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:

```
Top 5 ciphertext bigrams (count | frequency):
------------------------------
Bigram | Count  | Freq
------------------------------
сг     | 60     | 0.0158
жэ     | 59     | 0.0155
ям     | 54     | 0.0142
нг     | 52     | 0.0137
тм     | 51     | 0.0134
------------------------------
```

Пошук кандидатів у ключ

Функція key_candidates знаходить всі можливі ключі (a, b) афінного шифру для пари біграм, перетворюючи систему рівнянь a*X + b ≡ Y (mod m^2) на одне лінійне конгруентне рівняння A*a ≡ B (mod m^2). Спочатку обчислюються різниці A = X1 - X2 та B = Y1 - Y2, потім розв’язується конгруентне рівняння для a із перевіркою взаємної простоти з модулем, після чого обчислюється відповідне b = Y1 - a*X1 (mod m^2). Функція повертає всі допустимі ключі, які можуть з’єднати задану пару біграм відкритого тексту та шифртексту.

```python
def key_candidates(X1: int, X2: int, Y1: int, Y2: int):
    A = (X1 - X2) % mod
    B = (Y1 - Y2) % mod
    sols = solve_linear_congruence(A, B, mod)
    for a in sols:
        if gcd(a, m) != 1:
            continue
        b = (Y1 - a * X1) % mod
        yield a, b
```

Перебір кандидатів

```python
for X1, X2 in permutations(X_vals, 2):
    for Y1, Y2 in permutations(Y_vals, 2):
        for a, b in key_candidates(X1, X2, Y1, Y2):
            if (a, b) in seen_keys:
                continue
            seen_keys.add((a, b))
            pt = decrypt_affine(cipher_text, a, b)
            if pt and looks_like_ru(pt):
                msg = f"PASS (a={a}, b={b})"
                print(msg)
                print("    " + pt[:300] + "...\n")
                log(msg)
                results.append((a, b, pt))
            else:
                log(f"FAIL (a={a}, b={b})")
```

Принцип роботи програми полягає в тому що вона перебирає всі можливі пари топ-частих біграм російської мови та шифртексту, для кожної пари обчислює можливі значення ключа *a* і *b* за афінним рівнянням, перевіряє, чи ще не було такого ключа, дешифрує текст і автоматично оцінює, чи виглядає результат як змістовний текст російською, зберігаючи вдалий варіант для подальшого використання.

Результат роботи

```
Key search in progress...

PASS (a=300, b=400)
   поздновечеромнаверандесиделколяичтотописалвтемнотебумагуитутолкомнельзябылоразглядетьвремяотвременионвосклицалагаилииэтотожезначитемувголовупр
иходилоещечтонибудьподходящееедляегоспискапотомдверьчутьстукнулаточновсеткуотмоскитовудариласькночнаябабочкалинашепнулауфманонаселарядомснимнакачел
иводнойночной...


Checked 261 candidate keys.

Best key: a=300, b=400
```

Розшифрований текст:

поздновечеромнаверандесиделколяичтотописалвтемнотебумагуитутолкомнельзябылоразгл
ядетьвремяотвременионвосклицалагаилииэтотожезначитемувголовуприходилоещечтонибу
дьподходящеедляегоспискапотомдверьчутьстукнулаточновсеткуотмоскитовудариласьночна
ябабочкалинашепнулауфманонаселарядомснимнакачеливоднойночнойсорочкенетоненькая
каксемнадцатилетняядевочкакоторуюещенелюбятинетолстаякакпятидесятилетняяженщина
которуюуженелюбятноскладнаяикрепкаяименнотакаякакнадотаковыженщинывовсякомвоз
растееслионилюбимыонабылаудивительнаяеетелокакиегособственноевсегдадумалозанееото
лькоподругомуоновынашивалодетейиливходиловпередилеовкаждуюкомнатучтобынеулови
моизменитьтамсамыйвоздухподстатьнастроениюмужаказалосьонаникогданезадумываетсян
адолгомысльтотчаспередаваласьотееголовыплечампальцамипретворяласьвдействиетакнеза
метноиестественночтолеонесмогбыдаинехотелизобразитьэтокакимилибочертежамиэтамаш
инасказалаонанаконецненужнаонанамдаотозвалсяонноиногданужнопозаботитьсяиодругихя
вотвседумаючтотудавставитькинокартинырадиоприемникистереоскопическиеочкиеслисоб
ратьвсеэтовместевсякийчеловекпощупаетулыбнетсяискажетдадаэтоиестьсчастьесочинитьт
акуюхитруюмеханикудумалончтопускайучеловекапромоклиногиилиноетязваилиегомучает
бессонницаионворочаетсявпостеливсюночьнапролетидушуегогрызутзаботыавсеравнотвоя
машинадастемусчастьекактамагическаякрупинкасоличтоброшенавокеанивечнорождаетсол
ьиобратилавсеморевсолянойрастворктонерасшибсябывлепешкулишьбыизобреститакуюма
шинупустьемуответитнаэтотвопросцелыймирпустьответитвесьгородокпустьответитженали
насмущенномолчаласидярядомснимнакачеляхиеемолчаниеговорилояснеевсякихсловлеото
жеумолкзапрокинулголовуислушалкаксвищетветервгустойлиствемогучеговязанезабывайго
ворилонсебеиэтотшелестлистьевтоженуждлятвоеймашинычерезминутуверандаопустела
пустыекачелинеподвижноповисливтемнотедедушкаулыбнулсявоснеонпочувствовалэтуулы
бкуудивилсяейипроснулсяполежалнемногоприслушалсяксебеипонялоткудаонавзяласьибоо
нуслышалнечтогораздоболееважноенежелипениептицилишелестмолодойлиствыкаждыйгод
наступалденькогдаонвоттакпросыпалсяиждалэтогозвукакоторыйозначалчтотеперьтоужлето
началосьпонастоящемуононачиналосьвотвтакоеутрокогдактонибудьиздомочадцевилигосте
йплемянниксыниливнуквыходилналужайкуподегоокномиметаллическиеножииспицыкружа
извеняподушистойлетнейтравеприлежнообегалиеепокраямнасевернавостокнаюгназападоп
исываявсеменьшиеименьшиеквадратыкосилказвонкострекоталаизподножейбрызгаливолов
киклевераредкиезолотыеискрыуцелевшихпослесбораодуванчиковмуравьипалочкикамешки
остаткипрошлогоднегопразднованиячетвертогоиюляобгорелыешутихиикусочкитрутаногла
вноезанейстлалсяпрохладныйчистыйпотоксочнойзеленойтравыдедушкеужепредставлялось
каконащекочетегоногиохлаждаетразгоряченноелицонаполняетноздриизвечнымароматомвн
овьродившегосялетаиобещаетдамывсевсепроживемещецелыйгодвеликоечудокосилкаговор
илсебededушкакакойэтодураквыдумалчтоновыйгодначинаетсяпервогоянварянадобылопост
авитьдозорныхкараулитьросттравынамиллионахлужаекиллинойсаогайоилиайовыикказамет
ятчтоонасозреладлясенокосавтосамоеутровместофейерверковфанфарикриковпустьначинае
тсявеликаябурнаясимфониякосилоксрезающихсвежиетравынанеобятныхлуговыхпросторах
втотединственныйденьвгодукоторыйпонастоящемузнаменуетсобойначалолюдямнадобыбро
сатьдругвдруганеконфеттиинесерпантинапригоршнисвежескошеннойтравыдедушкахмыкн
улчтотоужбольнодолгуюфилософиюразвелвсталподошелкокнуивысунулсявласковыйсолне
чныйсветтакиестьфорестерновыйжилецмолодойгазетчиккакраззаканчиваетряддоброеутро

мистерсполдингтакеехорошенькобиллсжаромкрикнулдедушкаивскореужесиделвнизуиупле
талприготовленныйбабушкойзавтракширокоеокнобылораскрытоижужжаньекосилкисловно
подпевалозавтракуотэтойкосилкинадушестановитсяспокойнеезаметилдедушкатытолькопос
лушайтеперьужнедолгонамееслушатьотозвалась бабушкаипоставиланастолгоркупшеничны
хлепешекбиллфорестерпосеетсегодняновыйсорттравыеененадобудеткоситьнепомнюкактам
онаназываетсяноонакаквырастетскольконужнотаксамаиостановитсяибольшенерастетдеду
шкасизумлениемуставилсянаженудовольноглупаяшуткасказалоннаконецидипосмотрисамб
иллфорестерговоритэтоземленапользусказалабабушкаонужепривезновыесеменаонисложен
ызадомомвмаленькихкорзинкахнужновразныхместахвырытьямкиизасыпатьтудасеменаккон
цугодановаятраваубьетвсюстаруюитогдаможешьпродаватьсвоюкосилкуонатебебольшенепо
надобитсядедушкасорвалсясостулаимигомвыскочилводворбиллфорестеростановилкосилку
ижмурясьотсолнцасулыбкойподошелкнемувоттактосказалонвчеракупилновыесеменадайду
маюзасеювамлужайкупокаясвободенаменяпочемунеспросилилужайкатовсетакимоязакрича
лдедушкаядумалвыбудетедовольнымистерсполдингничегоянедоволенпокажитемнеэтучерт
овутравуонистояливозлемаленькихчетырехугольныхкорзиноксновомоднымисеменамидеду
шкаподозрительнопотыкалоднуизнихноскомбашмакапомоемуэтосамаяобыкновеннаятраваа
выуверенычтовасненадулиявкалифорниивиделкаконарастетвотнастольковырастетивсеесли
толькоонаприживетсявздешнемклиматенамуженабудущийгоднепридетсякаждуюнеделюпод
стригатьлужайкувтомтоибедасвашимпоколениемсказалдедушкамнестыднозавасбиллаещеж
урналиствыготовыуничтожитьвсечтоестьнасветехорошеготолькобытратитьпоменьшевреме
нипоменьшетрудавотчеговыдобиваетесьоннепочтительнопнулкорзинкуногойвотпоживетес
моетогдапойметечтомелкиерадостикудаважнеекрупныхраноутромповеснепрогулятьсяпешк
омневпримерлучшечемкатитьвосемьдесятмильвсамомроскошномавтомобилеазнаетепочем
употомучтовсевокругблагоухаетвсерастетицвететкогдаидешьпешкоместьвремяоглядетьсяв
округзаметитьсамуюмалуюкрасотуяпонимаюсейчасвамхочетсяохватитьвсесразуиэтонаверн
оестественноэтосвойствомолодостиногазетчикунадоуметьвидетьимелкийвинограданетольк
оогромныеарбузывамподавайцелыйскелетасменядовольноисследапальцевчтожтожепонятно
сейчасмелочикажутсявамскучныминоможетвыпростоещенезнаетеимценынеумеетенаходит
ьвнихвкусдайвамволювыбыиздализаконобустраниивсехмелкихделвсехмелочейнотогдава
мнечегобылобыделатьвперерывемеждубольшимиделамиипришлосьбыдоисступленияприд
умыватьсебезанятиечтобынесойтисуматакужлучшепоучилисьбыкоечемуусамойприродыпо
дстригатьтравуивыпалыватьсорнякитожеоднаизрадостейжизнисынокбиллфорестерласково
улыбнулсястарикузнаюзнаюсказалдедушкаястановлюсьслишкомболтливымвжизниникогон
еслушалстакимудовольствиемтогдапродолжимлекциюкустсиренилучшеорхидейиодуванчи
китожеичертополохапочемудапотомучтоонихотьненадолгоотвлекаютчеловекауводятегоотл
юдейигородазаставляютпопотетьивозвращаютснебесназемлюиужкогдатывесьтутиниктотеб
енемешаетхотьненадолгоостаешьсянаединессамимсобойиначинаешьдуматьодинбезпостор
оннейпомощикогдакопаешьсявсадусамоевремяпофилософствоватьниктообэтомнедогадыва
етсяниктотебянеобвиняетниктоинезнаетничегоатыстановишьсязаправскимфилософомэдак
ийплатонсредипионовсократкоторыйсамсебевыращиваетцикутутоткотощитнаспинепосвое
йлужайкемешокнавозасродниатласуукоторогонаплечахвращаетсяземнойшарсэмюэлсполди
нгэсквайрсказалоднаждыкопаяземлюпокопайсяусебявдушевертителопастиэтойкосилкибил
лидаороситвасживительнаяструяфонтанаюностилекцияоконченакрометогоизредкаоченьпо

льзительноотведатьзелениодуванчиковавыдавноелизеленьодуванчиковнаужинсэрнебудему точнятьбиллкивнулилегонькостукнулближайшуюкорзинкуноскомбашмакатаквотнасчетэто йтравыяещеневсевамсказалонарастеттакгусточтонаверняказаглушитиклевериодуванчикиго сподипомилуйзначитуженабудущийгодмыостанемсябезвинаизодуванчиковиниоднойпчелы надлужайкойдавыпростосумасошлипослушайтесколькovызаплатилизаэтисеменадолларкор зинкаякупилдесятьштуквамвподарокдедушкаполезвкарманвытащилстаромодныйдлинныйк ошелекотстегнулсеребрянуюзастежкуиизвлектрибумажкипопятьдолларовбиллвытолькочто совершилипревыгоднуюсделкузаработалипятьдолларовизвольтесейчасжеотправитьвсюэту чересчурпрозаическуютравувовragнапомойкусловомкудахотитетолькопокорнейшепрошуне сейтееуменяводвореязнаюувассамыепохвальныенамерениянoявсетакиужедостигвесьмапо чтенноговозрастаисмоимижеланияминегрехсчитатьсявпервуюочередьаа

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.