Міністерство освіти і науки, молоді та спорту України
Національний технічний університет України
“Київський політехнічний інститут”
Фізико-Технічний інститут

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3
за семестровий курс предмету «Симетрична криптографія»

Роботу виконали:
Студенти групи ФІ-03
Починок Юрій

Приймав:
Чорний Олег Миколайович

Київ-2023

СИМЕТРИЧНА КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ No3

Криптоаналіз афінної біграмної підстановки

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 No1, 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),(ba шляхом розв'язання системи (1).

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).

Хід роботи

Виникали проблеми з написанням звичайних функцій, а також ініціалізацією окремих даних потрібних для коректності виконання роботи. Проблеми вирішились 11 годинним марафоном.

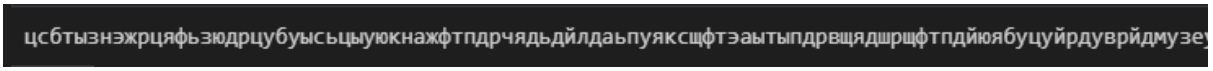
Розпізнавач

Розпізнавач базується на наявності популярних моно та біграм, а також перевірку на неіснуючі біграми. До перевірки надавалась найпопулярніша біграма "**ст**"

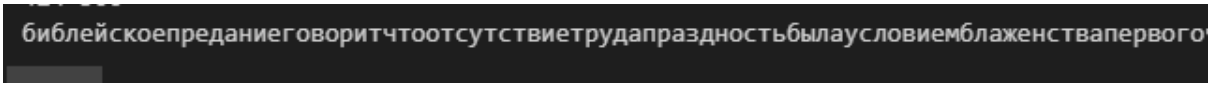
серед перших 5-ти найчастіших біграм, а також 2 найпопулярніші літери “**а**” та “**о**” серед 5-ти найчастіших біграм, перевірялись на неіснування біграми вигляду “**аь**” “**щщ**” і т.д. Коректність: За умови не знаходження тексту можна було збільшити кількість бі- або моно- грам що досліджувались, у випадку якщо було декілька текстів, що відповідають заданим критеріям їх можна було б розширит, але не довелось, також в випадку повернення всього декількох текстів можна було візуально визначити, який з них був змістовним.

Результати:

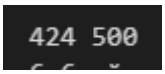
Початковий текст:



Розшифрований текст:



Ключ:



Висновки:

Якщо чесно. Ненавиджу програмувати.