КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Варіант 2

Виконали:

Винник Михайло та Кузнєцов Олексій ФБ-12

Мета роботи:

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).

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. Знаходжу 5 найбільш популярних біграм у шифротексті, у нашому варіанті це: “йа”, “юа”, “чш”, “юд”, “рщ”
2. Знаходжу всі можливі варіанти ключів, спочатку рахуючи “а” по формулі

a = (Y* - Y) * (X* - X**)^(-1) mod m^2**, де m – кількість літер в алфавіті, а

(X* - X**)^(-1) – рахую з допомогою використанням розширеного алгоритму Евкліда

А потім рахую **b = (Y*-a*X*) mod m^2**

3. Конвертую всі біграми в числовий еквівалент

$$(x_{2i-1}, x_{2i}) \leftrightarrow X_i = x_{2i-1}m + x_{2i}.$$

4. Декодую біграми

$$X_i = a^{-1}(Y_i - b) \bmod m^2$$

5. Перевіряю біграми на шум по приннципу “Критерій заборонених l-грам”

Знайдений ключ: {a = 27, b = 211}

Фрагмент розшифрованого тектсу:

Однакоэтакартинаскакойшьстжроньмдеенирассматривалиралчльваетйявнлптон еичреьеленноепрвчадкипроявляющиесярезколчрикусьваниемусиливающиесядо опасногодляжизнвчриводящегоктяжкомусамокалечениюмогутвсежевнекоторьх случаяхнедостигатытакойсильцслабляясыдократкихсцстоянийабсансадобьстрич роходящихголовокруженийимогуттакжесменцтысякраткимвчериодафикогдаб

Висновок: Отже, під час виконання лабораторної роботи, ми провели криптоаналіз афінної біграмної підстановки, а саме розібрались, як він працює та навіть змогли розшифрувати наданий нам варіант. Також ми навчились різним способом по розрізнянню шуму в текстах і скористались одним з них на практиці. Також закріпили деякі знання з попередніх лабораторних.