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

Варіант №2

Виконав: ФБ-11 Тимощук Ілья

Київ – 2023

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

Знайдені п'ять найчастіших біграм шифртексту - йа, юа, чш, рп, юд

Топ 5 найчастіших біграм з ЛР1 - ст, то, ен, но, ни

Опис роботи запропонованого мною автоматичного розпізнавача російської мови

Автоматичний розпізнавач російської мови одразу «відкидає» всі тексти, які містять заборонені біграми. Потім перевіряється чи входить в топ 5 найчастіших біграм біграма «ст».

Тобто автоматичний розпізнавач російської мови використовує *Критерій заборонених біграм* та *Критерій частих біграм*

Такого принципу автоматичного розпізнавання російської мови було достатньо щоб для тестового та реального тексту залишився лише один кандидат(хоча програма передбачає і більше, якщо частина вихідного тексту не відповідає очікуванням)

```
Top 5 encrypted bigrams:  ['йа', 'юа', 'чш', 'рп', 'юд']
Decryption successful!
однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопределенноеприпадкипроявляющи
Accept this key? (T/F): t
Decryption key: [27, 211]
```

Отже ключ – (27, 211)

Частина розшифрованого тексту(повний текст збережен в decrypted_task.txt):

однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопределенно
еприпадкипроявляющиесярезкосприкусываниемусиливающиесядоопасногодляжизнипривод

ящегоктяжкомусамокалечениюмогутвсежевнекоторыхслучаяхнедостигатьтакойсилыослабля
ясьдократкихсостоянийабсансадобыстропроходящихголовокруженийимогуттакжесменяться
краткимипериодамикогдабольнойсовершаетчуждыеегоприродепоступкикакбынаходясьвовла
стибессознательногообуславливаясьвобщемкакбыстранноэтониказалосьчистотелеснымиприч
инамиэтисостояниямогутпервоначальновозникатьпопричинамчистодушевнымиспугилимогу
твдальнейшемнаходитьсявзависимостиотдушевныхволненийкакнихарактернодляогромногоб
ольшинстваслучаевинтеллектуальноеснижениеноизвестенпокрайнеймереодинслучайкогдаэт
отнедугненарушилвысшейинтеллектуальнойдеятельностигельмгольцдругиеслучаивотношен
иикоторыхутверждалосьтожесамоененадежныилиподлежатсомнениюкакислучайсамогодосто
евскоголицастрадающиеэпилепсиеймогутпроизводитьвпечатлениетупостинедоразвитоститак
какэтаболезньчастосопряженасярковыраженнымидиотизмомикрупнейшимимозговымидефек
таминеявляяськонечнообязательнойсоставнойчастьюкартиныболезниноэтиприпадкисовсеми
своимивидоизмененияхмибываютиудругихлицулицсполнымдушевнымразвитиемискореесосве
рхобычнаявбольшинствеслучаевнедостаточноуправляемойимиаффективностьюнеудивительн
очтопритакихобстоятельствахневозможноустановитьсовокупностьклиническоюаффектаэпил

Труднощі, які виникли під час виконаня роботи

Під час виконання даної лабароторної роботи труднощів не виникало.

Висновок: в цій лабараторній роботі було засвоєно принцип розшифрування афінного шифру на основі частотного аналізу та за допомогою автоматичного розпізнавача мови.