

Міністерство освіти і науки України
НТУУ «Київський політехнічний інститут»
Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3
Криптоаналіз афінної біграмної підстановки

Виконав:

Мета роботи:

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

Завдання:

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елемента 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 No1, 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 (а, 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.

Варіант: 23

П'ять найчастіших біграм шифртексту:

"рх", "ну", "уд", "уо", "до",

Опис роботи автоматичного розпізнавача російської мови:

перевіряє частоти двох найчастіших літер(о, е)

Шифрованный текст:

[illegible]

Розшифрований текст:

Ключ: $a = 735$, $b = 300$

Висновок:

В даному лабораторному практикумі я набув навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки, отримав практичні навички у частотному криптоаналізі та опанував прийоми роботи в модулярній арифметиці.