КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконала: Левашова Світлана

Група: ФБ-13

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

Варіант 20

Хід роботи:

```
Топ 5 біграм шифртексту:
['шэ', 'чп', 'ьэ', 'ии', 'щп']
[772, 728, 834, 256, 790]
Топ 5 біграм мови:
['ст', 'но', 'то', 'на', 'ен']
[545, 417, 572, 403, 168]
```

- 1 рядок – найчастіші 5 біграм; 2 рядок – найчастіші 5 біграм в числовому значенні.

```
Знайдені кандидати в ключі:
Усього 162: {(721, 876), (664, 714), (96, 586), (161, 923),
```

- знайдено можливі кандидати ключів шляхом ‘комбінації’ числових значень біграм ШТ та мови.

```
Розшифрований текст для ключа (144, 89):
ростовпередоткрытиемкампанииполучилписьмоотродителейвкотором
```

- знайдено коректний ключ та розшифровано текст за допомогою нього.

Розшифрований текст в окремому файлику.

Опис роботи розпізнавача тексту російської мови:

Спершу алгоритм виділяє часті та рідко вживані літери, щоб отримати інформацію про мову, на якій написаний текст. Далі перевіряє наявність заборонених біграм у тексті, що вже завчасно встановлені. Це може бути корисно для виявлення некоректно розшифрованого тексту.

Якщо часті літери або рідкі літери зустрічаються у тексті занадто часто і відповідно навпаки, це може свідчити про коректність розшифровки.

Використання порогових значень для частот літер та заборонених біграм дозволяє адаптувати алгоритм до різних типів текстів.

Таким чином, розпізнавач може бути адаптований до різних мов та текстових особливостей.

Висновки:

Набули практичних навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки. Аналізуючи афінну біграмну підстановку, вдосконалили навички роботи в модулярній арифметиці.