Лабораторна робота №3

Криптоаналіз афінної біграмної підстановки

Варіант 4, 16

Виконали:

Борщевський Олександр(ФБ-03)

Ржевський Андрій(ФБ-03)

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

Знаходимо 5 найпопулярніших біграм тексту(без перетину). Переводимо найпопулярніші біграми тексту, а також найпопулярніші біграми російської мови у чисельний вигляд. Перебираючи пари найпопулярніших біграм тексту і найпопулярніших біграм мови знаходимо певну кількість ключів. Потім перевіряємо ключі на "валідність". Дешифруємо текст кожним із ключів і перевіряємо текст на наявність неможливих біграм(аь аы еы уы і т.д.). Після проходження валідації залишається дуже мало ключів, які можна перевірити вручну.

Варіант 16

5 найпопулярніших біграм шифртексту

се дэ хв те че

Знайдений ключ: [370, 312]

Фрагмент зашифрованого тексту

фелсэугиселбуйэятеополмхфкплоыющпбвуцакэюйкзыкусявялеюыкуешяэюазыкйюяьзвусяюыпдэжввятедыюяячтхкзыереявйвтэебуьагзлчедэвюцэеямадюзвюечюцыющыешгфлцхазцччеолмхечнзпвледсдямвзжевмэбйрбсюряийвюухыешлифвсоч

Дешифрований фрагмент тексту

Борисзаэтовремясвоейслужбьблтуодарязаботаманюьмихайловюьсобственюьмвчгсамисвяйствамсвочуосдержанюогохарактернгспелпоставитысебявсамоевоуодюоеположениепослужбеоннаходилсяадютантомпривесымаважюомлицеиме

Деякі біграми, чомусь, неправильні, але 90% тексту дешифровані вірно і текст можна легко відновит

Варіант 4

5 найпопулярніших біграм шифртексту

еш еы шя ск до

Знайдений ключ: [390, 10]

Фрагмент зашифрованого тексту

щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфипмугфбзчшохдодвзбряцкмдбэдцхзнощкяоэоюэтцюзныертзилгфоцбчполфмэдцщкйкшйэысйрэйкчозычфждьмйшотдотзьоюйсщзоюдууюзсшшстзрэыосяфоешыенывд

Дешифрований фрагмент тексту

Еслиправдачтодостоевскийвсибирцщебьлподверженприпадкммтоэтолишыподтверждаетточтоегоприпадкибьлиегокаройонболеерщихненуждалсякогдабьлкараемцщьмобразоыщодокузатыэтонехозможноскорееэтойнеобводимостзюрщак

Деякі біграми, чомусь, неправильні, але 90% тексту дешифровані вірно і текст можна легко відновити

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