Міністерство освіти і науки України
Національний технічний університет України
Київський політехнічний інститут імені Ігоря Сікорського
Фізико-Технічний інститут

Симетрична криптографія

Комп'ютерний практикум 3

Криптоаналіз афінної біграмної підстановки

Варіант 4

Виконав:
Волинець Сергій ФІ-03

Київ — 2023

1 Мета роботи

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

2 Завдання

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 шифротексту (за варіантом).

3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифротексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a, b) шляхом розв'язання системи рівнянь.

4. Для кожного кандидата на ключ дешифрувати шифротекст. Якщо шифротекст не є змістовним текстом російською мовою, відкинути цього кандидата.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним. У разі необхідності змінити кодування алфавіту (див. методичні вказівки).

Ось частина шифротексту для мого, четвертого, варіанту:

щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцк
мдыйдосштцмижбчфипмугфбзчшохдодвзбряцкмдбэдцхзнощк
яоэоюэтцюзныертзилгфоцбчполфмэдцщкйкшйэысйрэйкчозы
чфждьмйшотдотзьоюйсщзоюдууюзсшшстзрэыосяфоешыенывд
ьмиыыяшцрбгянямзюдшскдмыайыяаоешезвжпонорэкжцчж...

3 Пошук розшифрованого тексту

Для виконання даної роботи потрібно було створити якийсь розпізнавач мови. Я вирішив використати підхід з попереднього практикуму, обчислючи індекс відповідності. Якщо обчислений індекс задовільняє наступне:

$$|I - 0.0591| < 0.01,$$

то я буду вважати, що даний текст, це текст російською мовою. Даний підхід повинен працювати, бо 0.0591 це обчислене, в попередньому практикумі занчення, для біграм тексту на російській мові, а 0.03 — це значення індексу відповідності для шуму.

4 Результати

В результаті виконання практикуму було визначено, що п'ятьма найчастішими біграмами в шифро-тексті є: 'еш', 'шя', 'еы', 'до', 'зо', у порядку спадання. За замовчуванням відомо, що шайпоширенішими біграмами в нешифрованому тексті є: 'ст', 'но', 'то', 'на', 'ен'.

Попарно розв'язуючи систему рівнянь для пари біграм з наведених вище множин, я отримав наступні результати:

Ключ:

$$(390, 10)$$

Текст:

> еслиправдачтодостоевскийвсибиринебылподверженприпа
> дкамтоэтолишьподтверждаетточтоегоприпадкибылиегока
> ройонболеевнихненуждалсякогдабылкараеминымобразомн
> одоказатьэтоневозможноскорееэтойнеобходимостьювнак
> азаниидляпсихическойэконпмиидостоевскогообясняется
> точтоонпрошелнесломленнымчерезэтигодыбедствийиуниж
> енийосуждениедостоевскоговкачествеполитическогопре
> ступникабылонесправедливымиондолженбылэтознатьноон
> принялэтонезаслуженноенаказаниеотбатюшкицарякакзам
> енунаказаниязаслуженногоимзасвойгрехпоотношениюксв
> оемусобственномуотцу...

Алфавіт в даному випадку було скориговано на:

$$\text{абвгдежзийклмнопрстуфхцчшщьыэюя},$$

тобто символ 'ь' стоїть перед 'ы'.

5 Висновки

Шифр Афінної біграмної підстановки, як і шифр Віженера, добре піддається частотному криптоаналізу. Саме тому, його не слід використовувати.