КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Експериментальна оцінка ентропії на символ джерела відкритого тексту

ФБ-13 Владислав Садохін та Данило Розумовський

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.

Код:

```
import os
from collections import Counter

alphabet = "aбвгдежзийклмнопрстуфхцчшшыьэюя"

def ext_gcd(a, b):
    if a == 0:
        return (b, 0, 1)
    else:
        g, x, y = ext_gcd(b % a, a)
```

```
return (g, y - (b // a) * x, x)
def is letter in alphabet(letter):
def calculate non overlapping bigram frequencies(text):
     text = text.lower()
bigram count.items() }
calculate non overlapping bigram frequencies (encrypted text)
top_bigrams_encrypted = [bigram for bigram, _ in sorted(bigram_frequency.items(), key=lambda item: item[1], reverse=True)[:5]]
bigrams = ["cT", "HO", "TO", "HA", "eH"]
alphabet.index(bigrams[i][1])) % 961
alphabet.index(bigrams[k][1])) % 961
alphabet.index(top bigrams encrypted[n][1])) % 961
```

```
key candidates.append((a coefficient, b coefficient))
def decrypt affine cipher(input text, key, i):
    text = [encrypted text[i:i + 2] for i in range(0, len(encrypted text) - 1, 2)
            decrypted index2 = x % 31
            decrypted char1 = alphabet[decrypted index1]
m = 37
res = mod inverse(a, m)
print(f"Обернене до a = {a} за модулем {m} = {res}")
a = 39
m = 111
```

Результати:

Реалізована підпрограма із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь

```
Task1

Обернене до а = 5 за модулем 37 = 15

Розв'язок рівняння 39х = 30mod111 = [15, 52, 89]
```

5 найчастіших біграм запропонованого шифртексту (за варіантом №8).

```
Task2
['жц', 'дэ', 'цэ', 'сц', 'оц']
```

Перебір можливих варіантів співставлення частих біграм мови та частих біграм шифртексту, для кожного співставлення знайдено можливі кандидати на ключ

(a,b) шляхом розв'язання системи (1). Для кожного кандидата на ключ дешифрувано шифртекст. Якщо шифртекст не ϵ змістовним текстом російською мовою, його не враховано.

```
[(0, 208), (541, 390), (882, 18), (155, 301), (899, 363), (0, 208), (41, 927), (10, 524), (248, 549), (93, 456), (0, 208), (408, 800), (873, 118), (124, 85
Розшифрований текст для ключа (541, 390) збережено у файл decrypted_file_№1_key(541,390).txt
Розшифрований текст для ключа (882, 18) збережено у файл decrypted_file_№2_key(882,18).txt
Розшифрований текст для ключа (41, 927) збережено у файл decrypted_file_W6_key(41,927).txt
Розшифрований текст для ключа (10, 524) збережено у файл decrypted_file_№7_key(10,524).txt
Розшифрований текст для ключа (408, 800) збережено у файл decrypted_file_W11_key(408,800).txt
Розшифрований текст для ключа (420, 931) збережено у файл decrypted_file_W15_key(420,931).txt
Розшифрований текст для ключа (575, 63) збережено у файл decrypted_file_№18_key(575,63).txt
Розшифрований текст для ключа (358, 125) збережено у файл decrypted_file_W19_key(358,125).txt
Розшифрований текст для ключа (920, 394) збережено у файл decrypted_file_W20_key(920,394).txt
Розшифрований текст для ключа (207, 735) збережено у файл decrypted_file_W23_key(207,735).txt
Розшифрований текст для ключа (52, 642) збережено у файл decrypted_file_W24_key(52,642).txt
Розшифрований текст для ключа (677, 211) збережено у файл decrypted_file_W28_key(677,211).txt
Розшифрований текст для ключа (119, 645) збережено у файл decrypted_file_W29_key(119,645).txt
Розшифрований текст для ключа (79, 900) збережено у файл decrypted_file_№30_key(79,900).txt
Розшифрований текст для ключа (17, 94) збережено у файл decrypted_file_W34_key(17,94).txt
Розшифрований текст для ключа (951, 394) з6ережено у файл decrypted_file_№35_key(951,394).txt
   Розшифрований текст для ключа (800, 292) збережено у файл decrypted_file_№196_key(800,292).txt
```

```
Розшифрований текст для ключа (242, 416) збережено у файл decrypted_file_№197_key(242,416).txt
Розшифрований текст для ключа (630, 22) збережено у файл decrypted_file_№201_key(630,22).txt
Розшифрований текст для ключа (599, 22) збережено у файл decrypted_file_№202_key(599,22).txt
Розшифрований текст для ключа (331, 338) збережено у файл decrypted_file_W205_key(331,338).txt
Розшифрований текст для ключа (579, 338) збережено у файл decrypted_file_№208_key(579,338).txt
Розшифрований текст для ключа (424, 338) збережено у файл decrypted_file_№209_key(424,338).txt
Розшифрований текст для ключа (362, 896) збережено у файл decrypted_file_№210_key(362,896).txt
Розшифрований текст для ключа (610, 896) збережено у файл decrypted_file_W213_key(610,896).txt
Розшифрований текст для ключа (455, 896) збережено у файл decrypted_file_W214_key(455,896).txt
Розшифрований текст для ключа (382, 363) збережено у файл decrypted_file_W216_key(382,363).txt
Розшифрований текст для ключа (351, 363) збережено у файл decrypted_file_M217_key(351,363).txt
Розшифрований текст для ключа (537, 270) збережено у файл decrypted_file_№221_key(537,270).txt
Розшифрований текст для ключа (506, 270) збережено у файл decrypted_file_M222_key(506,270).txt
Файл decrypted_file_№127_key(17,94).txt є змістовним.
Файл decrypted_file_№197_key(242,416).txt є змістовним.
Файл decrypted_file_№34_key(17,94).txt є змістовним.
Файл decrypted_file_M35_key(951,394).txt є змістовним.
Файл decrypted_file_№76_key(4,462).txt є змістовним.
Process finished with exit code 0
```

На цьому скріншоті можемо побачити результат розшифровки файлу.

— decrypted_file_№34_key(17,94) – Блокнот Файл Правка Формат Вид Справка малыгикизаульбалисыисжаромеьялисюьаделоонирвалльолотиспзецвепзцветьчтонаводняютвесьмирпереплескиваютсяслужаекнамощеньеулэцьтухоныкостучатсявпржьеачньеокна погррбовнезнаютугомонумудержумвешвокрусьаливаютслеыяшимсверканиемрасплавленногосолнцакаждоелетоониточносцеписрываютсксказалдедушкапустымуянепротиввонихско лыкостоятторбаекаклыяэпосмотришынаникпидольшетакипроктутутрбявглгьахбархуведыпростойцеетокможносказатысорнаятраваниктоеенезамечаетамыуважаемсчитаемодуванч икмлагоршдноерастениеонинабралиполкземешкишдувангиковиунесливнльвпогребвьвалилиихизмешковивотымепогррбаргьлиложысияниевинныйпрессдгжидалсяухотхрьтыйболодн ьйзолотистьйпотоясогрелегодедушкапередвинулпрессповернулрумкцьавертелбьстрейюзстрейипрессмягкостиснулдобьчунувотвоттаксперватонкойструйкойпотомвсеоедрееоб илынеепобежалпгжелобувглиняньекувшиньсокпрекеасноггжаркогомесяцаемудалиперрбродитыснялипенуиеазлиливгистьебупэлкиизпшдкетчупаионивьстроилижырядаминаполках помлескиваявсумракепогребавинольшдувангиковсамьеэтисловаточнолетонаядзкевинольшдувангиковпойманншельакупоренношвбупэлкилетоитеперыкогдадуглафьналпонастоящ емцьналчтоонживойчтоонзатемибодитпжьемлечтобьвидетыиощущатымиронпонялеоещднонадочастэцувсегочтоонузналчастэцуэтогоособенногодняднясбораодуванчиковтожезаку поритыисохеанитыапотомнастанеттакомьимнийянварскийденыкогдавалитгустойснщгисолнцаужедавньмдавнониктоневиделиможетбьтжэточудопозаюэложыухорошобьегосновавсп омнитывоттогдаонщгооткупоритведыэтолетонепременнобудетлетомнежданньхчудесинадовсеихсберечыигдетоотложитыдлксрбячтоюэпослщвлюхойчаскогдавздумаешыпробеатыся наузпомкахвовлажкэйсумеакипротянутырукуитамрядзарядомбудутстоятыбупзлкисвиномизодуванчиковонобудетмягкомерцатыточнорасхрьвающиесянгьарецвепзасквжьытонкийс лойпьлибудетпомлескиватысолнцекэнешншгоиюнявзглянисквозыэтовинонахолшдкзмьимнийденыиснщгеастаетизпшднегопокажетсктеаванадеревыяхгживутптэцьлистваицветьсло вномириабэбахоченьатрепешутнаветруидажехолшдноесерщенехостанетголуюзмвжымилетоврукуналейлетовхокалвсайзйкроботныйконечноизкакоготолыкоисделаешыединственн ьйтерпкийглотохпшднесищгокгубамипожиламтвоимвместолютомьимьпобежитжаркщелетотеперыдождщвойвобзконечнжьдежыгодитсктолыкочистейшаяводадалынибозерсладосткзер осъбархатньхлуговчтовозносктсяназарехраспабнувшимсянавстречунебесамтамвпрохладкзхвьсяхонисобиралисычистоомьтьмигроздпямиветермчалишьасотнимилызаряжаяпопут иэлеятрическимльарядамиэтаводавобралавкаждуюсвоюкаплюеоехольшенебескогдападаладождемназеблюонавпиталавсебявосточкзйветерльападкзйисеверньйиюжньйиобратилас ывдождыадождывэтотчассвяоенншдействиуужестановитсятерпкимвиномдуглассхватилковшвьбежалводвориглухокопогрцьилшговхочоноясдождшвойводойвотонавшдабьлаточноше лкпржьеачный голуховалэйшелкеслиещым инмонакоснется губгорласердцамя гкокакласканоковшилольные додольное дольное додольное до дувдоменритантсяковарныймихробитогдальпогррбавжыникнетточнобогинялетабабушкапрячачтотоподввьанойшальюонапринесетэточтотовкомнатукаждогоболящщгоиеазолыетду шистщепржьеачнщевпрозрачкзестакакзистакакзэтиосушатоднимглоткоблекарствоиньхвременбалызамизсолнечньхлучейипргьдногоавгустовскогополудняедвасизшныйстукколе стележкисморгженьмчтокатитсяпомооекзмулицамшорохсеребристогофейерверкачторасгзпаетсяязсоковнрбеишелестсриьаннойтеаязфонтаномбыющейльподкосилкичтщдвижетсяп олугампомуеавыиномуцарствувсеэтовсшвшдномстаканедадажебабушкакогдаспуститсявзимнийпогррбзаиинемнавернобудетстоктытамтибоныкосовсемшднавтайномединениисосво имсохровенкзмсосвоейдушойкакидедушкаипапаидядябертидручиетгжесловнобеседуястенжюдавноушедшухднейспикникамистепизмдгждемсзапабомпшеничньхполейижарекзхкукур цькзшьеренисвежескошенногосенадажебабушкабудетповторктысноватежечудесньезолотящиесксловачтжьвучатсейчаскогдацветькладутпшдпресскакбудутикповторятыка ждуюзимувсрбельезийзвовсщвременасноваисноваонибудутслетатысгубкакуизбкаккнежданкэйсолнечньйзайчиквотымевинольшдувангиковвинольшдувангиковиноизодуванчиковвинольшдувангико вонипрухшдилинесизшноубодилипочтибесшумнотеавапригибаласымеаспрябляласывновыонисколызиливнльпоболмамточнотениомлаковэтобежалилетниемалычишкидугласотсталль аблудилсвьадьхаяжыотюзстрогобегаоностановилсянакеаюовраганасамойхромкенадпропастжюиоттудананщгшдохнулоболодомнавостривушиточнооленыонвдругучуялстаруюкакми аолудильсвадавляющих строй обестание и обестанием выдельность выдельных вышельных выдельных выдельных вышельных выдельных выдельных вышельных выш незрельеплидьдикойяблониитамеастутльреютавотэтакперсиковомусадуквиноградникукогороднымгрядамгдедреблютнасолнцеарбудзполосапзесловнокошкитигровоймастиэтатр

Висновки:

У ході виконання лабораторної роботи №3 ми вивчили та засвоїли навички роботи з інструментом частотного аналізу на прикладі розкриття моноалфавітної підстановки. Повторення роботи з модулярною арифметикою . Також варто зазначити ,що у ході виконання комп'ютерного практикуму ми повтроювали та отсаточно закріплювали навички ,отримані під час вионання попередніх комп'ютерних практикумів ,зокрема робота з частотами біграм та інше.