Грипас Владислав ФБ-12
Лабораторна робота №3
Варіант 15
Тема:

Криптоаналіз афінної біграмної підстановки

Мета:

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

Хід роботи;

Результат виконання програми:

```
[tdoors:...-23-24/cp3/hrypas_fb-12_cp3]$ python main.py
[('то', 12684), ('не', 8869), ('ст', 8632), ('ов', 8455), ('но', 8391)]
cyphertext:  цсбтызнэжрцяфьзюдрцубуысьцыуюкнажфтпдрчядьдйлдаь
possible solution: a = 424, b = 500
библейскоепреданиеговоритчтоотсутствиетрудапраздно
```

Розпізнавання тексту російської мови відбувається на основі порівнянна ентропії з “ідеальним” варіантом, що був обрахований на доволі великому тексті, було проведено декілька тестів на різних варіантах, результат розшиврування у всіх випадках відповідає відкритому тексту, для текстів меншої довжини можна збільшити допустиме відхилення ентропії

```
if  ideal_entropy - 0.1 <= shannon(dec_text) <= ideal_entropy + 0.1:
    print("possible solution: a = {}, b = {}".format(a, b))
    print(dec_text[:50])
```

Висновки:

В ході виконання лабораторної роботи я набув навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки, опанував прийоми роботи в модулярній арифметиці