КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Варіант 12

Виконали:
ФБ-05 Левицький Євген
ФБ-05 Дегтярьов Микола

Київ - 2022

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

Завдання:

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 шифротексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a , b) шляхом розв'язання системи.

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

Функції створені для виконання практичної роботи:
build_bigrams – створення біграм
bigram_to_int – перетворення біграм в числа
int_to_bigram – перетворення чисел в біграм
inverted_by_mod – обернення по модулю
linear_expression_solver – вирішення лінійного рівняння
system_solver – вирішення систем рівнянь
decrypt – розшифрування тексту
is_natural_text – перевірка тексту на натуральність
get_keys – пошук ключ для розшифрування

Було взято 5 найчастіших біграм з КП №1: 'ст', 'то', 'ен', 'но', 'пр'

Текст на змістовність перевіряємо за допомогою умови ['ф'] < 0.003, ['ц'] < 0.004, с['щ'] < 0.006, тобто частотою найменьш частих літер.

В результаті отримуємо єдиний результат зі зрозумілим текстом

```
 X : ('ст', 'то'), Y : ('вю', 'хк')
a = 555, b = 331
когдапожарныеисоседиушлилеоауфманосталсясдедушкойсполдингомдугласомитомомвсеонизадумчивосмотрелинадогорающие
```

Висновки

У ході даної лабораторної роботи ми набули навичок частотного аналізу на прикладі розкриття афінного шифру, поновили знання з модульної арифметики. Написали програму, яка розшифровує афінний шифр методом криптоаналізу афінної біграмної підстановки, відділяє змістовний текст від тексту-шуму при переборі можливих ключів.