Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Лабораторна робота №3

З дисципліни «Криптографія»

Виконали:

студенти 3 курсу ФТІ
групи ФБ-83
Волинко Д.В.
Бондаренко.Р.С.

Перевірив:

Чорний О. М.

Вариант - 5

Мета роботи:

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

Порядок виконання:

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 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, відкинути цього кандидата.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним

Хід роботи:

1)Реалізували підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв’язуванням лінійних порівнянь.

2)У ході роботи було алгоритмічно знайдено п'ять найчастіших біграмм з шифрованого тексту для п'ятого варіанту та, порівнюючи їх із найчастішими біграммами російської мови, шляхом розвязання лінійних порівнянь отримали кандідатів на ключ.

П'ять найчастіших біграмм:

вн

тн

дк

хщ

ун

3)Останнім кроком(перед записом у файл) було зроблено перевірку на змістовність отриманного тексту шляхом співставлення п'яти найчастіших букв російської мови та п'яти найчастіших букв з кандидата на розшифрований текст

4)Також в ході виконання виникла необхідність заміни місцями літер "ь" та "ы", бо інакше текст неможливо було розшифрувати.

Розшифрований текст можна переглянути у відповідному файлі, що йде разом з протоколом.

Висновок: У цій роботі ми отримали навички з алгоритмізації базових необхідних операцій із модульною арифметикою, а також було розшифровано текст,що був зашифрований шифром біграмних підстановок.