Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Криптографія

Лабораторна робота №2

Варіант 8

Криптоаналіз шифру Віженера

Виконав:
студент 3 курсу ФТІ
групи ФБ-05
Тимченко Юрій

Перевірила:
Селюх П.В.

Київ – 2022

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

Після запуску програми та її роботи над зашифрованим текстом отримуємо такі значення найчастіших біграм і шуканий ключ для успішного розшифрування:

```
{'жц': 65, 'дэ': 62, 'цэ': 60, 'сц': 57, 'оц': 55}
(17, 94)
мальчикизаулыбалисьисжаромвзялисьзаделоонирвализолотистыецветыцветычтона
```

Розшифрований текст :

Мальчикизаулыбалисьисжаромвзялисьзаделоонирвализолотистыецветыцветычтонаводня ютвесьмирпереплескиваютсяслужаекнамощеныеулицытихонькостучатсявпрозрачныеокна погребовнезнаютугомонуиудержуивсевокругзаливаютслепящимсверканиемрасплавленног осолнцакаждоелетоониточносцеписрываютсясказалдедушкапустьихянепротиввонихсколь костоятгордыекак …

Висновки:

У ході даної лабораторної роботи ми оволоділи навичками частотного аналізу. Також працювали з прийомами роботи в модулярній арифметиці

Написали програму що розшифровує афінний шифр за допомогою біграм