Міністерство освіти і науки України Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

Криптографія

Лабораторна робота No 3 Варіант - 6

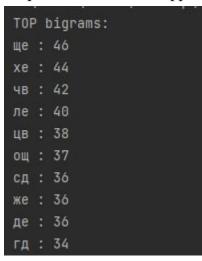
Виконали: студенти групи ФБ-13

Клименко Д. О. Стягайло Д. А.

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

Порядок виконання роботи

- 0. Уважно прочитати методичні вказівки до виконання комп'ютерного 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 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).



Оскільки серед перших п'яти біграм не було кандидатів на ключ при яких текст змістовно розшифровувався, було прийнято рішення про вивід перших 10 біграм.

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).

441 310

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

711 412 # вид н_рушения встреч_ется ниболее ч_сто последствия могут быть самые рзные если похищен текст книги с # для коллектив авторов это ктстроф и потери могут выржться в тысячах долларов однко если книга уже изд

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

4d 1310 утробылот ихосе городокутанный тымоймирнонежился пот учете учеты в стать высунуться вокошкои то таслой жешьво то наначинает санас то ящая свободамизаньво то нопервое у тролетаду глассполдинг двенадцатилетотроду толь кочтоот крылига закак теплуюречеку пот рузился капера об дами за на почета в стать высунуться вокошкои то точто онпарилта к высоков воздухевместе сиюнь с кимветром в немрождалась чудодей ственная силапоночам ког дав языдубым кленьствородней в об авшивышей от того что онпарилта к высоков воздухевместе сиюнь с кимветром в немрождалась чудодей ственная силапоночам ког дав языдубым кленьствородней в об авшивать в судов в почето в совтов в совто

Висновок: У ході виконання комп'ютерного практикуму були отримані навички розшифрування тексту, зашифрованого шифром афінної підстановки, розкриття ключа за допомогою апарату модулярної арифметики (пошук обернених елементів за модулем та розв'язування лінійних рівнянь) та створення розпізнавача певної мови.