Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут ім. Ігоря Сікорського”
Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали Студенти:
Дудченко І.В і Терпило С.Е
Варіант 2

Київ – 2022

Мета роботи:

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

Хід роботи:

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.

   Функції були реалізовані завдяки теоритичним відомостям описаним в методичці.

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

   Ми змінили код в комп'юетрному практикумі 1, щоб отримати біграми що ніколи не зустрічались в тексті.

```
impossible_bigrams = []
for bigram, frequency in bigram_frequency_without_space.items():
    if frequency == 0:
        impossible_bigrams.append(bigram)
print(impossible_bigrams)
```

   Ось що ми отримали, їх чимало як виявилось.

```
nonexistent_bigrams = ['аы', 'аь', 'бй', 'бф', 'бц', 'вй', 'гы', 'гй', 'гф', 'гц', 'гщ', 'гь', 'гю', 'дй', 'дщ', 'еы',
                       'еь', 'за', 'эб', 'зе', 'эж', 'эз', 'эи', 'эы', 'эн', 'эо', 'эр', 'эс', 'эу', 'эц', 'эч', 'эщ',
                       'эь', 'эю', 'эя', 'жы', 'жй', 'жф', 'жц', 'жш', 'жщ', 'жю', 'зй', 'зщ', 'иы', 'иь', 'ыы', 'ыь',
                       'йы', 'йй', 'йь', 'кы', 'кй', 'лй', 'лщ', 'мй', 'мю', 'нй', 'оы', 'оь', 'пг', 'пд', 'пэ', 'пж',
                       'пй', 'пф', 'пх', 'рэ', 'рй', 'сй', 'сщ', 'тй', 'тщ', 'уы', 'уь', 'фг', 'фэ', 'фж', 'фз', 'фй',
                       'фк', 'фп', 'фс', 'фх', 'фц', 'фч', 'фш', 'фщ', 'фю', 'хы', 'хй', 'хц', 'хь', 'хю', 'цй', 'цф',
                       'цц', 'цш', 'цщ', 'ць', 'цю', 'чы', 'чй', 'чф', 'чц', 'чщ', 'чю', 'шэ', 'шж', 'шз', 'шы', 'шй',
                       'шф', 'шц', 'шч', 'шш', 'шщ', 'шю', 'шя', 'щб', 'щв', 'щг', 'щж', 'щз', 'щы', 'щй', 'щк', 'щл',
                       'щм', 'щт', 'щф', 'щх', 'щц', 'щч', 'щш', 'щщ', 'щю', 'ьы', 'ьь', 'юы', 'юй', 'юь', 'яы', 'яь']
```

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 шляхом розв'язання системи (1).

   Найчастіші біграми зашифрованого тексту виявили таким е методом як і в першій лабі. Отримали такий результат.

```
most common bigrams in ciphertext:  ['йа', 'юа', 'чш', 'юд', 'рщ']
```

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

Змістовність тексту ми перевіряли перевіркою на найпоширенішу літеру, якщо це не «о» або «е», то текст явно нам не підходить. Також як додаткову перевірку взяли метод заборонених біграм, які були визначені в пункті 3.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

```
most common bigrams in ciphertext:  ['йа', 'юа', 'чш', 'юд', 'рщ']
possible keys: [(552, 232), (836, 173), (854, 934), (919, 105), (396, 684), (708, 741), (800, 573), (557, 390), (7
true key: (27, 211)
однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопределенноеприпадкипроявляющи
```

Ключі до афінного шифру 27, 211.