НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали:

ФБ-32 Рибчук Нікіта

ФБ-32 Луценко Євгеній

КПІ 2025

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).

$$\begin{cases} Y^{*} \equiv aX^{*} + b \pmod{m^2} \\ Y^{**} \equiv aX^{**} + b \pmod{m^2} \end{cases}, \quad (1)$$

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.

Хід роботи

(варіант 3)

Першим кроком розбиваємо текст на біграми (що не перетинаються) і виводимо п'ять найчастіших у шифротексті та п'ять найчастіших біграм російської мови:

```
[Крок 2] Знайдені 5 найчастіших біграм шифртексту:
  > ['тд', 'рб', 'во', 'щю', 'кд']
  > Відомі 5 найчастіших біграм відкритого тексту:
  > ['ст', 'но', 'то', 'на', 'ен']
```

Таким чином, під час атаки розглядалися 20 упорядкованих пар біграм з множини відкритого тексту (5×4) та 20 упорядкованих пар з множини шифротексту (5×4), що в сукупності дало 20×20 = 400 унікальних пар X/Y для перевірки.

Далі виконувалось відновлення параметрів ключа афінного шифру – коефіцієнтів a та b.

Для знаходження двох невідомих (a і b) програма використовувала дві пари біграм-припущень: (X*, Y*) та (X**, Y**). Це дозволяло скласти систему з двох лінійних порівнянь:

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

На основі цієї системи спочатку обчислювались можливі значення a:

$$Y^* - Y^{**} \equiv a(X^* - X^{**}) \pmod{m^2}.$$

І потім для кожного валідного a знаходилось відповідне b за формулою:

$$b = (Y^* - aX^*) \bmod m^2.$$

Для кожного кандидата (a, b) виконувалося дешифрування шифротексту. Програма перевіряла, чи схожий результат на російську мову за таким критерієм:

- сумарна частота літер «о», «а» та «е» перевищує 25%.

Як видно з виводу у коді та запису у decrypted_correct_key.txt: (a, b): (199, 700) – цей ключ успішно пройшов перевірку. Отже, дешифрований текст є осмисленим.

Розшифрований текст:

отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотд
ельногочеловекавовсякомслучаеоноглавныйисточникчувствавинынеизвестноед
инственныйлиисследованиямнеудалосьещеустановитьдушевноепроисхождение
виныипотребностиискупленияноотнюдьнесущественноединственныйлиэтоисто
чникпсихологическоеположениесложноинуждаетсявобъясненияхотношениемаль
чикакотцукакмыговоримамбивалентнопомимоненавистиизакоторойхотелосьб
ыотцакаксоперникаустранитьсуществуетобычнонекоторыядолянежностикнемуо
баотношениясливаютсявидентификациюсотцомхотелосьбызанятьместоотцапот
омучтоонвызываетвосхищениехотелосьбыбытькаконипотомучтохочетсяегоустр
анитьвсеэтонаталкиваетсянакрупноепрепятствиевопределенныймоментребенок
начинаетпониматьчтопопыткаустранитьотцакаксоперникавстретилабысосторон
ыотцанаказаниечерезкастрациюизстрахакастрациитоестьвинтересахсохранения
своеймужественностиребенокотказываетсяотжеланияобладатьматерьюиотустра
нениятцапосколькуэтожеланиеостаетсявобластибессознательногооноявляется
основойдляобразованиячувствавинынамкажетсячтомыописалинормальныепроц
ессыобычнуюсудьбутакназываемогоэдиповакомплексаследуетоднаковнестиваж
ноедополнениевозникаютдальнейшиеосложненияеслиуребенкасильнееразвитко
нституционныйфакторназываемыйнамибисексуальностьютогдаподугрозойпоте
римужественностичерезкастрациюукрепляетсятенденцияуклонитьсявсторонуж
енственностиболеетоготенденцияпоставитьсебянаместоматерииперенятьеероль
какобекталюбвиотцаодналишьбоязнькастрацииделаетэтуразвязкуневозможнойр
ебенокпонимаетчтоондолженвзятьнасебяикастрированиееслионхочетбытьлюби
мымотцомкакженщинатакобрекаютсянавытеснениеобапорыванеиавистькотцуи
влюбленностьвотцаизвестнаяпсихологическаяразницаусматриваетсявтомчтоотн
енавистикотцуотказываютсявследствиестрахапередвнешнейопасностьюкастрац
иейвлюбленностьжевотцавоспринимаетсякаквнутренняяопасностьпервичногоп
озываякотораяпосутисвоейсновавозвращаетсяктойжевнешнейопасностистрахпер
едотцамделаетненавистькотцунеприемлемойкастрацияужаснакаквкачествекары
такиценылюбвиизобоихфактороввытесняющихненавистькотцупервыйнепосред
ственныйстрахнаказанияикастрациисследуетназватьнормальнымпатогеническое
усилениепривноситсякаккажетсялишьдругимфакторомбоязньюженственнойуст
ановкиярковыраженнаябисексуальнаясклонностьстановитсятакимобразомодни
мизусловийилиподтверждениейневрозаэтусклонностьочевидноследуетпризнатьи
удостоевскогоионалатентнаягомосексуальностьпроявляетсявдозволенномвидев
томзначениикакоеимелавегожизнидружбасмужчинамивегодостранностинежно
мотношениихсоперникамвлюбвиивегопрекрасномпониманииположенийобясни
мыхлишьвытесненнойгомосексуальностьюкакнаэтоуказываютмногочисленные
примерыизегопроизведенийсожалеюноничегонемогуизменитьеелиподробности
оненавистиилюбвикотцуиобихвидоизмененияхподвлияниемугрозыкастрациине
сведущемувпсихоанализечителюпокажутсябезвкуснымиималовероятнымипр
едполагаючтоименнокомплекскастрациибудетотклоненсильнеевсегоносмеюуве
ритьчтопсихоаналитическийопытставитименноэтиявленияявнесякогосомнения

инаходитвнихключклюбомуневрозуиспытаемжеговслучаетакназываемойэпиле
псиинашегописателянонашемусознаниютакчуждытеявлениявовластикоторыхна
ходитсянашабессознательнаяпсихическаяжизньуказаннымвышенеисчерпывают
сявэдиповомкомплексепоследствиявытесненияненавистикотцуновымявляетсят
очтовконцеконцовотождествлениесотцомзавоевываетвнашемяпостоянноеместо
этоотождествлениевоспринимаетсянашимянопредставляетсобойвнемособуюин
станциюпротивостоящуюостальномусодержаниюнашегоямыназываемтогдаэтуи
нстанциюнашимсверхяиприписываемейнаследницеродительскоговлияниянаива
жнейшиефункцииеслиотецбылсуровнасильственжестокнашесверхяперенимаето
тнегоэтикачестваивегоотношениикяснованозникаетпассивностькоторойкакразн
адлежалобыбытьвытесненнойсверхясталосадистическимстановитсямазохистск
имтоестьвосновесвоейженственнопассивнымвнашемявозникаетбольшаяпотреб
ностьвнаказаниииияотчастиотдаетсебякактаковоевраспоряжениесудьбыотчастиж
енаходитудовлетворениевжестокомобращениисснимсверхясознаниевиныкаждая
караявляетсяведьвосновесвоейкастрациейикактаковаяосуществлениемизначаль
ногопассивногоотношениякотцуисудьбавконцеконцовлишьдальнейшаяпроекци
яотцанормальныеявленияпроисходящиеприформированиисовестидолжныпоход
итьнаописанныездесьанормальныенамещенеудалосьустановитьразграничениям
ежду нимизамечаетсячтонаибольшаярольздесьвконечномитогеприписываетсяпа
ссивнымэлементамвытесненнойженственностиищекакслучайныйфакторимеетз
начениеявляетсяливнушающийстрахотецивдействительностиособеннонасильст
веннымэтоотносится кдостоевскомуфактегоисключительногочувствавиныравно
какимазохистскогообразажизнимысводимкегоособенноярковыраженномукомпо
нентуженственностидостоевскогоможноопределитьследующимобразомособенн
осильнаябисексуальнаяпредрасположенностьиспособностьсособойсилойзащищ
атьсяотзависимостиотчрезвычайносуровогоотцаэтотхарактербисексуальностим
ыдобавляемкранееузнаннымкомпонентамегосуществараннийсимптомприпадко
всмертиможнорассматриватькакотождествлениесвоегоясотцомдопущенноевкач
ественаказаниясосторонысверхятызахотелубитьотцадабыстатьотцомсамомутеп
ерьтыотецноотецмертвыйобычныймеханизмистерическихсимптомовиктомужет
еперьтебяубиваетотецдлянашегоясимптомсмертиявляетсяудовлетворениемфант
азиимужскогожеланияиодновременномазохистскимпосредствомнаказаниятоест
ьсадистическимудовлетворениемобаяисверхяиграютрольотцаидальшевобщемот
ношениемеждуличностьюиобектомотцаприсохраненииегосодержанияперешлов
отношениемеждуяисверхяноваяинсценировканавторойсценетакиеинфантильны
ереакцииэдиповакомплексамогутзаглохнутьеслидействительностьнедаетимвдал
ьнейшемпищинохарактеротцаостаетсятемжесамымнетонухудшаетсясгодамитак
имобразомпродолжаетоставатьсяиненавистьдостоевскогокотцужеланиесмертиэ
томузломуотцустановитсяопаснымеслитакиевытесненныежеланияосуществляю
тсянаделефантазиясталареальностьювсемерызащитытеперьа

Висновки

У цьому комп’ютерному практикумі ми розглянули принцип шифрування біграм за допомогою афінного шифру та навчилися виконувати його криптоаналіз із застосуванням частотного підходу. У процесі виконання завдання повторили обчислення обернених елементів за модулем за допомогою розширеного алгоритму Евкліда та розв’язування лінійних рівнянь. Також була розроблена програма, яка автоматично визначає ключ та відновлює змістовний відкритий текст. У результаті вдалося знайти правильний ключ ($a = 199$, $b = 700$) і розшифрувати наданий шифротекст.