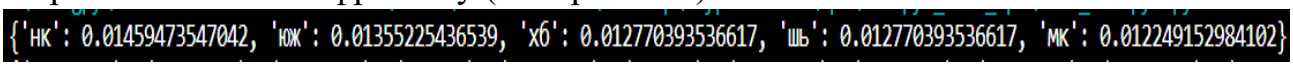
КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3
Криптоаналіз афінної біграмної підстановки

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

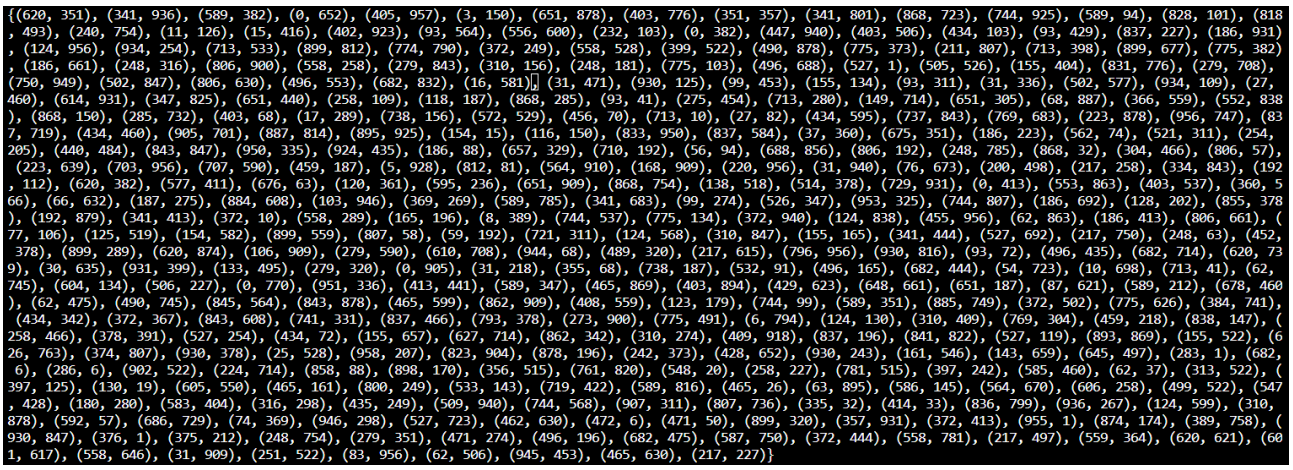
Варіант№11

Хід роботи:

0. Ознайомився з теоретичними відомостями та практичними вказівками до 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 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, знайшов 5 найчастіших біграм запропонованого шифртексту (за варіантом).



3. Перебрав можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення
знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).



4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинув цього кандидата.
5. Повторював дії 3-4 доти, доки дешифрований текст не буде змістовним ы записав його у файл "decrypted_text.txt"

Опис детектора російської:

Моя перевірка на те, російська це мова чи ні полягає у тому, щоб перевірити чи присутні заборонені біграми(banned_bigrams) в розшифрованому тексті. Якщо так – варіант відкидається.

Висновки: в ході виконання комп. Практикуму №3 я засвоїв методи частотного аналізу на прикладі розкриття моноалфавітноїпідстановки та опанував прийоми роботи в модулярній арифметиці. Навчився аналізувати шифротекст зашифрований методом афінної підстановки та проводити частотний аналіз з метою його розшифрування.