КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3
Криптоаналіз афінної біграмної підстановки

Виконав студент: Медвецький Давид
Група: ФБ-13
Варіант 11

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

Порядок виконання роботи
Підрахуємо частоти біграм у тексті

Біграма	Частота
нк	0,014595
юж	0,013552
хб	0,01277
шь	0,01277
мк	0,012249

Тепер перетворимо наші біграми у числові значення

```
[413, 905, 652, 771, 382]
[545, 417, 572, 403, 168]
```

1 рядок найчастіші біграми шифротексту
2 рядок найчастіші біграми російської мови

Потім перебираємо всі комбінації можливих ключів

```
171
Возможные ключи: {(224, 714), (858, 88), (182, 589), (589, 382), (154, 582), (875, 833), (549, 437),
```

отримали 171 унікальну комбінацію (a, b) шляхом розв’язання рівняння:

$$Y^* - Y^{**} \equiv a(X^* - X^{**}) \pmod{m^2}.$$

$$b = (Y^* - aX^*) \bmod m^2.$$

Шляхом перебору всіх комбінацій ключів, розшифровки текстів і аналізу тексту на змістовність (метод біграм, що не зустрічаються в мові)

отримали змістовний текст і наш ключ

```
Наш ключ: (703, 956)
```

розшифрований текст наведено окремим файликом*

Ще один момент, який я підглянув у групі з лаб, це те що треба поміняти місцями “ь” та “ы” щоб в отриманому тексті не було “шуму”. Уривок було взято зі збірки Рея Бредбері “Вино из одуванчиков”

Висновок

У ході виконання лабораторної роботи, ми на практиці реалізували атаку на афінний шифр, набули деяких навичок частотного аналізу і розглянули способи розпізнавання змістовного тексту.