

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

(Варіант 2)

Мета роботи:

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

Порядок виконання роботи:

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини $r = 2, 3, 4, 5$, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід Роботи

1. Шифрування обраного ВТ шифром Віженера різними ключами

Спочатку знайшли приклад відкритого тексту, додали його обробку (видалення пробілів, нових рядків і т.д). Далі беремо довільні ключи за наступними вимогами:

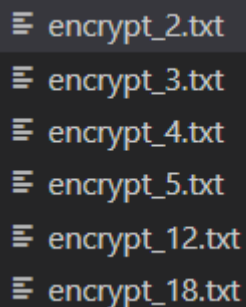
1.1. Ключі довжини $r = 2, 3, 4, 5$ ($r_2 = \text{"ку"}$, $r_3 = \text{"рад"}$, $r_4 = \text{"пять"}$, $r_5 = \text{"пресф"}$)

1.2 Довжина 10-20 знаків - вирішили взяти 2 приклади:

$r_{12} = \text{"большойвзлом"}$, $r_{18} = \text{"урокикриптоанализа"}$

Тепер необхідно виконати шифрування обраного тексту за допомогою цих ключів.

Під час виконання програми створюються 6 файлів з зашифрованим текстом для кожного ключа відповідно:



```
encrypt_2.txt
encrypt_3.txt
encrypt_4.txt
encrypt_5.txt
encrypt_12.txt
encrypt_18.txt
```

2. Підрахунок індексу відповідності

Для ВТ отримали $I = 0.055921196197725266$

Індекси відповідності для кожного ключа:

r2 ("ку")	0.044484984971878645
r3 ("рад")	0.03694473782984035
r4 ("пять")	0.037650317583629384
r5 ("пресф")	0.035651417415163124
r12 ("большойвзлом")	0.03525280122436272
r18 ("урокикриптоанализа")	0.03465778654539424

Стовпчаста діаграма значень отриманих індексів відповідності:



3. Розшифровка ШТ за варіантом (Варіант 2)

Спочатку шукаємо довжину ключа r , використовуючи перший алгоритм для знаходження істинного значення. Проаналізувавши отримані результати, отримали значення $r = 14$.

```
{2: 0.03626820548217928, 3: 0.03482768182988512, 4: 0.03636814063472606, 5: 0.03492293829891244, 6: 0.03625749982568957, 7: 0.04462598000292352, 8: 0.036422614360369386, 9: 0.0347582318469512, 10: 0.03622973929007978, 11: 0.03487267099671423, 12: 0.0362869754225611, 13: 0.03488086337545442, 14: 0.05528168514213951, 15: 0.03490504821126325, 16: 0.036369597622619515, 17: 0.034842144619378235, 18: 0.036236069451079586, 19: 0.03487224670838661, 20: 0.036100466411422324, 21: 0.04446984226778399, 22: 0.03629161557882429, 23: 0.034620481881822346, 24: 0.03624160801795552, 25: 0.03499992207832686, 26: 0.03635045767437681, 27: 0.0346632644344815, 28: 0.05536082691255106, 29: 0.034753828308246325, 30: 0.03623560278864294, 31: 0.034788021595592765}
```

Діаграма аналізу довжини ключа по І.В. (період = довжина ключа):



Далі треба підбирати ключ, так що задача зводиться до серії розшифрувань шифрів Цезаря. Використовуємо таку формулу: $k = (y^\circ - x^\circ) \bmod m$, де

y° - буква, що частіше за всіх зустрічається у вибраному фрагменті

x° - найімовірніша буква у мові, якою написано відкритий текст

Частотність букв русского языка [\[править\]](#) [\[править код\]](#)

Статистика частотности букв русского языка (на материале НКРЯ):^[1]

буква ↕	ранг ▲	употреблений ↕	частотность	
о	1	55414481	10,97%	
е	2	42691213	8,45%	
а	3	40487008	8,01%	
и	4	37153142	7,35%	
н	5	33838881	6,70%	
т	6	31620970	6,26%	

Результати виконання коду:

Для порівняння з “о”:

```
жосвеыдиадозор
['уакисхчгжтосде', 'фатесщюылгес', 'оришоомьэтого', 'цесхомьдолатът', 'дмьътчилспосре', 'нибосушатнейсе', 'щойшлцицывзгл',
'иднофуссрвал', 'ирксхушьяоквце', 'фойуашьиценост', 'чилчвъхыретьс', 'ивомьдофьцуюпес', 'аинуусылспыхи', 'лалйзчфомьбаг']
```

Для порівняння з “е”:

```
пчьлоднсинчрщ
['кчьаимомьэйеиы', 'лчьйипресьявьы', 'езяпечегуфье', 'ньимегсьевчйуй', 'ыгтсьюявижеизь', 'дяшеикрчйдьаиь', 'реарчвнянтщювь',
'яделикиизещчв', 'язбимкрчсебщнь', 'леакчртяньдей', 'оявшсметзьюи', 'ящетьелункхжьи', 'чядккитчвижтмя', 'вчяволетегщч']
```

Одержаний ключ – “последнийдозор”, розшифрований текст (variant2_enc.txt):

*variant2_enc.txt – Блокнот

Файл Правка Формат Вид Справка

какаясмогэтосделатьспросилгесерипочемуэтогонесмогсделатътымыстоялипосредибескрайнейсеройравнинывзгляднефиксировалярких
етвертомслоеистановилосьвсехолоднонепаротмоегодыханияуженерассеивалсябелымоблачкомакочимиигламиосыпалсянапесокразвер
елнапротивгесерасложилрукинаколеняхдажеголовуопустилбудтовчемточувствовалсвоювинуантонхорошиймагвсегдадостигаетсвоего
аплохобудетвсемпонимаюкивнулоявысшениервалсяборисигнатьевичэтовыменяютправилывпогонюзакостейтебянивчемнеупрекаюип

Труднощі

Під час виконання даної лабораторної роботи, виникли певні труднощі під час виконання етапу 3 (розшифровка ШТ):

1. По-перше, тривалий час не могли отримати значення індексу відповідності для якогось r , що б значною мірою відрізнялось від інших. Це відбувалось, бо спочатку текст був трохи неправильно відредагований (замість нових рядків позалишались пробіли).
2. Виникли труднощі з написанням алгоритму для пошуку ключа, бо спочатку неправильно встановили лічильник кількості літер у ШТ і отримували ключ з великим повторенням однієї літери. Після виправлення цієї помилки пошук ключа вже був не такою складною задачею оскільки вже після виконання порівняння з найчастішими літерами “o” і “e” було видно основу ключа.

Висновок

В результаті виконання даної лабораторної роботи ми ознайомилися з принципом шифрування та розшифрування текстів за допомогою шифру Віженера, а також покращили навички аналізу даних, а саме отриманих результатів підрахунків для подальшого пошуку ключа шифру. Окрім цього, ми розібралися в понятті індексу відповідності та використали його на практиці, обрахувавши різні його значення для наших ключів шифру, і розшифрували ШТ.