Лабораторна робота №3

Криптоаналіз афінної біграмної підстановки

Виконали:

Анучін Максим ФБ-11

Ступак Ярослав ФБ-11

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

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

Використовуючи шматок коду з лабораторної роботи 1 аналізуємо біграми шифртексту, там беремо 5 найпопулярніших. Після цього порівнюємо їх з найпопулярнішими біграмами рос алфавіту: 'ст', 'но', 'ен', 'то', 'на'. Перебравши всі можливі пари отримуємо певну кількість ключів. Далі дешифруємо текст отриманими ключами, та використовуючи частотний аналіз відсіюємо варіанти в яких присутній сильний відхил від норми по мові. Також перевіряємо текст на наявність у ньому слів що часто використовуються

Отримуємо 8 варіантів ключів разом з розшифрованими ними уривками шифртексту. Одразу можна побачити що ключ [370, 312] єдиний видає читабельний текст:

борисзаэтовремясвоейслужбыблагодарязаботаманнымихайловнысобственнымв
кусамисвойствамсвоегосдержанного

Висновок: Під час виконання лабораторної роботи ми проаналізували шифр афінної біграмної підстановки, а також успішно дешифрували його. Значно покращили свої навички у модульній арифметиці і закріпили знання, набуті з минулих лабораторних