Міністерство освіти і науки України

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

Криптографія

Комп’ютерний практикум №3

Криптоаналіз афінної біграмної підстановки

Виконали:

Студенти 3 курсу

Гончаров Д. К. та Сергеев А. А.

МЕТА РОБОТИ

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

ПОСТАНОВКА ЗАДАЧІ ТА ВАРІАНТ ЗАВДАННЯ

Завдання: Провести криптоаналіз шифртексту, зашифрованого за допомогою афінної біграмної підстановки, використовуючи частотний аналіз біграм. Знайти ключ шифрування (a, b) та розшифрувати текст.

Шифртекст: 02.txt

Параметри шифру:

- Алфавіт: 31 буква російської мови.
- Модуль шифрування: ***m^2 = 31^2 = 961.***
- Правило шифрування: ***Y = (aX + b) mod m^2***.
- Правило розшифрування: ***X = a^(-1) * (Y - b)*** mod m^2.
- Умова для ключа "a": a повинно бути взаємно простим з m^2.

ХІД РОБОТИ

РЕАЛІЗАЦІЯ МАТЕМАТИЧНИХ ПІДПРОГРАМ

1. **Розширений Алгоритм Евкліда:** Реалізовано функцію для обчислення ***d = gcd(a, n)*** та коефіцієнтів u, v таких, що ***d = ua + vn.***
2. **Обчислення Оберненого Елемента:** Реалізовано функцію для знаходження a^(-1) mod n, що існує лише за умови ***gcd(a, n) = 1***.
3. **Розв'язування Лінійних Порівнянь:** Реалізовано функцію для розв'язання ax = b (mod n), з коректною обробкою випадків, коли порівняння має один, декілька або не має розв'язків.

Функції реалізовані у скрипті: CryptoLab3FindKeys.py

ЧАСТОТНИЙ АНАЛІЗ ШИФРТЕКСТУ

За допомогою програми підрахунку частот біграм знайдено 5 найчастіших біграм шифртексту.

Еталонні біграми російської мови (для порівняння): "ст", "но", "то", "на", "ен".

Знайдені найчастіші біграми шифртексту:

```
--- Аналіз (31 букв, 'ё' -> 'е') ---
Файл 02.txt завантажений. Всього символів для аналізу: 4958

--- 5 найбільш частих біграм ---
'йа': 49 раз
'юа': 45 раз
'чш': 41 раз
'юд': 36 раз
'рщ': 31 раз

------------------------------
Список біграм:
------------------------------
ciphertext_top_N = ['йа', 'юа', 'чш', 'юд', 'рщ']
------------------------------
```

'йа', 'юа', 'чш', 'юд', 'рщ'

Скрипт: CryptoLab3FindBigrams.py

Для кожного співставлення двох біграм (X_k -> Y_i) та (X_l -> Y_j) розв'язана система порівнянь:

Y_i - Y_j = a * (X_k - X_l) (mod m^2)

Це дозволило знайти всі можливі значення **a**. Для кожного **a** знайдено відповідне **b** за формулою:

b = (Y_i - a * X_k) mod m^2

Відібрані кандидати на ключ (a, b) для подальшої перевірки знайдені(ключі збережені у файлі keys.txt).

```
Алфавіт: 31 букв. Модуль M = m*m = 961
Пошук ключів...
Знайдено 219 ключів.
Ключі збережені у файл 'keys.txt'.
```

Перші 10 ключів (a, b):

```
 1   4,533
 2   6,350
 3   8,5
 4   14,579
 5   18,703
 6   27,211
 7   30,886
 8   35,99
 9   42,911
10   45,66
```

Скрипт: CryptoLab3FindKeys.py

ВИКОРИСТАННЯ КЛЮЧІВ ДЛЯ РОЗШИФРУВАННЯ

Отримаємо варіанти відкритих текстів, використовуючи ключі для розшифрування

```
#195: Тестуємо ключ a=871, b=489...
#196: Тестуємо ключ a=872, b=874...
#197: Тестуємо ключ a=879, b=260...
#198: Тестуємо ключ a=889, b=124...
#199: Тестуємо ключ a=895, b=211...
#200: Тестуємо ключ a=895, b=552...
#201: Тестуємо ключ a=903, b=440...
#202: Тестуємо ключ a=908, b=954...
#203: Тестуємо ключ a=913, b=734...
#204: Тестуємо ключ a=916, b=775...
#205: Тестуємо ключ a=916, b=779...
#206: Тестуємо ключ a=919, b=105...
#207: Тестуємо ключ a=926, b=118...
#208: Тестуємо ключ a=931, b=916...
#209: Тестуємо ключ a=934, b=6...
#210: Тестуємо ключ a=934, b=10...
#211: Тестуємо ключ a=934, b=248...
#212: Тестуємо ключ a=934, b=252...
#213: Тестуємо ключ a=934, b=589...
#214: Тестуємо ключ a=934, b=630...
#215: Тестуємо ключ a=943, b=721...
#216: Тестуємо ключ a=947, b=841...
#217: Тестуємо ключ a=953, b=292...
#218: Тестуємо ключ a=955, b=325...
#219: Тестуємо ключ a=957, b=645...
----------------------------
Розшифрування завершено.
```

Тексти збережені у файлі all_decryptions.txt

```
1   a=4, b=533
2   яшяэходкятрмьфяэнтятиутбпккмйпурсчтпимшлюрбкюфкэгфьэяеабкэькщюхпэ
3   a=6, b=350
4   жарнфойбеьжчштрндьеьцззыжбвчцщуезфэщлчцмеезбптннитоныиыыннобвшящщ
5   a=8, b=5
6   срстэлдйснккаостшнснхюыфщйзкжььмлаыьжкющбмтйбозтуоатбцсфзтайпгмьа
7   a=14, b=579
8   дисткобдяшцйююстгшяшвлнэндзйзбьуцхобвйпцхуйдгюютающтызяэютмдрежбр
9   a=18, b=703
10  яфнощдхкйюкзеыноуюйюпмаифкузптдбажстцзщшфбкквымокывоьвьимовкиээты
```

Скрипт: CryptoLab3Decode.py

РОЗПІЗНАВАЧ РОСІЙСЬКОЇ МОВИ

Опис роботи розпізнавача (з обґрунтуванням коректності):

Для розпізнавання було обрано порівняння частот символів у тексті та знаходження суми квадратів різниць частот. То ж для кожного текста буде оцінка, яка буде вказувати на схожість тексту на довільний відкритий.

Чим нижче оцінка, тим більше текст нам підходить.

```
Читання файла 'all_decryptions.txt'...
Знайдено 438 строк. Починаємо аналіз...
----------------------------
Строка: 002 | Оцінка: 0.02752497
Строка: 004 | Оцінка: 0.02346516
Строка: 006 | Оцінка: 0.02330161
Строка: 008 | Оцінка: 0.02531509
Строка: 010 | Оцінка: 0.03230579
Строка: 012 | Оцінка: 0.00068761
Строка: 014 | Оцінка: 0.02853929
Строка: 016 | Оцінка: 0.02584738
Строка: 018 | Оцінка: 0.02362762
Строка: 020 | Оцінка: 0.02484736
Строка: 022 | Оцінка: 0.02463919
Строка: 024 | Оцінка: 0.02047907
Строка: 026 | Оцінка: 0.02313711
Строка: 028 | Оцінка: 0.00709310
Строка: 030 | Оцінка: 0.02380270
Строка: 032 | Оцінка: 0.02650108
Строка: 034 | Оцінка: 0.02574539
Строка: 036 | Оцінка: 0.02199428
Строка: 038 | Оцінка: 0.00654238
```

Далі знаходимо строку с найнижчою оцінкою

```
Аналіз завершений.
Найбільше співпадіннь частот у строці: 12
Оцінка(нижче - краще): 0.00068761

Початок текста:
однакоэтакартинаскакойшьстжроньмдеенирассматривалиралчльваетйявнлптонеичреьеленноепрвчадкипроявляющи...
```

Таким чином знайшли ключ і відповідний текст

```
11   a=27, b=211
12   однакоэтакартинаскакойшьстжроньмдеенирассматривалиралчльваетйявнлптонеичреьеленноепрвчадкипроявляющиесярезколчрикусьваниемуси
```

Скрипт: CryptoLab3FindText.py

РЕЗУЛЬТАТ

Ключ: (27, 211)

Текст:

однакоэтакартинаскакойшьстжроньмдеенирассматривалиралчльваетйявнлптон
еичреьеленноепрвчадкипроявляющиесярезколчрикусьваниемусиливающиесяд
оопасногодляжизнвчриводящегоктяжкомусамокалечениюмогутвсежевнекоторьх
случаяхнедостигатытакойсильцслабляясыдократкихсцстоянийабсансадобьстри
чроходящихголовокружениймогуттакжесменцтысякраткимвчериодафикогдабол
ынойсовершаешпуждьеегоприродячцступкикакшьнаходясывовластибессознате
лыногообуславливаясывобщемкакбьстранноэтониказалцсбпистотелесньмвчрич
инафиэтисцстояниямогумчервоначалыновозникатфчичричинатпистодушевньми
спугилимогутвдалынейшемнаходитыйявзависимцстиотдушевньхволненийкакни
характернодляогромногоболышинстваслщпаевинтнллектуалыноеснижениеноиз
вестезчокрайнеймереодинслщпайкогдаэтотнедлгненарушигвьсшейинтнллектуа
лынойдеятелыностигнлымголыцдругиеслучаивотношениикотжрьхутверждалос
ытожесамоененадежньилвчодлежатсомнениюкакислучайсамогодцстоевскоголи
цастрадающиеэпилепсиеймогутпроизводитывпечатлениетупостинеджразвитост
итаккакэыаболезнбпастосопряженасярковьраженньмидиотизмомикрупнейшиф
имозговьмидефэкыафинеявляясыконлпнообязатнлынойсоставноппастыюкарти
ньболезниноэтипрвчадкисовсемисвоимивидоизмененияфишьваютиудрлгихлицу
лиосполньмдушевньмразвитиефискжреесосверхошьчнаявболышинствеслщпае
внедцсыаточноуправляемойимиаффэктивнцстыхнеудивителыночтичриыакихоб
стоцтнлыствахневозможноусыановитысовокупнцстыклинопескоюаффэкыацчил
ячсиитфптопроявляетсяводнороднцстиуказанньхсимптомовтребуемчовидимом
уфункционалыногопониманиякакеслишьмеханизманжрмалыноговьсвобожьени
шчервичньхпозьвовбьлподготовленорганопескимеханизмкоторьйилчолызуетсш
чриналичиивесымаразньхусловийкадчринарушениимозговойдеятелыностчрит
яжкомзаболеваниитканейилитоксопескодзаболеванииыакипринедцсыаточномк
онтроледушевнойекономиикризисномфункционированиидушевнобэнергиизаэти
мраздлениемнадвавидамьчувствуемньентопностымеханизмалежащеговоснов
евьсвобожденияпервопньпчозьвовэтотмеханизмнедалекиотсексуалыньпчроцес
совпорождаемьхвсвоейосноветоксическиужедревнейшиеврюпиназьваликоитус

малойцчилячсиейивиднливполовомактесмяйпениеиадаптациювьсвобожьенияэ
пилептопескогоотводараздраженияэпилептопескаяреакциякаковьфименеммож
ноназватывсеэтовместевзятоенесомненнотакжепостнчаетиврапоряжениеневр
озасущнцстыкотороговтомчтобьликвидироватысоматическимассьраздраженияс
которьфиневрознеможетсправитысшчсихическиэпилептопескигчрипадоксыанов
итсцтакимобразомсимптомомистериииеюадщчтируетйяивидоизменяетсшчодоб
нотомукакэтопроисходитпринжрмалыномтлпениисексуалыногопроцессаыакимо
бразоммьлчолньжчравомразличаемжрганическуюиаффэктивнуюцчилячсиачрак
топескоезначениеэтогоследующеестрадающигчервогчжраженболезныюмозгаст
радающийвторойневротиквпервомслщпаедушевнаяжизнфчодверженанарушен
июизвневовторомслучаенарушениеявляетйявьражениемсамойдушевнойжизнив
есымавероцтночтоэпилепсиядостоевскогоотносится яковторомувидуточнодоказа
тыэтонелызяыаккаквтакомслщпаенужнобьлобьвклдпитывцелокупнцстыегодуше
внойжизниначалопрвчадковипоследующиевидоизмененияэтихпрвчадковадляэт
огоунаснедостатфпноданньхичисаниясафипчрипадковничегонедаютсведенияцс
оотношенияннмеждупрвчадкафивчереживанияфинеполньичастичротиворечивьв
сеговероятнеепредположенилптопрвчадкиначалисыьдцстоевскогоужевдетствеч
тоонивнюпалехарактеризовалисыболееслашьфисижчтомафиитолыкичцслепотр
ясшегоегичереживаниянавосемнадцатомгодужизниубийстваотцапринялифжрму
цчилячсиибьлобьвесымауместноеслишьичравдалцсытфптоонвчолностыюпрэкр
атилисывовремяотбьванияимкаторгивсибириноэтомнчротиворечатдругиеуказан
ияочевиднаясвязымеждуотцеубийствомвбратыяхкарамазовьхисьдгбойотцадост
оевскогобрцсиласывглазанеодномубиографьдцстоевскогоипослужилаимуказан
иемнаизвестноесовременноепсихологопескоенщчравлениепсихоанализтаккадч
одраяумеваетйяименноонсклоненвидетывэтомсошьтиитягчайшуютравмуивреак
циидцстоевскогонаэтоклдпевойпунктегоневрозаеслияначнуобосновьватыэтуусы
ановкнчсихоаналитопескиичасаюсычтоокажусынепонятньмдлявсехтехкомунезн
акомьучениеивьраженишчсихоанализаунасодиннадежньйисходньгчунктнафизв
естенсмьслпервьхпрвчадковдцстоевскоговегоюношескиегодьзадоугодичоявлен
ияцчилячсииуэтихпрвчадковбьличодобиесмертиониназьвалисыстрахомсмертии
вьражалисывсостояниилетаргическогцснаэтаболезнынаходилананеговнюпалэк
огдаоншьлещемалычикомкаквнезщчнаябезотчетнаяподавленностбпувствокакоз
чозжерассказьвалсвоемьдругусоловыевутакоекакбьдтошьемнчредстоялцсейча
сжеумеретыивсамомднленаступалосостояниесовершенничодобноедействител

ынойсмертиегобратандрейрассказьвасптофедоружевмолоддегодьпередтемкакз
аснутыцсыавлялзаписколтобоитйяночыюзаснутысмертоподобньмсномвчросимч
оэтомучтобдегопохоронилитолыкочеребчцтыднейдцстоевскийзарулеткойвведен
иеснамизвестньсмьслинамерениетакихпрвчадковсмертониозначаюттотожьеств
лениесумершимчеловекомкотжрьйьействитнлыноумериличпнловэкомживьмещ
енокоторомумьжелаемсмертивтжройслщпайболеезначителезчрипадоквуказанн
омслучаеравноцененнаказаниюмьпожелалисмертидрлгомутячерымьсыалисаф
иэтимдрлгимисамиумерлитутпсихоаналитическоещпениеутверждаетчтоэтотдру
гойдлямалычикаобвпноотециименуемьйистериейпрвчадокявляетйяыакимобраз
омсамонаказаниемзапожеланиесмертиненавистномуотцуа

ВИСНОВКИ

Мета роботи – набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки та опанування прийомами роботи в модулярній арифметиці – була повністю досягнута.

1. **Розкриття шифру:** Криптоаналіз афінної біграмної підстановки шифртексту було успішно завершено.
2. **Ефективний метод:** Найефективнішим методом виявився **частотний аналіз біграм**, який дозволив, шляхом розв'язання системи лінійних порівнянь у модулярній арифметиці, знайти 219 кандидатів на ключ.
3. **Ключові знання:** Успішно опановано прийоми роботи в модулярній арифметиці, зокрема реалізація Розширеного Алгоритму Евкліда та розв'язання лінійних порівнянь для пошуку ключів (a, b).
4. **Знайдений ключ:** На основі частотного аналізу символів розшифрованих текстів, найбільш імовірний відкритий текст було знайдено за допомогою ключа **(a, b) = (27, 211)**.