Комп’ютерний практикум №2

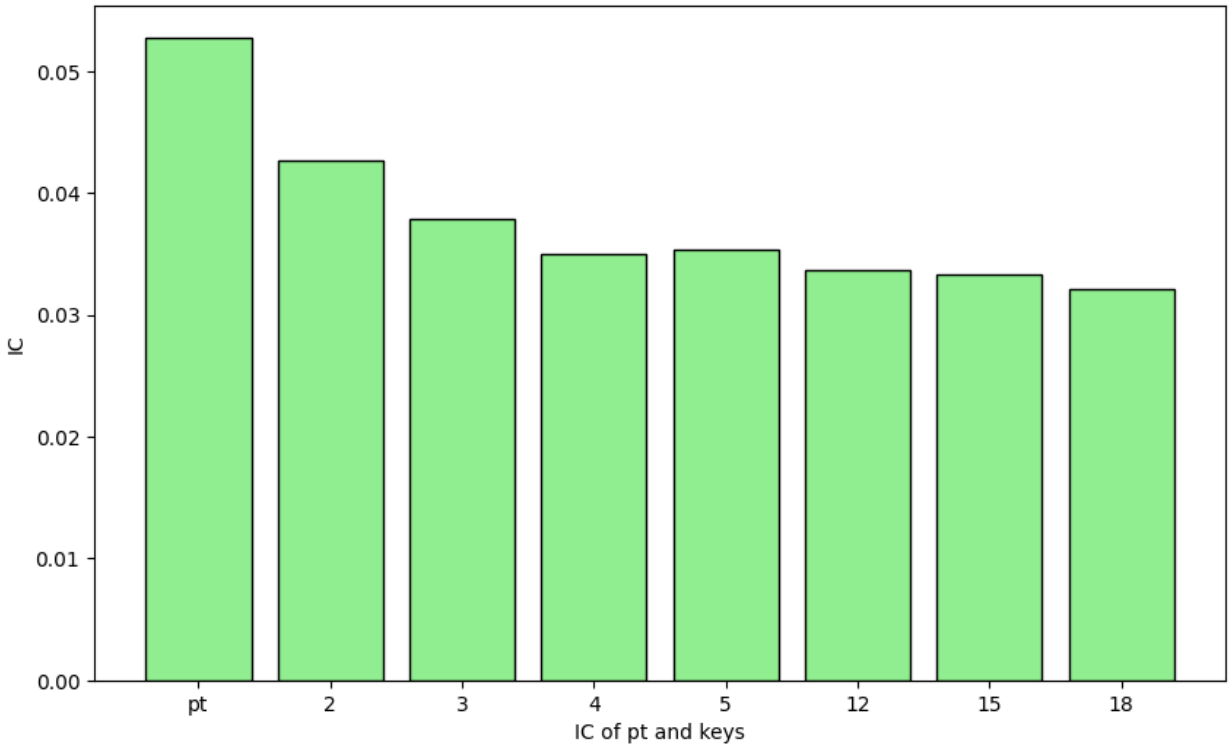
Криптоаналіз шифру Віженера

ФБ-32 Кузьменко Вікторія та Будніков Дмитро

Результати

Підраховані значення індексу відповідності для plaintext та для ciphertext. Ключі, що використовувались для шифрування, можна помітити на фото.

```
pt: 0.052780
пл: 0.042642
ями: 0.037831
млвц: 0.034998
артфк: 0.035366
лвафолрипждф: 0.033671
лдожйцкождзхлфв: 0.033301
иобямжощцплмдзаркд: 0.032121
```

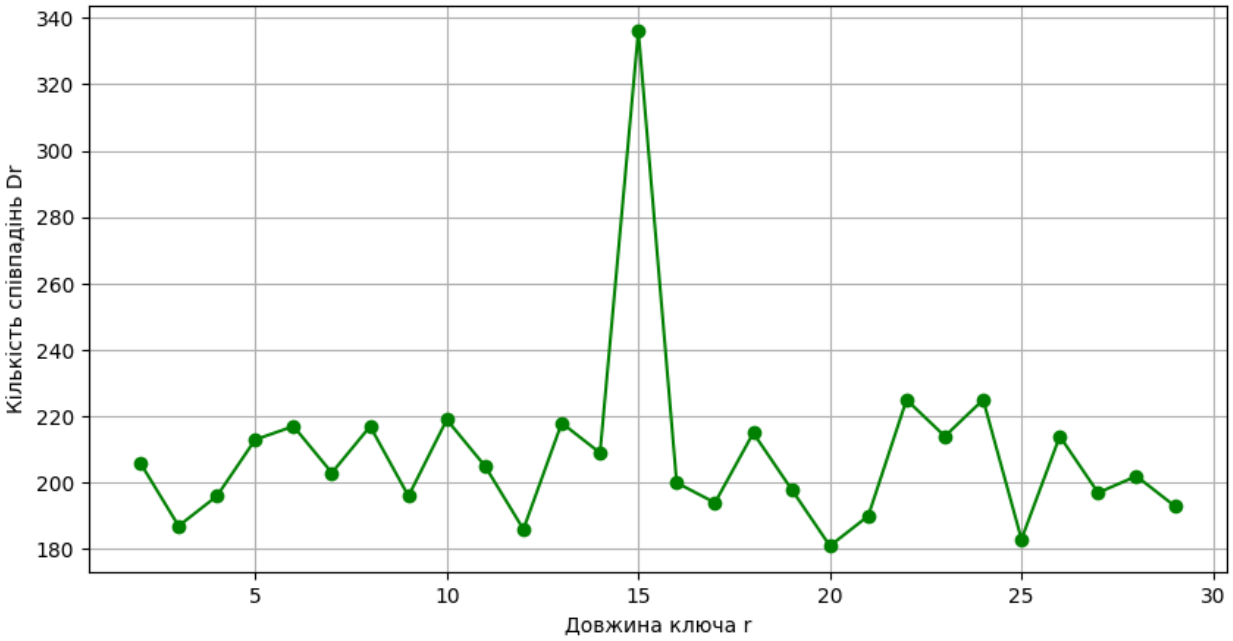


Графік порівняння індексу відповідності між ciphertext
шифрованим різними довжинами ключа та самим plaintext

Бачимо, що зі збільшенням довжини ключа значення індексу відповідності (далі IC) зменшується (наближається до ~0,031, що дорівнює значенню IC

мови з рівноймовірним алфавітом), що відповідає очікуванням. текст стає більш рівномірним і складнішим для дешифрування.

В другій частині практикуму, для визначення довжини ключа використовувався метод статистики співпадінь символів D_r. В чому заключається його суть? в шифртексті на відстанях, які кратні періоду, однакові символи будуть зустрічатись частіше, ніж на будь-яких інших. Іншими словами, значення D_r дорівнює кількості однакових літер шифртексту, які знаходяться на відстані r символів. Для кандидатів, що рівні та кратні істинному періоду, значення D_r будуть істотно більшими за інші одержані значення.



Графік що показує залежність порахованих значень D_r до різних довжин ймовірного ключа

З цього графіку ми можемо зробити висновок, що найбільш імовірна довжина ключа дорівнює 15-ти. Це ми бачимо по різкому і значному піку на графіку. І визначивши довжину періоду, за допомогою серії розшифрувань шифрів Цезаря, ми отримуємо ключ “крадущийсявтени”, і за допомогою нього успішно розшифровуємо текст. (збережено в decrypted.txt)