



Міністерство освіти і науки України
НТУУ «Київський політехнічний інститут»
Фізико-технічний інститут

Лабораторні роботи № 3
з предмету «Криптографія»
на тему: «Криптоаналіз афінної біграмної підстановки»

Варіант №15

Виконала:
Студентка III
курсу
ФТІ групи ФБ-84
Матвієнко В.С.
Перевірив:
Чорний О. М.

Київ-2020

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).
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:

Перед написанням коду я ознайомила з теоретичними відомостями і методичними вказівками. За допомогою програмного коду з лабораторної роботи №1 я знайшла 5 найчастіших біграм мови. У коді lab3.py реалізовані такі математичні операції: розширений алгоритм Евкліда, знаходження НСК чисел. Знайшла 5 найчастіших біграм шифротексту і знайшла усі можливі ключі. За допомогою автоматичного користувача знайшла змістовний текст російською мовою.

Найчастіші біграми шифротексту:

| Біграма | Частота(частота*100) |
|---------|----------------------|
| ьу | 1.0859 |
| як | 0.7963 |
| юк | 0.6636 |
| ьп | 0.6515 |
| оу | 0.5671 |

Автоматичний розпізнавач російської мови:

У своїй лабораторній роботі я зробила розпізнавач, що шукає індекс відповідності, який є найбільш близьким до теоретичного значення індексу відповідності(0,55), після чого перевіряє розшифрований текст на частоту частих літер. А саме щоб у 5ці найчастіших літер у розшифрованому тексті були літери «о», «а», «е» і не було літер «щ», «ь», «ф». Якщо розшифрований текст не підходить під критерії розпізнавача, то процедура повторюється, поки не буду знайдений розшифрований текст, що підходить даним критеріям.

| |
|--|
| <p>Ключ(424, 500)</p> <p>Індекс відповідності: $I(X)=0.05707641824451285$</p> |
|--|

| Зашифрованный текст | Розшифрованный текст |
|---|--|
| цбтызнэжрцяфьзюдрбубьсыццуаюкнажфдлпдрцядьдййдаьпуаксфцзгтыгпдрвцяшдршфцтдйюабцуйрдув рйдмузеуэйньюоеочшлукцкйиддьяпуактукляктафвкежспнйяршцтцпйзуюуирутшкдрлфюоцэрькдлщцтып | библейскоепреданиеговоритчтоотсутствиетрудлаприданностьбылаусловиемблагенствапервогочелове кадогоспадениялюбовькприданностиоказаласьтажеинадшемчеловекеинопроклятиевяготеетнадчелов |

[illegible][illegible]

Висновки:

Під час виконання комп'ютерного практикуму №3 я ознайомилась з шифром афінної біграмної підстановки, навчилась розшифровувати зашифровані тексти цим шифром. Зробила автоматичний розпізнавач, найбільш надійним є перевірка індексу відповідності. Я у своєму розпізнавачу використала і індекс відповідності, і частотний аналіз частих літер.