Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут ім. Ігоря Сікорського”
Фізико-технічний інститут

Лабораторна робота № 3

з предмету «Криптографія»

«Криптоаналіз афінної біграмної підстановки»

Варіант 3

Виконали:
Студентки ФБ-33
Яремко Аліна,
Журавльова Марія

Київ - 2025

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

Порядок виконання роботи

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:

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

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.

Спочатку ми працювали з файлом **V3.txt** з папки fot_test. Для нього ми отримали 5 найчастіший біграм, які надалі були зіставлені з найбільш поширеними біграмами російської мови («ст», «но», «то», «на», «ен»)

```
Довжина очищеного тексту: 2540 символів
Кількість неперекривних біграм: 1270

Топ-5:
ыв — 30 разів (2.3622%)
хр — 22 разів (1.7323%)
хф — 20 разів (1.5748%)
йз — 19 разів (1.4961%)
ыя — 18 разів (1.4173%)
```

На основі усіх можливих пар зіставлення частих біграм відкритого тексту та шифртексту було складено та розв'язано систему двох лінійних порівнянь, що дозволило отримати множину кандидатів на ключ (a, b) афінного перетворення. Для кожного знайденого ключа було виконано дешифрування шифртексту. Оскільки не кожен результат є осмисленим текстом, було реалізовано автоматичний розпізнавач російської мови, який оцінював:

- сумарну частоту вживання частих літер («о», «е», «а»);

- сумарну частоту рідкісних літер («ф», «щ», «ь»).

Отриманий ключ:

```
ЗНАЙДЕНО ВІРНИЙ КЛЮЧ: a = 890, b = 102
```

Дешифрований текст:
виднарушениявстречаетсянаиболеечастопоследствиямогутбытьсамыеразныееслипохи
щентекстknигисправочниканакоторуюпотраченымесяцыработыдесятковлюдейтодлякол
лективаавторовэтокатастрофаипотеримогутвыражатьсявтысячахдолларроводнакоесликн
игаужеизданатодостаточнолишьслегкапожуритьпохитителяирассказатьослучившемсяво
тделеновостейгазетыилипотелевидениюпохитительможетсделатькнигевеликолепнуюре
кламуоченьважнуюинформациюоберегаемуюотраскрытияпредставляютсведенияолюдя
хисторииболезниписьмасостояниясчетоввбанкаходнакопомнениюбольшогочисласпеци
алистовугрозыличностисведениемкомпьютеровосталисьнатомжеуровнеивтомжесостоя
ниичтоидообширногоиспользованияэвмведениевсовременномиретуризмстановитсяв
себолееважнойбыстроразвивающейсяотрасльюхозяйствадоходыоттуризмастановятсява
жнойчастьювалютныхпоступленийвомногихстранахразвитиетуризмаспособствуетрост
убщественногопроизводстваулучшениюегоструктурыроступроизводительноститрудав
омногихотрасляхэкономикидаженеимеющихктуризмупрямогоотношениямеждународно
етуристскоепотреблениестимулируетмногочисленныеэкономическиепроцессыоткрыва
ющиедополнительныерынкидляпродукциинетуристскихотраслейсоздаваятемсамымусл
овиядляростапроизводствавсеэтифакторыделаютразвитиеиндустриитуризмаоченьважн
ымдлястранспереходнымтипомэкономикиеономическиетрудностикоторыепереживаютэ
тигосударстванемогутнесказатьсянауровнеразвитиятуризманоприэтомкаждаястранаиме
етвэтомотношениисвоюспецификуцельданнойработырассмотретьипроанализироватьор
ганизациютуристскойдеятельностивстранепереходнымтипомэкономикинапримеревен
гриивначалерассматриваютсятеоретикометодическиеположенияисследованиязатемдает
сяоценкаразличныхфакторовразвитияиндустриитуризмавенгрииприродноресурсныйкул
ьтурноисторическийиинфраструктурныйпотенциалкомплексноетуристскоерайонирован
иедалеепроводитсяанализсовременногосостоянияиндустриитуризмавенгриииеотдельны
хкомпонентовнафонеобщегоуровняэкономическогоразвитиястраныдаетсяоценкасоциал
ьноэкономическойролииндустриитуризмавэкономикевенгриивзаключениепроводится
общийанализорганизациитуристскойдеятельностивстранахпереходнымтипомэкономи
кивобщемивенгриивчастностивенгияпринадлежакстранамспереходнымтипомэкономик
иимееттемнеменееспецифическиечертыкоторыеотличаютееотдругихстранэтоготипавот
ношенииразвитияиндустриитуризмаосновнойтакойчертойявляетсяточтотуризмвенгрии
развиваетсяужедавноешевначаледвадцатоговекавэтойстранесложилисьтрадиционныету
ристскиесвязитуризмявляетсяважнойотрасльюнародногохозяйствасовременнойвенгрии
количествоиностранныхтуристовпосещающихвенгриюрастетизгодавгодтомунемалоспо
собствуетбогатейшийкультурноисторическийиприрод

Далі ми працювали з основним файлом **03.txt** з папки variants. Аналогічно знайшли найчастіші біграми:

```
Довжина очищеного тексту: 5630 символів
Кількість неперекривних біграм: 2815

Топ-5:
тд — 77 разів (2.7353%)
рб — 53 разів (1.8828%)
во — 52 разів (1.8472%)
щю — 45 разів (1.5986%)
кд — 42 разів (1.4920%)
```

Ключ:

```
ЗНАЙДЕНО ВІРНИЙ КЛЮЧ: a = 199, b = 700
```

Але при самому розшифруванні виникли проблеми. Можна побачити, що дешифрований текст виходить спотвореним:
отцеубийствокакизвестноосновноеиизначалыноягрестнглениечеловечестваиотделыноц очеловекавовсякомслучаеонфплавньйисточникчувствавиньнеизвестноединственньйлии сследованиямнеудалосыещеустановитыдушевноепроисхыждениевиньипотребностииск нглениянноотнюдынесзщественноединствебньйлиэтоисточнидгси……

Проаналізувавши методичні вказівки та отриманий текст, було виявлено, що автор шифру використовував варіант алфавіту, в якому літери “ы” та “ь” займали зворотні позиції порівняно з алфавітом, який ми використовували спочатку. Врахування цієї особливості дозволило отримати повністю змістовний текст.

Дешифрований текст:
отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотдельного человекавовсякомслучаеоноглавныйисточникчувствавинынеизвестноединственныйлии сследованиямнеудалосьещеустановитьдушевноепроисхождениевиныипотребностииску плениянноотнюдьнесущественноединственныйлиэтоисточникпсихологическоеположени есложноинуждаетсявобясненияхотношениемальчикакотцукакмыговоримамбивалентно помимоненавистииззакоторойхотелосьбыотцакаксоперникаустранитьсуществуетобычн онекотораядолянежностикнемуобаотношениясливаютсявидентификациюсотцомхотело сьбызанятьместоотцапотомучтоонвызываетвосхищениехотелосьбыбытькаконипотомуч тохочетсяегоустранитьвсеэтонаталкиваетсянакрупноепрепятствиевопределенныймомен требенокначинаетпониматьчтопопыткаустранитьотцакаксоперникавстретилабысосторо ныотцанаказаниечерезкастрациюизстрахакастрациитоестьвинтересахсохранениясвоей мужественностиребенокотказываетсяотжеланияобладатьматерьюиотустраненияотцапо сколькуэтожеланиеостаетсявобластибессознательногооноявляетсяосновойдляобразован иячувствавинынамкажетсячтомыописалинормальныепроцессыобычнуюсудьбутакназы ваемогоэдиповакомплексаследуетоднаковнестиважноедополнениевозникаютдальнейши еосложненияеслиуребенкасильнееразвитконституционныйфакторназываемыйнамибисе ксуальностьютогдаподугрозойпотеримужественностичерезкастрациюукрепляетсятенде нцияуклонитьсявсторонуженственностиболеетоготенденцияпоставитьсебянаместомате

рииперенятьеероликакобекталюбвиотцаодналишьбоязнькастрацииделаетэтуразвязкуне
возможнойребенокпонимаетчтоондолженвзятьнасебяикастрированиееслионхочетбытьл
юбимымотцомкакженщинатакобрекаютсянавытеснениеобапорываненавистькотцуивлю
бленностьвотцаизвестнаяпсихологическаяразницаусматриваетсявтомчтоотненавистико
тцуотказываютсявследствиестрахапередвнешнейопасностьюкастрацииейвлюбленностьж
евотцавоспринимаетсякаквнутренняяопасностьпервичногопозывакотораяпосутисвоейс
новавозвращаетсяктойжевнешнейопасностистрахпередотцамделаетненавистькотцунеп
риемлемойкастрацияужаснакаквкачествекарытакиценылюбвиизобоихфактороввытесня
ющихненавистькотцупервыйнепосредственныйстрахнаказанияикастрациисследуетназва
тьнормальнымпатогеническоеусилениепривноситсякаккажетсялишьдругимфакторомбо
язньюженственнойустановкиярковыраженнаябисексуальнаясклонностьстановитсятаки
мобразомоднимизусловийилиподтвержденийневрозаэтусклонностьочевидноследуетпр
изнатьиудостоевскогоионалатентнаягомосексуальностьпроявляетсявдозволенномвидев
томзначениикакоеимелавегожизнидружбасмужчинамивегодостранностинежномотноше
нииксоперникамвлюбвиивегопрекрасномпониманииположенийобяснимыхлишьвытесн
еннойгомосексуальностьюкакнаэтоуказываютмногочисленныепримерыизегопроизведе
нийсожалеюноничегонемогуизменитьеелиподробностионенавистиилюбвикотцуиобихв
идоизмененияхподвлияниемугрозыкастрациинесведущемувпсихоанализечителюпока
жутсябезвкуснымиималовероятнымипредполагаючтоименнокомплекскастрациибудетот
клоненсильнеевсегоносмеюуверитьчтопсихоаналитическийопытставитименноэтиявлен
иявневсякогосомненияинаходитвнихключклюбомуневрозуиспытаемжеговслучаетакна
зываемойэпилепсиинашегописателянонашемусознаниютакчуждытеявленияявластикот
орыхнаходитсянашабессознательнаяпсихическаяжизньуказаннымвышенеисчерпывают
сявэдиповомкомплексепоследствиявытесненияненавистикотцуновымявляетсяточтовко
нцеконцовотождествлениесотцомзавоевываетвнашемяпостоянноеместоэтоотождествле
ниевоспринимаетсянашимянопредставляетсобойвнемособуюинстанциюпротивостоящу
юостальномусодержаниюнашегоямыназываемтогдаэтуинстанциюнашимсверхяиприпис
ываемейнаследницеродительскоговлияниянаиважнейшиефункцииеслиотецбылсуровна
сильственжестокнашесверхяперенимаетотнегоэтикачестваивегоотношениикясновавозн
икаетпассивностькоторойкакразнадлежалобыбытьвытесненнойсверхясталосадистическ
имстановитсямазохистскимтоестьвосновесвоейженственнопассивнымвнашемявозник
аетбольшаяпотребностьвнаказанииияотчастиотдаетсебякактаковоевраспоряжениесудьб
ыотчастиженаходитудовлетворениевжестокомобращениинимсверхясознаниевиныкажд
аякараявляетсяведьвосновесвоейкастрациейикактаковаяосуществлениемизначальногоп
ассивногоотношениякотцуисудьбавконцеконцовлишьдальнейшаяпроекцияотцанормаль
ныеявленияпроисходящиеприформированиисовестидолжныпоходитьнаописанныездесь
анормальныенамещенеудалосьустановитьразграниченияміждунимизамечаетсячтонаиб
ольшаярольздесьвконечномитогеприписываетсяпассивнымэлементамвытесненнойженс
твенностиищекакслучайныйфакторимеетзначениеявляетсяливнушающийстрахотецивд
ействительностиособеннонасильственнымэтоотносится кдостоевскомуфактегоисключи
тельногочувствавиныравнокакимазохистскогообразажизнимысводимкегоособенноярко
выраженномукомпонентуженственностидостоевскогоможноопределитьследующимобр
азомособенносильнаябисексуальнаяпредрасположенностьиспособностьсособойсилойза
щищатьсяотзависимостиотчрезвычайносуровогоотцаэтотхарактербисексуальностимыд

обавляемкранееузнаннымкомпонентамегосуществараннийсимптомприпадковсмертимо
жнорассматриватькакотождествлениесвоегоясотцомдопущенноевкачественаказаниясос
торонысверхятызахотелубитьотцадабыстатьотцомсамомутеперьтыотецноотецмертвыйо
бычныймеханизмистерическихсимптомовиктомужетеперьтебяубиваетотецдлянашегояс
имптомсмертиявляетсяудовлетворениемфантазиимужскогожеланияиодновременномазо
хистскимпосредствомнаказаниятоестьсадистическимудовлетворениемобаяисверхяигра
ютрольотцаидальшевобщемотношениемеждуличностьюиобектомотцаприсохраненииег
осодержанияперешловотношениемеждуяисверхяноваяинсценировканавторойсценетаки
еинфантильныереакцииэдиповакомплексамогутзаглохнутьеслидействительностьнедает
имвдальнейшемпищинохарактеротцаостаетсятемжесамымнетонухудшаетсясгодамитак
имобразомпродолжаетоставатьсяиненавистьдостоевскогокотцужеланиесмертиэтомузло
муотцустановитсяопаснымеслитакиевытесненныежеланияосуществляютсянаделефант
азиясталареальностьювсемерызащитытеперьа

Висновки.

У ході роботи було реалізовано криптоаналіз афінного шифру на біграмах. Було обчислено частоти біграм шифртексту та визначено п’ять найбільш уживаних.
На основі зіставлення частих біграм відкритого тексту та шифртексту було складено та розв’язано систему рівнянь, що дозволило знайти кандидати на ключ шифрування.
Після дешифрування для кожного ключа та перевірки змістовності тексту було визначено правильний ключ та відновлено початковий текст.