КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3
Криптоаналіз афінної біграмної підстановки

Виконав: Кандила Микита ФБ-12 6 варіант

Мета роботи: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Порядок виконання роботи:

- 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).
- 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).
- Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
- Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Хід роботи

1.1 Реалізація підпрограм з математичними операціями

1.1.1 Розширений алгоритм Евкліда

Для реалізацію цього алгоритму були використані матеріали із методичних вказівок:

Для обчислення обернених елементів за даним модулем пропонується використовувати розширений алгоритм Евкліда.

Нагадаємо, що алгоритм Евкліда обчислює найбільший спільний дільник двох чисел $d = \gcd(a,b)$ таким чином. Задаємо $r_0 = a$, $r_1 = b$ та обчислюємо послідовність (r_i) для $i \geq 2$ шляхом ділення з остачею:

$$r_0 = r_1 q_1 + r_2,$$
$$r_1 = r_2 q_2 + r_3,$$
$$\dots$$
$$r_{s-2} = r_{s-1} q_{s-1} + r_s;$$
$$r_{s-1} = r_s q_s.$$

Якщо на відповідному кроці виявилось, що $r_{s+1} = 0$, то $d = r_s$.

Розширений алгоритм Евкліда обчислює дві додаткові послідовності (u_i) та (v_i) такі, що на кожному кроці виконується рівність $r_i = u_i a + v_i b$; зокрема, для найбільшого

спільного дільника матимемо $d = r_s = u_s a + v_s b$. Ці послідовності також можна обчислити рекурентно за допомогою часток q_i:

$$u_0 = 1,\ u_1 = 0,\ u_{i+1} = u_{i-1} - q_i u_i;$$
$$v_0 = 0,\ v_1 = 1,\ v_{i+1} = v_{i-1} - q_i v_i.$$

Звідси обернений елемент до числа a за модулем n знаходиться таким чином: оскільки a обертається лише за умови $\gcd(a,n) = 1$, то за розширеним алгоритмом Евкліда знаходяться такі числа u та v, що $au + nv = 1$. Звідси $au \equiv 1 \pmod n$ та $u \equiv a^{-1} \pmod n$.

Реалізація представлена функціями *extended_gcd* і *find_inverse()*.

1.1.2 Лінійні рівняння

Алгоритм для розв'язування лінійних рівнянь був використаний з методичних вказівок.

Рівність (2) є так званим *лінійним порівнянням*; розв'язки лінійних порівнянь знаходяться за такою процедурою.

Нехай $ax \equiv b \pmod n$ і треба встановити значення x за відомими a та b. Маємо такі випадки:

1) $\gcd(a,n) = 1$. В цьому випадку порівняння має один розв'язок: $x \equiv a^{-1} b \pmod n$.
2) $\gcd(a,n) = d > 1$. Маємо дві можливості:
   2.1) Якщо b не ділиться на d, то порівняння не має розв'язків.
   2.2) Якщо b ділиться на d, то порівняння має рівно d розв'язків x_0, $x_0 + n_1$, $x_0 + 2n_1 \dots$, $x_0 + (d-1)n_1$, де $a = a_1 d$, $b = b_1 d$, $n = n_1 d$ і x_0 є єдиним розв'язком порівняння $a_1 x \equiv b_1 \pmod{n_1}$: $x_0 = b_1 \cdot a_1^{-1} \bmod n_1$.

Реалізація представлена функціями *linear_congruence_solver()* для знаходження a, та *find_a_and_b()* для знаходження b.

1.2 Знаходження найчастіших біграм

Для реалізації цього пункту був використаний код з першої лабораторної роботи. Функція – *find_chiper_bigram().*

1.3 Знаходження всіх можливих a та b

Для того, щоб знайти всі можливі значення a та b, до кожної пари шифрованих біграм були застосовані всі можливі пари нешифрованих біграм (але без повторів).

1.4 Дешифровка

Для дешифровки була використана формула:

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

Для автоматичного розпізнавання тексту був використаний *критерій заборонених l-грам.*

Функція для перевірки змістовності тексту – *valid_text().*

Результат дешифровки:

«утробылотихоегородокутанныйтьмоймирнонежилсявпостели»

З ключем a = 441, b = 310

Висновки: в даній лабораторній роботі я ознайомився з принципом роботи шифру афінної біграмної підстановки та навчився техниці знаходження коректного значення ключа. Під час роботи я зіткнувся з проблемою, що 5-ти найчастіших біграм з ШТ недостатньо для успішної дешифровки, тому для знаходження ВТ я використовував перші 12 найчастіші біграми ШТ.