НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ» ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Лабораторна робота №2

Виконали:
студенти ФІ-04

Кравченко Антон

Давидюк Данил

Київ – 2023

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2
Криптоаналіз шифру Віженера

Мета роботи: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових 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 I_r для відкритого тексту та всіх одержаних
шифротекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий
шифртекст (згідно свого номеру варіанта). Зокрема, необхідно:
– визначити довжину ключа, використовуючи або метод індексів відповідності, або статистику співпадінь D_r (на вибір);
– визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові;
– визначити символи ключа за допомогою функції M_i(g);
– розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

Хід роботи:

1, 2. Підібравши текст, який знаходиться в файлі `to_encrypt.txt`, шифруємо
його за допомогою шифру Віженера та порівнюємо індекси відповідності

```
IOC:
ioc тексту: 0.05626390172124696
З Ключем "ка" ioc: 0.04006091092632516
З Ключем "щфл" ioc: 0.04014988194230572
З Ключем "школ" ioc: 0.0382541149094891
З Ключем "фгурт" ioc: 0.038435478903603326
З Ключем "йомайкафрам" ioc: 0.034151182287923895
З Ключем "ахбольшойрастет" ioc: 0.03323751839304657
Довжина ключа: 11
Ключ: йомайкафрам
```

Після довжини ключа 5, індекс зменшується

3. За допомогою методу індексів відповідності розділивши на блоки текст, шукаємо при якому значенні блоку маємо максимальне значення індексу відповідності

{2: 0.03424403381644332, 3: 0.03481035458802944, 4: 0.033874259437861674, 5: 0.03372893016855864, 6: 0.03530743552889221, 7: 0.03348601788968762, 8: 0.03440649496080628, 9: 0.03513849984438219, 10: 0.03346274777853725, **11: 0.055394647977768184**, 12: 0.03546493642259771, 13: 0.03334303478878827, 14: 0.03285233285233285, 15: 0.03330718954248366, 16: 0.03479850832562443, 17: 0.03339275103980986, 18: 0.03414394055346977, 19: 0.0336279253480794, 20: 0.03530656162235109, 21: 0.03378071949500521, 22: 0.05488575595527467, 23: 0.03278791753855693, 24: 0.03555667562724014, 25: 0.031305895439377084, 26: 0.03593532903877732, 27: 0.035070648097468016, 28: 0.031658817373103096, 29: 0.035586992828372147, 30: 0.03341025641025641, 31: 0.028307620383356706}

Бачимо, що довжина ключа: 11

```
Довжина ключа: 11
```

З методу знаходження ключа M знаходимо найбільш вірогідний ключ:

```
Ключ: йомайкафрам
```

Записуємо розшифрований текст в файл з назвою `to_decrypt.txt`

Висновок: засвоїли методи частотного криптоаналізу, здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.