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.

Спочатку треба було реалізувати підпрограми з операціями. Я виділила їх як функції в програмі.

Алгоритм Евкліда я реалізувала через цикл, а не рекурсивно, бо так швидше. Функція повертає u, v та gcd:

```
def evclid(a, b):
    u, u_temp, v, v_temp = 1, 0, 0, 1
    while (b!=0):
        q = a // b
        a, b = b, a % b
        u, u_temp = u_temp, u - u_temp*q
        v, v_temp = v_temp, v - v_temp*q
    return (u, v, a)
```

Розв'язок лінійного порівняння виконала через if. Бо маємо різну кількість коренів в залежності від умови. Функція повертає масив (список) коренів:

```
def rivnyanya(a, b, n):
    all_x = []
    gcd = evclid(a, n)[2]
    if (gcd==1):
        all_x.append((evclid(a, n)[0])*b%n)
        return all_x
    if (b%gcd!=0):
        return None
    x = (evclid(a//gcd, n//gcd)[0])*(b//gcd)%(n//gcd)
    for i in range(gcd):
        x_temp = x + (n//gcd)*i
        all_x.append(x_temp)
    return all_x
```

Потім шукаємо частоти біграм. У мене це такі біграми:

```
Counter({'то': 3852, 'ст': 2964, 'но': 2830, 'ен': 2629, 'на': 2611, '
Counter({'уф': 113, 'иж': 103, 'ьи': 93, 'хф': 86, 'щф': 84, 'кщ': 80,
```

Потім вирішуючи систему рівнянь і беручи два із першого списку, і два із другого і відкидаю не потрібних кандидатів. Я думала, що мені знадобляться майже усі умови змістовного тексту, але у

моєму випадку вистачило перевірити м'який знак після голосних. Ще більше мені повезло з тим, що перший варіант ключа (725, 100) виявився правильним. І ось частина розшифрованого тексту:

```
key:  [725] [100]
князьандрейприехалвглавнуюквартируармиивконцеиюнявойскапервойармиитойприкоторойна
```

Висновок: знайшла ключ і розшифрувала текст атакою на афінний шифр.