НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

«Криптографія»

Комп’ютерний практикум №3

Студенти: Маврикін Едуард
Слобода Ірина
Група: ФБ-25
Варіант 2

Київ – 2025

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(), обернений елемент за модулем обраховується з використанням алгоритму Евкліда. Обчислення лінійних порівнянь, використовуючи попередні дві. Розглянемо приклади обрахунку оберненого елементу:

```
PS C:\Users\Eduard\Desktop\kpi\crypto\crypto25-26\lab3\Mavrykin_FB_25_Sloboda_FB-25_cp3> python .\task1.py
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.
```

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

```python
def calc(filename):
    with open(filename, 'r', encoding='utf-8') as file:
        text = file.read()
    count = {}
    total = 0

    for i in range(0, len(text) - 1):
        bi = text[i:i+2]
        if len(bi) == 2:
            if bi in count:
                count[bi] += 1
            else:
                count[bi] = 1
            total += 1

    freq = {bi: cnt / total for bi, cnt in count.items()}
    top5 = sorted(freq.items(), key=lambda x: x[1], reverse=True)[:5]
    return freq, top5

filename = '02.txt'
freq, top5 = calc(filename)

print("Частоти 5 найпоширеніших біграм:")
for bigram, f in top5:
    print(f"'{bigram}': {f:.2%}")

```

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:

```
PS C:\Users\Eduard\Desktop\kpi\crypto\crypto25-26\lab3\Mavrykin_FB_25_Sloboda_FB-25_cp3> python .\task2.py
Частоти 5 найпоширеніших біграм:
'йа': 1.00%
'юа': 0.94%
'чш': 0.86%
'рп': 0.82%
'юд': 0.76%
```

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
ct_bis = ['йа', 'юа', 'чш', 'рп', 'юд']
tv_bis = ['ст', 'но', 'то', 'на', 'ен']
```

Система:

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

Результат:

```
PS C:\Users\Eduard\Desktop\kpi\crypto\crypto25-26\lab3\Mavrykin_FB_25_Sloboda_FB-25_cp3> python .\task3.py
5 найчастіших біграм шифртексту: ['йа', 'юа', 'чш', 'рп', 'юд']
5 найчастіших біграм російської мови: ['ст', 'но', 'то', 'на', 'ен']

Кількість кандидатів: 442

Кандидати (a, b):
(0, 279)
(806, 186)
(552, 232)
(779, 486)
(836, 173)
(0, 279)
(806, 186)
(800, 573)
(934, 579)
(557, 390)
(0, 279)
(713, 899)
(660, 954)
```

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:

Виводимо 10 ключів з найменшою кількістю непоширених біграм і бачимо що при значенні ключа (27, 211) маємо найменшу кількість непоширених біграм, а саме 5.

```
Ключі з найменшою кількістю рідкісних біграм:
1. Ключ (27, 211) - Кількість рідкісних біграм: 5
2. Ключ (740, 800) - Кількість рідкісних біграм: 9
3. Ключ (337, 676) - Кількість рідкісних біграм: 10
4. Ключ (833, 459) - Кількість рідкісних біграм: 10
5. Ключ (192, 241) - Кількість рідкісних біграм: 10
6. Ключ (182, 304) - Кількість рідкісних біграм: 12
7. Ключ (90, 190) - Кількість рідкісних біграм: 13
8. Ключ (423, 953) - Кількість рідкісних біграм: 13
9. Ключ (89, 304) - Кількість рідкісних біграм: 14
10. Ключ (538, 687) - Кількість рідкісних біграм: 14
```

Спробуємо розшифрувати текст, використовуючи цей ключ:

Текст:

однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопределенноеприпадкипроявляющиесярезкосприкусываниемусиливающиесядоопасногодляжизниприводящегоктяжкомусамокалеченииомогутвсежевнекоторыхслучаяхнедостигатьтакойсилыослабляясьдократкихсостоянийабсансадобыстропроходящихголовокруженийимогуттакжесменятьсякраткимипериодамикогдабольнойсовершаетчуждыеегоприродепоступкикакбынаходясьвовластибессознательногообуславливаясьвобщемкакбыстранноэтониказалосьчистотелеснымипричинамиэтисостоянияхмогутпервоначальновозникатьпопричинамчистодушевнымиспугилимогутвдальнейшемнаходитьсявзависимостиотдушевныхволненийкакнихарактернодляогромногобольшинствеслучаевинтеллектуальноеснижениеноизвестенпокрайнеймереодинслучайкогдаэтотнедугненарушилвысшейинтеллектуальнойдеятельностигельмгольцдругиеслучаивотношениикоторыхутверждалосьтожесамоененадежныилиподлежатсомнениюкакислучайсамогодостоевскоголицастрадающиеэпилепсиеймогутпроизводитьвпечатлениетупостинедоразвитоститаккакэтаболезньчастосопряженасярковыраженнымидиотизмомикрупнейшимимозговымидефектаминеявляяськонечнообязательнойсоставнойчастьюкартиныболезниноэтиприпадкисовсемисвоимивидоизмененияхмибываютиудругихлицулицсполнымдушевнымразвитиемискореесосверхобычнаявбольшинствеслучаевнедостаточноуправляемойимиаффективностьюнеудивительночтопритакихобстоятельствахневозможноустановитьсовокупностьклиническоюаффектаэпилепсииточтопроявляетсяводнородностиуказанныхсимптомовтребуетповидимомуфункциональногопониманиякакеслибымеханизманормальноговысвобожденияпервичныхпозывовбылподготовленорганическимеханизмкоторыйиспользуетсяприналичииивесьмаразныхусловийкакпринарушениимозговойдеятельностипритяжкомзаболеваниитканейилитоксическомзаболеванииткакипринедостаточномконтроледушевнойэкономиикризисномфункционированиидушевнойэнергиизаэтимразделениемнадвавидамычувствуемндентичностьмеханизмалежащеговосновевысвобожденияпервичныхпозывовэтотмеханизмнедалекиотсексуальныхпроцессовпорождаемыхвсвоейосноветоксическиужедревнейшиеврачиназываликоитусмалойэпилепсиейивиделивполовомактесмягчениеиадаптациювысвобожденияэпилептическогоотводараздраженияэпилептическаяреакциякаковымименемможноназватьвсеэтовместевзятоенесомненнотакжепоступаетиврасполяжениеневрозасущностькотороговтомчтобыликвидироватьсоматическимассыраздраженияскоторыминеврознеможетсправитьсяпсихическиэпилептическийприпадокстановитсятакимобразомсимптомомистерииеюадаптируетсяивидоизменяетсяподобнотомукакэтопроисходитпр

инормальномтечениисексуальногопроцессатакимобразоммысполнымправомразличаем органическуюиаффективнуюэпилепсиюпрактическоезначениеэтогоследующеестрадаю щийпервойпораженболезньюмозгастрадающийвторойневротиквпервомслучаедушевная жизньподверженанарушениюизвневовторомслучаенарушениеявляетсявыражениемсамо йдушевнойжизнивесьмавероятночтоэпилепсиядостоевскогоотносится ковторомувидуто чнодоказатьэтонельзятаккаквтакомслучаенужнобылобывключитьвцелокупностьегодуш евнойжизниначалоприпадковипоследующиевидоизмененияэтихприпадковадляэтогоуна снедостаточноданныхописаниясамихприпадковничегонедаютсведенияосоотношенияхм ездуприпадкамииипереживанияминеполныичастопротиворечивывсеговероятнеепредпо ложениечтоприпадкиначалисьудостоевскогоужевдетствечтоонивначалехарактеризовали сьболееслабымисимптомамиитолькопослепотрясшегоегопереживаниянавосемнадцатом годужизниубийстваотцапринялиформуэпилепсиибылобывесьмауместноеслибыоправда лосьточтоониполностьюпрекратилисьвовремяотбыванияимкаторгивсибириноэтомупро тиворечатдругиеуказанияочевиднаясвязьмеждуотцеубийствомвбратьяхкарамазовыхису дьбойотцадостоевскогобросиласьвглазанеодномубиографудостоевскогоипослужилаиму казаниемнаизвестноесовременноепсихологическоенаправлениепсихоанализтаккакподр азумеваетсяименноонсклоненвидетьвэтомсобытиитягчайшуютравмуиврeакциидостоев скогонаэтоключевойпунктегоневрозаеслияначнуобосновыватьэтуустановкупсихоанали тическиопасаюсьчтоокажусьнепонятнымдлявсехтехкомунезнакомыучениеивыражения психоанализаунасодиннадежныйисходныйпунктнамизвестенсмыслпервыхприпадковдо стоевскоговегоюношескиегодызадолгодопоявленияэпилепсииуэтихприпадковбылоподо биесмертиониназывалисьстрахомсмертиивыражалисьвсостоянииилетаргическогоснаэта болезньнаходилананеговначалекогдаонбылещемальчикомкаквнезапнаябезотчетнаяпода вленностьчувствокаконпозжерассказывалсвоемудругусоловьевутакоекакбудтобыемупре дстоялосейчасжеумеретьивсамомделенаступалосостояниесовершенноподобноедействи тельнойсмертиегобратандрейрассказывалчтофедоружевмолодыегодыпередтемкакзасну тьоставлялзаписькчтобоитсяночьюзаснутьсмертоподобнымсномипроситпоэтомучтобы егопохоронилитолькочерезпятьднейдостоевскийзарулеткойвведениеснамизвестнысмыс линамерениетакихприпадковсмертониозначаютотождествлениесумершимчеловекомко торыйдействительноумерилисчеловекомживымещенокоторомумыжелаемсмертивторой случайболеезначителенприпадоквуказанномслучаеравноцененнаказаниюмыпожелалис мертидругомутеперьмысталисамиэтимдругимисамиумерлитутпсихоаналитическоеучен иеутверждаетчтоэтотдругойдлямальчикаобычноотециименуемыйистериейприпадокявл яетсятакимобразомсамонаказаниемзапожеланиесмертиненавистномуотцуа

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.