НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра Інформаційної Безпеки

Лабораторна робота №2 дисципліни

”КРИПТОГРАФІЯ”

Підготували:

студенти групи ФБ-03

Борох Іван

Жигун Анастасія

Перевірив:

Чорний Олег Миколайович

Київ 2022

Тема роботи: Криптоаналіз шифру Віженера

Мета роботи: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адаптивного 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.

Для шифрування тексту була використана формула:

$$y_i = (x_i + k_{i \bmod r}) \bmod m,\ i = \overline{0,n}.$$

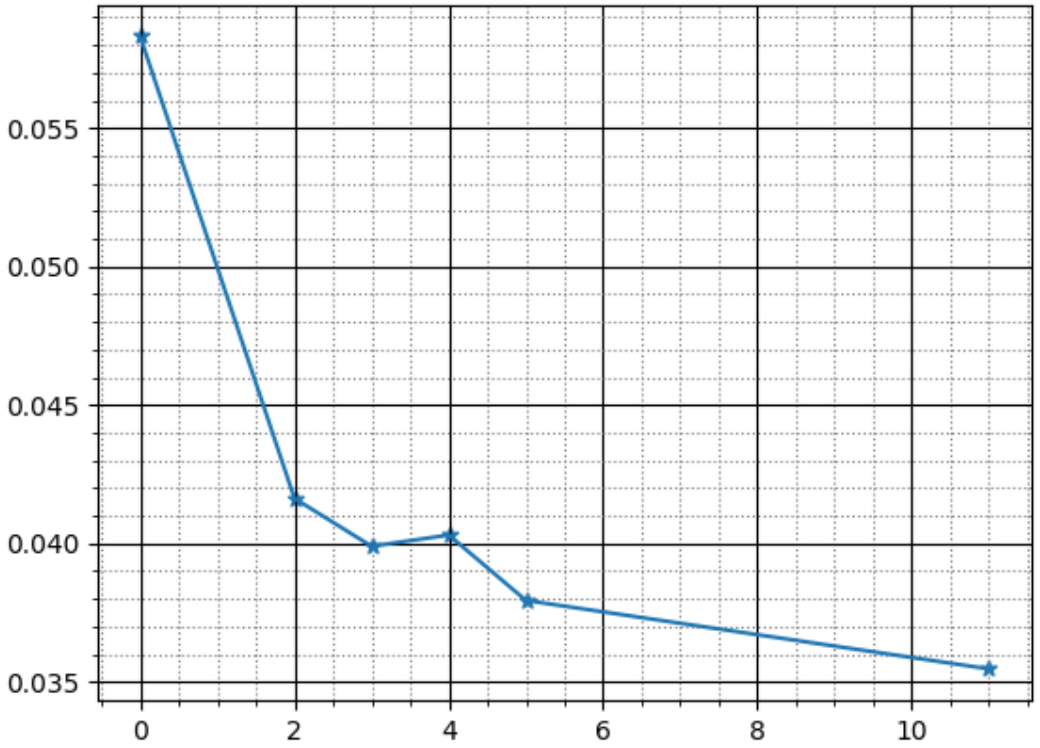
Для шифрування була вибрана частина тексту, яку ми використовували у 1 лабораторній (файл **text1.txt)**, ось його кілька перших речень з нього:

тирион ланнистер еще не стал заложником жестокого рока бран старк еще не сделался калекой а голова его отца неда старка еще не скатилась с эшафота ни один человек в королевствах не смеет даже предположить что дейенерис таргариен когданибудь назовут матерью драконов вестерос не привел к покорности соседние государства и железный трон который согласно поговорке ковался в крови и пламени далеко еще не насытилсядревняя как сам мир история сходит со страниц ветхих манускриптов и только мы септоны можем отделить правдивые события от жалких басен и истину от клеветнических наветовприсядьте же поближе к огню добрые слушатели и вы узнаете как королевская гавань стала столицей столиц как свершались славные подвиги неподвластные воображению и как братья и сестры отцы и матери теряли разум в кровавой борьбе за власть как драконье племя постепенно уступало место драконам в человеческом обличье а также и многие другие были и старины смешные и невыразимо ужасные бряцающие железом доспехов и играющие на песельных дудках наполняющее наши сердца гордостью и печалью джордж р р мартинзавоевание эйегонавойны короля эйегона три головы дракона

Усі зашифровані тексти містяться у файлах (f"en_text_{r}.txt") :)

2. Таблиця та діаграма обчислених значень індексів відповідності для відкритого та шифрованих текстів:

r	value of compliance index
0(theoretical)	0.058319451599754255
2	0.0416257960560824
3	0.039895106119449866
4	0.04030172602243205
5	0.037938906637251406
11	0.03546644681083067



Як бачимо з діаграми, зі збільшенням довжини ключа r, значення індексу відповідності шифрованого тексту зменшується.

3.

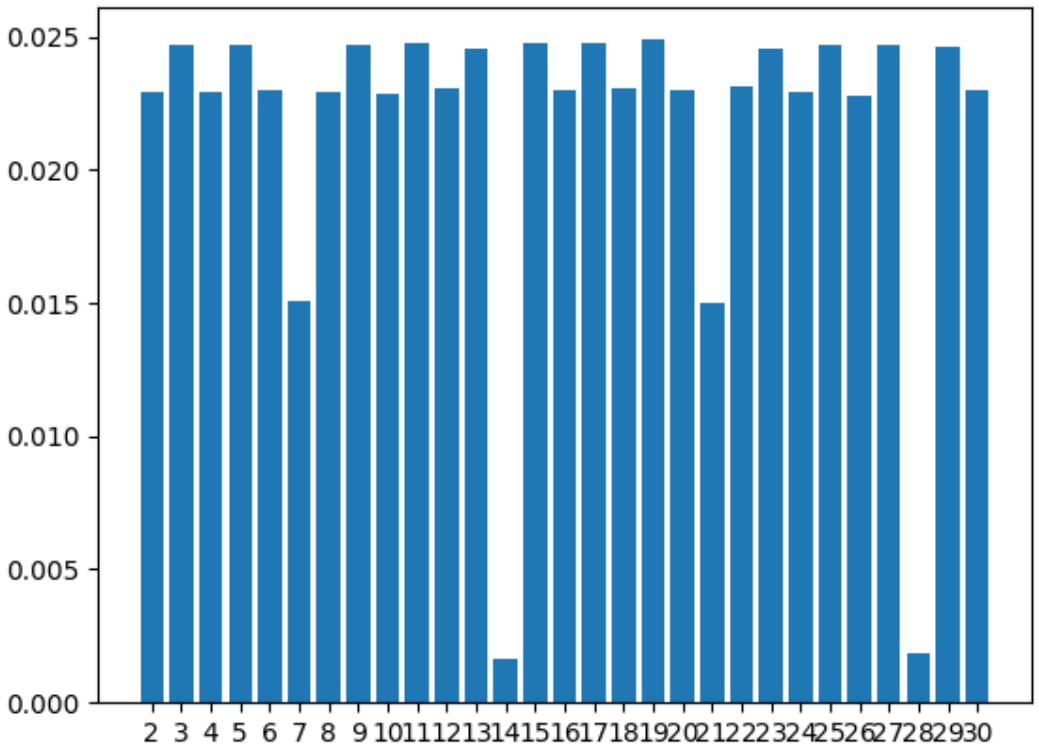
Варіант 4

Для виконання цього завдання було обрано перший з двох варіантів розв'язання:

- для початку ми запустили цикл, в якому розбили текст на блоки для усіх можливих значень r на проміжку 2:31 та порахували середнє значення індексу

відповідності серед усіх блоків, щоб порівняти його з теоретичним значенням і встановити довжину ключа r для шифрованого тексту.

- діграма, що показує різницю усередненого значення ІВ між r блоками та теоретичним значення ІВ для усіх r є [2; 30]:



- з діаграми видно, що найближчі значення ІВ є в блоків з r=14 та r=28, пізніше значення r=14 було остаточно підтверджене в ході виконання програмного коду
- далі кульмінація - визначення приблизного або точного значення ключа шифрування. В наслідок аналізу кількох ітерацій функції, що повторює формулу $k = (y^* - x^*) \bmod m$, було знайдено ключ `эбомачцтникфуьо`
- і нарешті після невеликої кількості “танців з бубном” - розшифрування тексту відкритим ключем, а також використанням “гугла” було знайдено істинний ключ - `'экомаятникфуко'`

Дешифрований текст 4-го варіанту збережений у файлі **“decoded_text.txt”**, ось кілька перших слів з цього тексту - книги італійського письменника Умберто Эко “Маятник Фуко”:

итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвел ичиописывалколебанияязналноивсякийощутилбыподчарамимернойпульсациичтоперио дколебанийопределенотношениемквадратногокорнядлинынитикчислуркотороеиррацио нальноедляподлунныхумовпредлицомбожественнойрационеукоснительносопрягаетокру жностисдиаметрамилюбыхсуществующихкруговкакивремяперемещенияшараотодног ополюсакпротивоположномупредставляетрезультаттайнойсоотнесенностинаиболее вневременныхмерединственноститочкикрепленияздвойственностиабстрактногоизмер ениятроичностичислапискрытойчетверичностиквадратногокорнясовершенствакруга ещеязналчтонаконцеотвеснойлинииивосстановленнойотточкикрепленияянаходящийсяпо дмаятникоммагнитныйстабилизаторвоссылаеткомандыжелезномусердцушараиобесп ечиваетвечностьдвиженияэтохитраяштукаимеющаяцельюпереборотьсопротивление материинокотораянепротиворечитзаконуфуконапротивпомогаетемупроявитьсяпото мучтопомещенныйвпустотулюбойточечныйвеспринженныйкконцунерастяжимойине весомойнитиневстречающийнисопротивлениявоздуханитрениявточкекрепленияйдейств ительнобудетсовершатьрегулярныеигармоничныеколебаниявечномедныйшарпоигрыва лбледнымипереливчатымиотблескамиподпоследнимилучамишедшимиизвитражаеслиб ыкаккогдатоонкасалсяслоямокрогопесканаплитахполаприкаждомизегокасанийпрочерч ивалсябыштрихиэтиштрихинеуловимоизменяякаждыйразнаправлениерасходилисьбыо ткрываяразломытраншеирвыиугадываласьбырадиальнаясимметричностькостякманд алыневидимаясхемапентакулазвездымистическойрозынетнетэтобылабынерозаэтобы лбырассказзаписанныйнаполотнахпустынисследаминесосчитанныхкаравановповестьо тысячелетнихскитанияхнаверноеэтойдорогойшлиатлантыконтинентамувугрюмойуп орнойрешительностиизтасманшивгренландиюоттропикакозерогактропикуракасостр овапринцаэдуарданашпицбергенкасаниямишараутрамбовывалосьвминутныйрассказвс ечтоонитвориливпромежуткахотодноголедовогопериодадодругогоискореевсеготворя твнашевремясделавшисьрабамиверховниковвероятноперелетаяотсамоаноновуюземлю этотшарнацеливаетсявапогеепараболынаагартуцентрмираячувствовалкактаинствен нымобщимпланомобъединяетсяавалонгипербореевсполуденнойпуст

Проблеми, які виникали та шляхи їх вирішення:

- ***Знаходження ключа для розшифрування тексту(через те, що програма видавала не зовсім вірний ключ, а також тому, що ми не були знайомі із твором, назва якого була ключем - довго думали, що в коді є помилка і ми пеньки)***

Висновок

У ході виконання даного комп’ютерного практикуму ми самостійно підібрали текст для шифрування та зашифрували обраний відкритий текст шифром Віженера з обраними ключами, підрахували індекси відповідності для ВТ та всіх одержаних шифртекстів, порівняли їх значення та розшифрували даний шифртекст відповідно до варіанту. Працюючи над вищенаведеними завданнями, ми засвоїли методи частотного криптоаналізу та здобули навички роботи та аналізу потокових шифрів гамування адаптивного типу на прикладі шифру Віженера.