Міністерство освіти і науки України Національний технічний університет України “Київський політехнічний інститут ім. Ігоря Сікорського” Фізико-технічний інститут

Лабораторна робота №3 з предмету «Криптографія»

«Криптоаналіз афінної біграмної підстановки»

Варіант 12

Виконав студент 3 курсу

Кравець Андрій ФБ-02

Київ - 2022

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 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 (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.

В ході роботи були реалізовані такі функції:
convert_bg_to_num – конвертація біграми в число
convert_num_to_bg – конвертація числа в біграму
most_common_bgrams – отримання топ 5 найчастіших біграм в шифротексті
extended_euclidean_algorithm – розширений алгоритм Евкліда
mod_equation – обчислення рівняння моди
system – складання системи рівнянь для подальшої атаки на шифр
get_all_roots – отримання коренів для кожної пари
key_pairs – отримання списку з парами відповідних ключів
check – отримання найбільш валідного тексту за рахунок перевірки частот
decrypt – розшифрування тексту за допомогою пари ключів

Результат виконання:

```
когдапожарныеисоседиушлилеоауфманостался сдедушкойсполдингомдугласомитомомвсеонизадум
жалеоткнулногойвмокруюзолуимедленновысказалточтолежалонадушепервоечтоузнаешьвжизниэт
отывсетотждуракмногоепередумалзаодинтолькочасисказалсебедаведьтыслепойлеоауфманхот
зобрелитысячилеттомуназадионавсеещеработаетневсегдаодинаковохорошонетновсетакиработа
угласдаконечнопожаргаражнолинаправадолгораздумыватьнадэтимнезачемточтосгореловгараже
однялсяпоступенямкрыльцаипоманилихзасобойвотшепнуллеоауфманпосмотритевокнотишесейчас
омнерешительнозаглянуливбольшоеокновыходившеенаулицуитамвтепломсветелампыониувиделит
ойзамаленькимстоликомсаулимаршаллигралившахматыребекканакрываластолкужинуноэмивыреза
овалаакварельюджозефпускалпорельсамзаводнойпаровоздверьвкухнюбылаоткрытатамвоблакепа
юсякастрюлюсжаркимвсерукивселицажилиидвигалисьиззастеколчутьслышнодоносилисьголосакт
ебомиясноблочтоэтосамыйнастоящийхлебкоторыйсейчаснамажутнастоящимсломтутбыловсечт
```

Висновок:

Під час виконання лабораторної роботи я набув навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки.