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

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Експериментальна оцінка ентропії на символ джерела відкритого тексту

Виконали:
Студенти 3 курсу
Остапова О. А.
Литвин М. Р.

Київ – 2025

Мета роботи

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

Постановка задачі

Задача полягає у проведенні криптоаналізу шифртексту, зашифрованого методом афінної біграмної підстановки, з метою визначення ключа шифрування та відновлення змістовного російськомовного тексту. Для цього необхідно реалізувати програмні модулі для обчислень у модулярній арифметиці, провести частотний аналіз біграм шифртексту, знайти кандидати на ключ, здійснити дешифрування та створити автоматичний розпізнавач осмисленого тексту.

Варіант 10

Порядок виконання роботи

1. Уважно ознайомитись із методичними вказівками до комп'ютерного практикуму та теоретичними основами афінної біграмної підстановки.
2. Реалізувати підпрограми для виконання математичних операцій у модулярній арифметиці:
    - знаходження оберненого елемента за модулем за допомогою розширеного алгоритму Евкліда;
    - розв'язування лінійних порівнянь із можливістю отримання кількох розв'язків.
3. За допомогою програми підрахунку частот біграм (розробленої у практикумі №1) визначити п'ять найчастіших біграм шифртексту.
4. Провести частотне співставлення найпоширеніших біграм російської мови («ст», «но», «то», «на», «ен») із найчастішими біграмами шифртексту.
5. Для кожної пари біграм скласти систему рівнянь афінного шифру та обчислити можливі значення ключа (a, b).
6. Для кожного кандидата на ключ здійснити дешифрування шифртексту за афінною формулою.
7. Реалізувати автоматичний розпізнавач змістовного тексту російською мовою на основі частотних характеристик літер та біграм.
8. Визначити правильний ключ шифрування, який дає осмислений російський текст, і записати отриманий результат.
9. Оформити звіт, у якому подати мету, варіант завдання, опис алгоритмів, знайдені біграми, метод автоматичного розпізнавання, отриманий ключ, зашифрований та розшифрований тексти, а також висновки.

Хід роботи

Підготовка

Перед початком роботи нормалізуємо текст: приводимо всі літери до нижнього регістру, замінюємо «ё» на «е» та «ъ» на «ь», видаляємо всі символи, що не належать алфавіту, і, якщо довжина тексту непарна, обрізаємо останній символ, щоб можна було розбивати текст на біграми.

```python
def clean_text(text: str) -> str:
    text = text.lower().replace("ё", "е").replace("ъ", "ь")
    text = re.sub(f"[^{alphabet}]", "", text)
    if len(text) % 2 == 1:
        text = text[:-1]
    return text
```

Частотний аналіз

У російській мові найбільш уживаними є біграми «ст», «но», «то», «на», «ен». Тому можна припустити, що найчастіші біграми в шифртексті, ймовірно, відповідають цим частим біграмам відкритого тексту.

Після аналізу виділяємо такі топ-біграми:

```
ТОП-5 біграм шифртексту (неперекриті):
  сг: 60 входжень  (1.577%)
  жэ: 59 входжень  (1.551%)
  ям: 54 входжень  (1.419%)
  нг: 52 входжень  (1.367%)
  тм: 51 входжень  (1.340%)
```

Пошук кандидатів у ключ та перебір можливих кандидатів

Фрагмент коду перебирає всі можливі пари топ-5 біграм шифртексту та топ-5 біграм російської мови, і для кожної пари використовує лінійне конгруентне рівняння для знаходження кандидатів на ключ (a, b) афінного шифру. Для кожного потенційного ключа виконується дешифрування тексту та обчислюється оціночний score, що відображає відповідність розшифровки російській мові. Потім кандидати сортуються за score, вибирається найкращий ключ, а всі ключі записуються у файл candidates.txt з позначкою

pass для найкращого та fail для інших.

```
logged_keys = set()
keys_list = []

for plain_pair in permutations(top_rus_bigrams, 2):
    x1 = bigram_to_num(plain_pair[0])
    x2 = bigram_to_num(plain_pair[1])
    for cipher_pair in permutations(top_cipher_bigrams, 2):
        y1 = bigram_to_num(cipher_pair[0])
        y2 = bigram_to_num(cipher_pair[1])
        a_candidates = solve_linear_congruence((x2 - x1) % MOD, (y2 - y1) % MOD, MOD)
        for a in a_candidates:
            b = (y1 - a * x1) % MOD
            if (a,b) in logged_keys:
                continue
            logged_keys.add((a,b))
            keys_list.append((a,b))

total_keys = len(keys_list)
if total_keys == 0:
    print("Не знайдено кандидатів ключів.")
    return

candidates_data = []
for idx, (a,b) in enumerate(keys_list, start=1):
    print(f"Перевірка кандидата {idx}/{total_keys}...", end="\r")
    sys.stdout.flush()
    decrypted = decrypt_affine_bigram(ciphertext, a, b)
    if decrypted is None:
        sc = 0.0
        dec = None
    else:
        sc = score_russian_likeness(decrypted)
        dec = decrypted
    candidates_data.append((a,b,sc,dec))
print(" " * 60, end="\r")
```

Результат роботи

```
Правильний (обраний) ключ для розшифровки: key(300,400)  score=107.5989
Усього унікальних кандидатів: 285. Кращий ключ записано у 'decrypted.txt', усі кандидати у 'candidates.txt'.
```

Розшифрований текст:

поздновечеромнаверандесиделколяичтотописалвтемнотебумагуитутолкомнельзябылоразгл
ядетьвремяотвременионвосклицалагаилииэтотожезначитемувголовуприходилоещечтонибу
дьподходящеедляегоспискапотомдверьчутьстукнулаточновсеткуотмоскитовудариласьночн
аябабочкалинашепнулауфманонаселярядомснимнакачеливоднойночнойсорочкенетоненька
якаксемнадцатилетняядевочкакоторуюещенелюбятинетолстаякакпятидесятилетняяженщи
накоторуюуженелюбятноскладнаяикрепкаяименнотакаякакнадотаковыженщинывовсякомв

озрастееслионилюбимыонабылаудивительнаяеетелокакиегособственноевсегдадумалозанее
толькоподругомуоновынашивалодетейиливходиловпередилеовкаждуюкомнатучтобынеуло
вимоизменитьтамсамыйвоздухподстатьнастроениюмужаказалосьонаникогданезадумывает
сянадолгомысльтотчаспередаваласьотееголовыплечампальцамипретворяласьвдействиетак
незаметноиестественночтолеонесмогбыдаинехотелизобразитьэтокакимилибочертежамиэта
машинасказалаонанаконецненужнаонанамдаотозвалсяонноиногданужнопозаботитьсяиодр
угихявотвседумаючтотудавставитькинокартинырадиоприемникистереоскопическиеочкиес
лисобратьвсеэтовместевсякийчеловекпощупаетулыбнетсяискажетдадаэтоиестьсчастьесочи
нитьтакуюхитруюмеханикудумалончтопускайучеловекапромоклиногиилиноетязваилиегом
учаетбессонницаионворочаетсявпостеливсюночьнапролетидушуегогрызутзаботыавсеравн
отвоямашинадастемусчастьекактамагическаякрупинкасоличтоброшенавокеанивечнорожда
етсольиобратилавсеморевсолянойрастворктонерасшибсябывлепешкулишьбыизобреститак
уюмашинупустьемуответитнаэтотвопросцелыймирпустьответитвесьгородокпустьответитж
еналинасмущенномолчаласидярядомснимнакачеляхиеемолчаниеговорилояснеевсякихслов
леотожеумолкзапрокинулголовуислушалкаксвищетветервгустойлиственогучеговязанезаб
ывайговорилонсебеиэтотшелестлистьевтоженуждлятвоеймашинычерезминутуверандаоп
устелапустыекачелинеподвижноповисливтемнотедедушкаулыбнулсявоснеонпочувствовал
этуулыбкуудивилсяейипроснулсяполежалнемногоприслушалсяксебеипонялоткудаонавзял
асьибоонуслышалнечтогораздоболееважноенежелипениептицилишелестмолодойлиствыка
ждыйгоднаступалденькогдаонвоттакпросыпалсяиждалэтогозвукакоторыйозначалчтотепер
ьтоужлетоначалосьпонастоящемуононачиналосьвотвтакоеутрокогдактонибудьиздомочадц
евилигостейплемянниксыниливнуквыходилналужайкуподегоокномиметаллическиеножиис
пицыкружаизвеняподушистойлетнейтравеприлежнообегалиеепокраямнасевернавостокнаю
гназападописываявсеменьшиеименьшиеквадратыкосилказвонкострекоталаизподножейбры
згалиголовкиклевераредкиезолотыеискрыуцелевшихпослесбораодуванчиковмуравьипалоч
кикамешкиостаткипрошлогоднегопразднованиячетвертогоиюляобгорелыешутихиикусочк
итрутаноглавноезанейстлалсяпрохладныйчистыйпотоксочнойзеленойтравыдедушкеужепр
едставлялоськаконащекочетегоногиохлаждаетразгоряченноелицонаполняетноздриизвечны
мароматомвновьродившегосялетаиобещаетдамывсевсепроживемещецелыйгодвеликоечудо
косилкаговорилсебедедушкакакойэтодураквыдумалчтоновыйгодначинаетсяпервогоянваря
надобылопоставитьдозорныхкараулитьросттравынамиллионахлужаекиллинойсаогайоилиа
йовыикакзаметятчтоонасозреладлясенокосавтосамоеутровместофейерверковфанфарикрик
овпустьначинаетсявеликаябурнаясимфониякосилоксрезающихсвежиетравынанеобятныхлу
говыхпросторахвтотединственныйденьвгодукоторыйпонастоящемузнаменуетсобойначало
людямнадобыбросатьдругвдруганеконфеттиинесерпантинапригоршнисвежескошеннойтра
выдедушкахмыкнулчтотоужбольнодолгуюфилософиюразвелвсталподошелкокнуивысунул
сявласковыйсолнечныйсветтакиестьфорестерновыйжилецмолодойгазетчиккакраззаканчив
аетряддоброеутромистерсполдингтакеехорошенькобиллсжаромкрикнулдедушкаивскореуж
есиделвнизуиуплеталприготовленныйбабушкойзавтракширокоеокнобылораскрытоижужж
аньекосилкисловноподпевалозавтракуотэтойкосилкинадушестановитсяспокойнеезаметилд
едушкатытолькопослушайтеперьужнедолгонамееслушатьотозваласьбабушкаипоставилана
столгоркупшеничныхлепешекбиллфорестерпосеетсегодняновыйсорттравыеененадобудетк
оситьнепомнюкактамонаназываетсяноонакаквырастетскольконужнотаксамаиостановитсяи

большенерастетдедушкасизумлениемуставилсянаженудовольноглупаяшуткасказалоннако
нецидипосмотрисамбиллфорестерговоритэтоземленапользусказалабабушкаонужепривезно
выесеменаонисложеныздомомвмаленькихкорзинкахнужновразныхместахвырытьямкииза
сыпатьтудасеменакконцугодановаятраваубьетвсюстаруюитогдаможешьпродаватьсвоюкос
илкуонатебебольшенепонадобитсядедушкасорвалсясостулаимигомвыскочилводворбиллфо
рестеростановилкосилкуижмурясьотсолнцасулыбкойподошелкнемувоттактосказалонвчера
купилновыесеменадайдумаюзасеювамлужайкупокаясвободенаменяпочемунеспросилилуж
айкатовсетакимоязакричалдедушкаядумалвыбудетедовольнымистерсполдингничегоянедов
оленпокажитемнеэтучертовутравуонистояливозлемаленькихчетырехугольныхкорзиноксно
вомоднымисеменамидедушкаподозрительнопотыкалоднуизнихноскомбашмакапомоемуэто
самаяобыкновеннаятраваавыуверенычтовасненадулиявкалифорниивиделкаконарастетвотн
астольковырастетивсееслитолькоонаприживетсявздешнемклиматенамуженабудущийгодне
придетсякаждуюнеделюподстригатьлужайкувтомтоибедасвашимпоколениемсказалдедушк
амнестыднозавасбиллаещежурналиствыготовыуничтожитьвсечтоестьнасветехорошеготоль
кобытратитьпоменьшевременипоменьшетрудавотчеговыдобиваетесьоннепочтительнопнул
корзинкуногойвотпоживетесмоетогдапойметечтомелкиерадостикудаважнеекрупныхраноу
тромповеснепрогулятьсяпешкомневпримерлучшечемкатитьвосемьдесятмильвсамомроско
шномавтомобилеазнаетепочемупотомучтовсевокругблагоухаетвсерастетицвететкогдаидеш
ьпешкоместьвремяоглядетьсявокругзаметитьсамуюмалуюкрасотуяпонимаюсейчасвамхоче
тсяохватитьвсесразуиэтонаверноестественноэтосвойствомолодостиногазетчикунадоуметьв
идетьимелкийвинограданетолькоогромныеарбузывамподавайцелыйскелетасменядовольно
иследапальцевчтожтожепонятносейчасмелочикажутсявамскучныминоможетвыпростоеще
незнаетеимценынеумеетенаходитьвнихвкусдайвамволювыбыиздализаконобустранениивсе
хмелкихделвсехмелочейнотогдавамнечегобылобыделатьвперерывемеждубольшимиделами
ипришлосьбыдоисступленияпридумыватьсебезанятиечтобынесойтисуматакужлучшепоучи
лисьбыкоечемуусамойприродыподстригатьтравуивыпалыватьсорнякитожеоднаизрадостей
жизнисынокбиллфорестерласковоулыбнулсястарикузнаюзнаюсказалдедушкаястановлюсьс
лишкомболтливымвжизниникогонеслушалстакимудовольствиемтогдапродолжимлекциюк
устсиренилучшеорхидейиодуванчикитожеичертополохапочемудапотомучтоонихотьненадо
лгоотвлекаютчеловекауводятегоотлюдейигородазаставляютпопотетьивозвращаютснебесна
землюиужкогдатывесьтутиниктотебенемешаетхотьненадолгоостаешьсянаединессамимсоб
ойиначинаешьдуматьодинбезпостороннейпомощикогдакопаешьсявсадусамоевремяпофило
софствоватьниктообэтомнедогадываетсяниктотебянеобвиняетниктоинезнаетничегоатыста
новишьсязаправскимфилософомэдакийплатонсредипионовсократкоторыйсамсебевыращив
аетцикутутоткотащитнаспинепосвоейлужайкемешокнавозасродниатласуукоторогонаплеч
ахвращаетсяземнойшарсэмюэлсполдингэсквайрсказалоднаждыкопаяземлюпокопайсяусебя
вдушевертителопастиэтойкосилкибиллидаороситвасживительнаяструяфонтанаюностилекц
ияоконченакрометогоизредкаоченьпользительноотведатьзелениодуванчиковавыдавноелиз
еленьодуванчиковнаужинсэрнебудемуточнятьбиллкивнулилегонькостукнулближайшуюко
рзинкуноскомбашмакатаквотнасчетэтойтравыяещеневсевамсказалонарастеттакгусточтона
верняказаглушитиклевериодуванчикигосподипомилуйзначитуженабудущийгодмыостанем
сябезвинаизодуванчиковиниоднойпчелынадлужайкойдавыпростосумасошлипослушайтеск
ольковызаплатилизаэтисеменадолларкорзинкаякупилдесятьштуквамвподарокдедушкаполе

звкарманвытащилстаромодныйдлинныйкошелекотстегнулсеребрянуюзастежкуиизвлектри бумажкипопятьдолларовбиллвытолькочтосовершилипревыгоднуюсделкузаработалипятьдо лларовизвольтесейчасжеотправитьвсюэтучересчурпрозаическуютравувовраг напомойкусло вомкудахотитетолькопокорнейшепрошунесейтееуменяводвореязнаюувассамыепохвальны енамерениянояв сетакиужедостигвесьмапочтенноговозрастаисмоимижеланияминегрехсчит атьсявпервуюочередьаа

Висновок

У процесі виконання лабораторної роботи були набуті практичні навички криптоаналізу моноалфавітної підстановки. Зокрема, опановано метод частотного аналізу біграм, що дозволяє знаходити відповідність між зашифрованими біграмами та типовими біграмами мови для розкриття шифртексту.

Також було закріплено знання модулярної арифметики та розв’язання лінійних конгруенцій, що є основою для побудови та аналізу шифрів на основі афінних перетворень.

Виконання роботи сприяло розвитку практичних навичок у сфері комп’ютерної безпеки та криптографії, поглибило розуміння принципів шифрування та методів дешифрування, а також сформувало досвід систематичного підходу до виявлення криптографічних слабкостей.