь, будемо розглядати три основні випадки: єдиний розв'язок, декілька розв'язків та відсутність розв'язків:

```
Приклад 4:
Розв'язки для 6x ≡ 18 (mod 24): [3, 7, 11, 15, 19, 23]

Приклад 5:
Розв'язок для 7x ≡ 5 (mod 13): [10]

Приклад 6:
Для 6x ≡ 5 (mod 12) немає розв'язків.
(base) violetta@MacBook-Pro-Violetta ~ %
```

2. **За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму No1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).**

Для цього візьмемо функцію з першого комп'ютерного практимуму, яка мала наступний вигляд:

```python
#----------БІГРАМИ----------
def bi_calc(text, no_space=False):
    text = filt(text)
    if no_space:
        text = text.replace(' ', '')

    bi_count = {}
    total_bis = 0

    #--------ПЕРЕТИНАЮЧІ----------
    for i in range(0, len(text) - 1):
        bi = text[i:i+2]
        if len(bi) == 2:
            if bi in bi_count:
                bi_count[bi] += 1
            else:
                bi_count[bi] = 1
            total_bis += 1

    bi_fr = {bi: cnt / total_bis for bi, cnt in bi_count.items()}

```

У контексті завдання цього практикуму нас цікавлять лише перетинаючі біграми, тому беремо саме цю частину функції та модифікуємо для виведення 5 найпоширеніших біграм з відповідною частотою:

```
(base) violetta@MacBook-Pro-Violetta Злаба % /opt
3 курс/1 сем/крипта/лабы/Злаба/task2.py"
Частоти 5 найпоширеніших біграм:
'вн': 0.95%
'тн': 0.86%
'дк': 0.85%
'ун': 0.85%
'хщ': 0.81%
(base) violetta@MacBook-Pro-Violetta Злаба %
```

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).**

З методичних вказівок знаємо, що найчастіщі біграми російської мови це «ст», «но», «то», «на», «ен». Також з попереднього кроку знаємо найчастіші біграми шифротексту, на основі цього створюємо два списки:

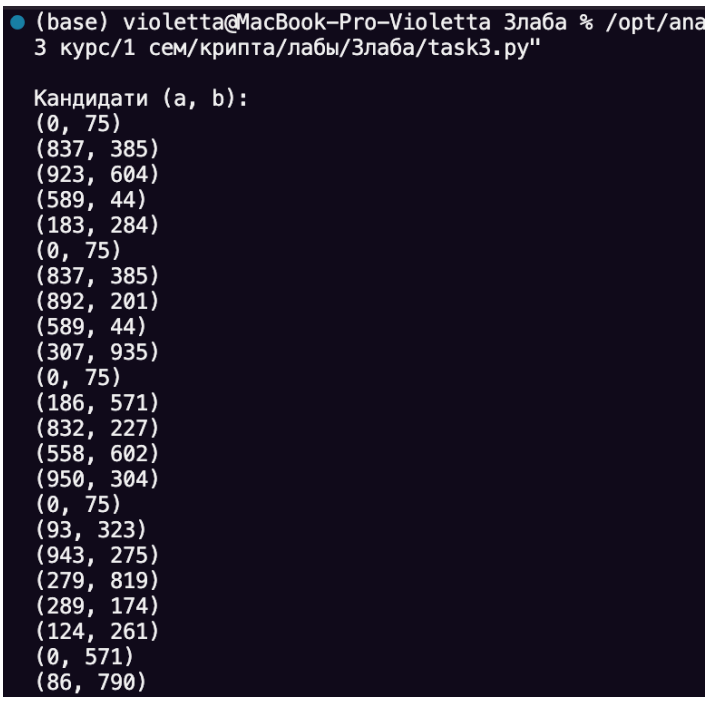
```python
#---------------БІГРАМИ----------------------------
ct_bis = ['вн', 'тн', 'дк', 'ун', 'хщ']
tv_bis = ['ст', 'но', 'то', 'на', 'ен']
```

Кандидатів на ключ будемо знаходити, розв’язуючи систему:

$$\begin{cases} Y^{*} \equiv aX^{*} + b \pmod{m^2} \\ Y^{**} \equiv aX^{**} + b \pmod{m^2} \end{cases},$$

Де припущено що біграма X * перейшла при шифруванні у біграму Y * , а біграма X ** – у біграму Y ** .

Отримали досить велику кількість кандидатів на ключі:



4. **Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.**

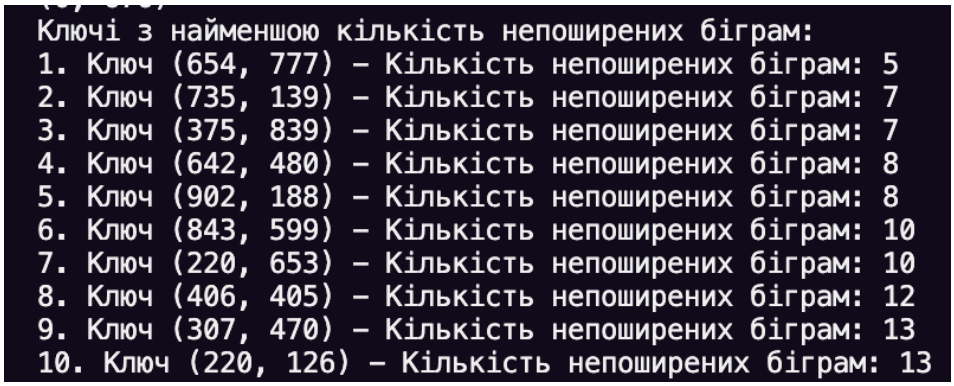
5. **Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.**

Для розпізнання змістовності тексту будемо рахувати скільки разів зустрічаються найнепоширеніші біграми російської мови. Візьмемо 20 непоширених біграм з таблиці, яку отримували при виконанні першого комп’ютерного практикуму:

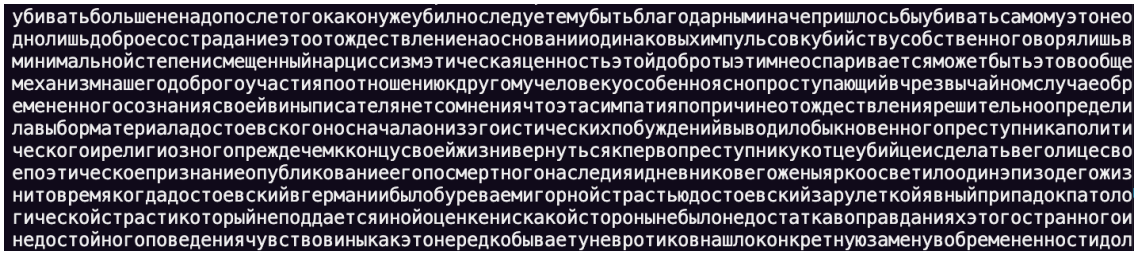
мэ	1,97E-06
хэ	1,97E-06
бц	1,97E-06
оэ	1,97E-06
фм	1,97E-06
вщ	1,97E-06
иэ	1,97E-06
бб	1,97E-06
ёт	1,97E-06
эм	1,97E-06
бт	1,97E-06
фк	1,97E-06

фс	1,97E-06
уу	1,97E-06
ъ	1,97E-06
эг	1,97E-06
лщ	1,97E-06
нж	1,97E-06
дщ	1,97E-06
ыц	1,97E-06
ыя	1,97E-06

Виводимо 10 ключів з найменшою кількістю непоширених біграм і бачимо що при значенні ключа (654, 777) маємо найменшу кількість непоширених біграм, а саме 5.



Спробуємо розшифрувати текст, використовуючи цей ключ:



Дійсно отримали змістований текст.

Відкритий текст:
убиватьбольшененадопослетогокаконужеубилноследуетемубытьблагодарны
миначепришлосьбыубиватьсамомуэтонеоднолишьдоброесостраданиеэтоотож
дествлениенаоснованииодинаковыхимпульсовкубийствусобственноговоряли
шьвминимальнойстепенисмещенныйнарциссизмэтическаяценностьэтойдобр
отыэтимнеоспаривается можетбытьэтовообщемеханизмнашегодоброгоучасти
япоотношениюкдругомучеловекуособенноясноп роступающийвчрезвычайном
случаеобремененного сознанияс воейвиныписателянетсомнениячтоэтасимпати
япопричинеотождествления решительноопределилавыборматериаладостоевск
огоносначалаонизэгоистическихпобужденийвыводилобыкновенногопреступн
икаполитическогоирелигиозногопреждечемкконцусвоейжизнивернутьсякпер
вопреступникукотцеубийцеисделатьвеголицесвоепоэтическоепризнаниеопуб
ликованиеегопосмертногонаследияидневниковегоженыяркоосветилоодинэпи
зодегожизнитовремякогдадостоевскийвгерманиибылобуреваемигорнойстраст
ьюдостоевскийзарулеткойявныйприпадокпатологическойстрастикоторыйнеп
оддаетсяинойоценкенискакойстороны небылонедостаткавоправданияхэтогост
ранногоинедостойногоповеденияч увствовиныкакэтонередкобываетуневротик
овнашлоконкретнуюзаменувобремененностидолгамиидостоевскийморотгова
риватьсятемчтоонпривыигрышеполучилбывозможностьвернутьсявроссиюиз
бежавзаключенияв тюрьмукредиторами ноэтобылтолькопредлогдостоевскийб
ылдостаточнопроницателенчтобыэтопонятьидостаточночестенчтобывэтомпр
изнатьсяонзналчтоглавнымбылаиграсамапосебевсеподробностиегообусловле

нногопервичнымипозывамибезрассудногоповеденияслужаттомудоказательст
вомиещекоечемуиномуоннеуспокаивалсяпоканетерялвсегоиграбыладлянегот
акжесредствомсамонаказаниянесчетноеколичествораздавалонмолодойженесл
овоиличестноесловобольшенеиграть илинеиграть вэтотденьионнарушалэтосло
вокаконарассказываетпочтивсегдаеслионсвоимипроигрышамидоводилсебяие
едокрайнебедственногоположенияэтослужилодлянегоещеоднимпатологическ
имудовлетворениемонмогпереднеюпоноситьиунижатьсебяпроситьеепрезират
ьегораскаиватьсявтомчтоонавышлазамужзанегостарогогрешникаипослевсейэ
тойразгрузкисовестинаследующийденьиграначиналасьсноваимолодаяженапр
ивыклакэтомуциклутаккакзаметилачтотоотчеговдействительноститкоимо
жнобылоожидатьспасенияписательствоникогданепродвигалосьвпередлучшеч
емпослепотеривсегоизакладыванияпоследнегоимуществасвязивсегоэтогоона
конечнонепонималакогдаегочувствовиныбылоудовлетворенонаказаниямикко
торымонсамсебяприговорилтогдаисчезалазатрудненностьвработетогдаонпозв
олялсебесделатьнесколькошаговнапутикуспехурассматриваярассказболеемол
одогописателянетрудноугадаткакиедавнопозабытыедетскиепереживаниянах
одятвыявлениявигорнойстрастиустефанацвейгапосвятившегомеждупрочимдо
стоевскомуодинизсвоихочерковтримастеравсборникесмятениечувствестьнов
елладвадцатьчетыречасавжизниженщиныэтотмаленькийшедеврпоказываетка
кбудтолишьтокакимбезответственнымсуществомявляетсяженщинаинакакиеу
дивительныедлянеесамойзаконо нарушенияеетолкаетнеожиданноежизненное
впечатлениеноновеллаэтаеслиподвергнутьеепсихоаналитическомутолковани
юговоритоднакобезтакойоправдывающейтенденциигораздобольшепоказывае
тсовсеминоеобщечеловеческоеилискореообщемужскоеитакоетолкованиестол
ьявноподсказаночтонетвозможностиегонедопуститьдлясущностихудожестве
нноготворчествахарактерночтописательскоторымменясвязываютдружескиео
тношениявответнамоирасспросыутверждалчтоупомянутоетолкованиеемучуж
доивовсеневходиловегонамерениянесмотрянаточтоврассказвплетенынекотор
ыедеталикакбырассчитанныенаточтобыуказыватьнатайныйследвэтойновелле
великосветскаяпожилаядамаповеряетписателюотомчтоейпришлосьпережить
болеедвадцатилеттомуназадраноовдовевшаяматьдвухсыновейкоторыевнейбо
леененуждалисьотказавшаясяоткакихбытонибылонадеждснасороквторомгоду
жизнионапопадаетвовремяодногоизсвоихбесцельныхпутешествийвигорныйз
алмонакскогоказиногдесредивсехдиковинеевниманиеприковываютдверукико
торыеспотрясающейнепосредственностьюисилойотражаютвсепереживаемые
несчастнымигрокомчувстварукиэтирукикрасивогоюношиписателькакбыбезо
всякогоумысладелаетегоровесникомстаршегосынанаблюдающейзаигройжен
щиныпотерявшеговсеивглубочайшемотчаяниипокидающегозалчтобывпаркеп
окончитьсосвоеюбезнадежнойжизньюнеизяснимаясимпатиязаставляетженщи
нуследоватьзаюношейвпредпринятьвседляегоспасенияонпринимаетеезаодну
измногочисленныхвтомгороденавязчивыхженщинихочетотнееотделатьсяноо
нанепокидаетегоивынужденавконцеконцоввсилусложившихсяобстоятельство
статьсявегономереотеляиразделитьегопостельпослеэтойимпровизированнойл
юбовнойночионавелитказалосьбыуспокоившемусяюношедатьейторжественн
оеобещаниечтоонникогдабольшенебудетиграть снабжаетегоденьгаминаобрат

ныйпутьисосвоейстороныдаетобещаниевстретитьсяснимпередуходомпоездан
авокзаленозатемвнейпробуждаетсябольшаянежностькюношеонаготовапожер
твоватьвсемчтобытолькосохранитьегодлясебяионарешаетотправитьсяснимвм
естевпутешествиевместотогочтобыснимпроститьсявсяческиепомехизадержив
аютееионаопаздываетнапоездвтоскепоисчезнувшемуюношеонасноваприходи
твигорныйдомисвозмущениемобнаруживаеттамтежерукинаканувевозбудивш
иевнейтакуюгорячуюсимпатиюнарушительдолгавернулсякигреонанапоминае
темуобегообещаниииноодержимыйстрастьюонбранитсорвавшуюегоигрувелит
ейубиратьсявонишвыряетденьгикоторымионахотелаеговыкупитьопозоренная
онапокидаетгородавпоследствииузнаетчтоейнеудалосьспастиегоотсамоубийс
твазтаблестящеибезпробеловвмотивировкенаписаннаяновеллаимеетконечноп
равонасуществованиекактаковаяинеможетнепроизвестиначитателябольшогов
печатленияоднакопсихоанализучитчтоонавозникланаосновеумопостроряемого
вожделенияпериодаполовогосозреванияокаковомвожделениинекоторыевспо
минаютсовершенносознательносогласноумопостроряемомувожделениюматьд
олжнасамаввестиюношувполовуюжизньдляспасенияегоотзаслуживающегоп
асенияврадаонанизмастольчастыесублимирующиехудожественныепроизведе
ниявытекаютизтогожепервоисточникапороконанизмазамещаетсяпорокомиго
рнойстрастиударениепоставленноенастрастнуюдеятельностьрукпредательски
свидетельствуетобэтомотводеэнергиидействительноигорнаяодержимостьявля
етсяэквивалентомстаройпотребностивонанизмениоднимсловомкромесловаиг
ранельзяназватьетееаа

Висновки: під час виконанняя комп’ютерного практикуму дослідили логіку шифрування тексту шифром афінної біграмної підстановки та розшифрували віповідний текст. Також ознайомилися з методами розпізнання змістовності тексту та запровадили в програму один з них.