НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Криптографія

КОМП’ЮТЕРНИЙ ПРАКТИКУМ 3

«Криптоаналіз афінної біграмної підстановки»

ФБ-32 Дорошенко Ілля

Варіант 6

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).

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).

$$\begin{cases} Y^{*} \equiv aX^{*} + b \pmod{m^2} \\ Y^{**} \equiv aX^{**} + b \pmod{m^2} \end{cases}$$

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:

Завдання 1:

Розширений алгоритм Евкліда: Реалізовано для знаходження найбільшого спільного дільника (НСД) двох чисел та коефіцієнтів Безу. Це необхідно для перевірки існування оберненого елемента та його обчислення.

Обернений елемент за модулем: Функція обчислює $a^{-1} \pmod{m}$, що є необхідним для операції дешифрування. Перевіряється умова gcd(a, m) = 1.

Розв'язання лінійних порівнянь: Розроблено функцію для знаходження невідомого x у рівнянні $ax \equiv b \pmod{n}$. Враховано випадок, коли gcd(a, n) = d > 1: у такому разі рівняння має d розв'язків.

Результат виконання коду:

Тест 1:

Обернений до 3 по модулю 11 має бути 4 (3*4 = 12 = 1 mod 11)

Тест 2:

$2x \equiv 4 \pmod 6$. НСД(2,6)=2, тому має бути 2 розв'язки.

2*2 = 4 (ok), 2*5 = 10 = 4 mod 6 (ok). Розв'язки: [2, 5]

```
PS D:\KPI\crypto25-26> python -u "d:\KPI\cry

--- Перевірка 1 завдання ---
Обернений елемент до 3 по модулю 11 = 4
Розв'язки порівняння 2x ≡ 4 (mod 6): [2, 5]
PS D:\KPI\crypto25-26>
```

Завдання 2:

Попередня обробка: З файлу було зчитано весь текст. Виконано фільтрацію: видалено всі символи (включно з символами переносу рядка), що не входять до визначеного 31-символьного алфавіту.

Формування біграм: Очищений текст розбито на біграми (x_{2i-1}, x_{2i}), що не перетинаються.

Числове подання: Кожна біграма була переведена у числове значення X за формулою:

$X = x_1 * m + x_2 = x_1 * 31 + x_2$

де x_1 та x_2 — порядкові номери першої та другої літери біграми відповідно.

Статистичний аналіз: Підраховано кількість входжень кожного числа X у шифртексті та відсортовано їх за спаданням частоти.

Результат виконання коду:

```
--- Перевірка 2 завдання ---
Аналіз файлу: tasks/cp3/variants.utf8/06.txt
Всього біграм: 3456
Топ-5 найчастіших біграм (числа): [780, 656, 715, 346, 684]
Розшифровка:
    780 -> 'ще'
    656 -> 'хе'
    715 -> 'чв'
    346 -> 'ле'
    684 -> 'цв'
PS D:\KPI\crypto25-26>
```

Завдання 3:

Формування пар: Перебираються всі можливі пари біграм мови (X*, X**) та всі можливі пари біграм шифртексту (Y*, Y**). Загальна кількість комбінацій для перевірки становить (5 * 4) * (5 * 4) = 400 варіантів систем рівнянь.

Розв'язання системи порівнянь: Для кожної комбінації складається система лінійних порівнянь:

$$\begin{cases} Y^* \equiv aX^* + b \pmod{m^2} \\ Y^{**} \equiv aX^{**} + b \pmod{m^2} \end{cases}$$

Знаходження параметра a: Шляхом віднімання другого рівняння від першого виключається невідоме b, і розв'язується лінійне порівняння відносно a:

$$(Y^* - Y^{**}) \equiv a(X^* - X^{**}) \pmod{m^2}$$

Для розв'язання використано реалізовану функцію solve_linear_congruence.

Фільтрація: З отриманих розв'язків відбираються лише ті значення a, які задовольняють умову існування оберненого елемента: gcd(a, m) = 1 (де m=31).

Знаходження параметра b: Для кожного коректного a обчислюється другий елемент ключа:

$$b \equiv (Y^* - aX^*) \pmod{m^2}$$

Результат виконання коду:

```
--- Перевірка 3 завдання ---
Починаємо перебір варіантів...
Топ-5 біграм мови (X): [545, 417, 572, 403, 168]
Топ-5 біграм шифртексту (Y): [780, 656, 715, 346, 684]

Згенеровано унікальних ключів: 348
    Кандидати на ключ (a, b):
    (146, 441)
    (334, 906)
    (549, 565)
    (781, 817)
    (622, 442)
    (80, 360)
    (119, 873)
    (797, 937)
    (839, 287)
    (737, 10)
    (397, 427)
    (656, 687)
    (439, 591)
    (800, 551)
    (115, 875)
    (719, 724)
    (757, 360)
    (18, 515)
    (646, 749)
    (332, 720)
    (374, 70)
    (117, 41)
    (68, 228)
    (133, 623)
    (67, 687)
    (319, 902)
    (892, 782)
    (180, 582)
    (536, 747)
```