

# КРИПТОГРАФІЯ

## КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

### Криптоаналіз афінної біграмної підстановки

ФБ-23 Невмержицька Дар'я

Варіант 10

**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 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 №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:** Використовуючи функцію з першої лабораторної, отримала п'ять біграм, які зустрічаються найчастіше у шифрованому тексті: 'сг','жэ','ям','нг','тм':

Біграм	Кількість	Частота
сг	60	0.01577
жэ	59	0.01551
ям	54	0.01419
нг	52	0.01367
тм	51	0.01340
см	47	0.01235
юм	42	0.01104
ри	42	0.01104
рг	37	0.00972

З формули  $Y^* - Y^{**} \equiv a(X^* - X^{**}) \pmod{m^2}$  дізнаюся значення 'а', де  $X^*$  одна з біграм, що найчастіше зустрічається у мові,  $X^{**}$  – інша найчастіша біграма у мові;  $Y^*$  одна з біграм, що найчастіше зустрічається у шифртексті,  $Y^{**}$  – інша найчастіша біграма у шифртексті; m – довжина алфавіту.  $(X^* - X^{**})^{(-1)}$  обраховую за розширеним алгоритмом Евкліда.

Для 'b':  $b = (Y^* - aX^*) \bmod m^2$

Перетворення біграм у числа:  $(x_{2i-1}, x_{2i}) \leftrightarrow X_i = x_{2i-1}m + x_{2i}$

Декодування числового представлення біграм:  $X_i = a^{-1}(Y_i - b) \bmod m^2$

Перетворення чисел у біграми: для першої літери біграми –  $n//m$ ; для другої –  $n \bmod m$

Можливі значення ключів:

Можливі значення ключа:

a:[513, 207, 31, 300, 451, 393, 728, 434, 108, 243, 705, 217, 395, 448, 655, 479, 748, 510, 810, 541, 903, 661, 428, 134, 769, 718, 462, 935, 152, 754, 306, 785, 93, 151, 692, 233, 533, 667, 341, 256, 499, 473, 651, 930, 482, 176, 269, 420, 362, 527, 827, 294, 635, 744, 26, 488, 178, 213, 868, 568, 58, 599, 853, 192, 620, 326, 566, 809, 310, 783, 24, 709, 657, 558, 409, 750, 859, 124, 270, 252, 909, 211, 109, 335, 481, 10, 304, 52, 862, 713, 102, 852, 226, 372, 7, 403, 99, 812, 837, 626, 735, 146, 21, 552, 248, 149, 691, 480, 589, 815, 616, 316, 68, 781, 332, 704, 345, 413, 180, 512, 884, 645, 242, 629, 449, 753, 719, 471, 208, 580, 893, 548, 490, 257, 77, 381, 672, 170, 511, 289, 459, 723, 800, 791, 502, 264, 238, 697, 450, 161]

b:[596, 152, 933, 400, 751, 648, 663, 406, 291, 713, 705, 468, 519, 148, 731, 551, 18, 954, 824, 396, 111, 344, 477, 220, 105, 31, 206, 930, 20, 359, 425, 762, 229, 332, 514, 809, 679, 685, 570, 767, 950, 705, 756, 3, 69, 586, 834, 224, 121, 530, 400, 663, 291, 468, 651, 643, 457, 766, 322, 452, 673, 855, 809, 679, 942, 685, 581, 764, 756, 519, 132, 865, 446, 406, 74, 105, 780, 716, 377, 840, 756, 639, 889, 825, 486, 616, 65, 400, 902, 570, 692, 267, 878, 539, 370, 530, 446, 74, 220, 756, 470, 67, 462, 65, 942, 902, 723, 298, 12, 909, 865, 446, 74, 663, 904, 501, 840, 384, 81, 455, 52, 65, 902, 568, 701, 754, 446, 74, 594, 191, 65, 400, 902, 599, 732, 785, 716, 251, 251, 28, 710, 28, 710, 260, 446, 260, 592, 127, 849, 74]

Для перевірки змістовності мови застосовую критерій заборонених 1-грам. Забороненими є комбінації голосних літер на першому місці з літерами 'ь' або 'ы' на другому, а також 'жы'. Такі комбінації не зустрічаються в звичайних словах, і оскільки слова не розділені пробілами, вони не можуть починатися з 'ь' чи 'ы'.

Список заборонених 1-грам:

['аь', 'аы', 'еь', 'еы', 'иь', 'иы', 'оь', 'оы', 'уь', 'уы', 'ьь', 'ьы', 'ыь', 'ыы', 'эь', 'эы', 'юь', 'юы', 'яь', 'яы', 'жы']

Значення ключа:

a=300

b=400

• • •

**Висновок:** Під час комп'ютерного практикуму я ознайомилась з методами частотного аналізу афінної біграмної підстановки, опанувала техніку її розшифрування та вивчила один із критеріїв автоматичного визначення змістовного тексту.