КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

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 №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:

1. Реалізуємо функції з необхідними математичними операціями:

розширений алгоритм Евкліда

```
def euclid(a, b):
    if b == 0:
        return a, 1, 0
    else:
        g, x, y = euclid(b, a % b)
        return (g, y, x - y * (a // b))
```

обчислення оберненого елементу за модулем

```
def inverted(a, mod):
    g, x, y = euclid(a, mod)
    if g != 1:
        return None
    return x
```

розв'язання лінійних порівнянь

```python
def solve_eq(a, b, mod):
    g, x, y = euclid(a, mod)
    if b%g != 0:
        return None
    if g == 1:
        return [(inverted(a, mod) * b) % mod]
    a = a // g
    b = b // g
    mod1 = mod // g
    x = []
    xx = (inverted(a, mod1) * b) % mod1
    while xx < mod:
        x.append(xx)
        xx += mod1
    return x
```

2. знайдемо 5 найчастіших біграм запропонованого шифртексту (варіант 16):

```
Most frequent bigrams in encrypted text: ['се', 'дэ', 'хв', 'те', 'че']
```

3-5. Переберемо всі комбінації найчастіших біграм відкритого та зашифрованого тексту, порахуємо ключ для кожної з них, спробуємо розшифрувати текст отриманими ключами та перевіримо кожен з отриманих текстів на змістовність.

Будемо відкидати тексти, які ми не змогли розшифрувати та тексти які містять біграму, яка не існує в російській мові:

```
impossible_bigrams = ["уь", "еь", "оь", "аь", "яь", "иь", "ыь", "ьь", "юь", "шы", "жы"]
```

```
Key: [770, 416]
Wrong text! уь found!
Key: [801, 943]
Wrong text! уь found!
Key: [832, 509]
Wrong text! уь found!
Key: [863, 75]
Wrong text! уь found!
Key: [894, 602]
Wrong text! уь found!
Key: [925, 168]
Wrong text! уь found!
Key: [956, 695]
Wrong text! уь found!
Key: [124, 718]
Failed to decrypt!
Key: [775, 253]
Failed to decrypt!
Key: [370, 312]
Text checked successfully!
```

Ми отримали ключ – 370, 312

Розшифрований текст у файлі 16_decrypted.txt

Висновок:

В ході цієї лабораторної я навчився використовувати частотний аналіз для розшифрування афінної біграмної підстановки.