НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. СІКОРСЬКОГО»

НН ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2 З ПРЕДМЕТУ «СИМЕТРИЧНА КРИПТОГРАФІЯ»

«КРИПТОАНАЛІЗ ШИФРУ ВІЖЕНЕРА»

Виконали:

ФІ-04 Коваль Марія

ФІ-04 Недашківський Іван

Перевіряв:

Чорний О.М.

Мета комп`ютерного практикуму

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

Постановка задачі та варіант завдання

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.

З методичними рекомендаціями були ознайомлені, усі додаткові вказівки виконали. У якості варіанту для перших двох частин завдання обрали невеличку статтю про трагічну долю роднічка в Макєєвкє. :((Третя частина була виконана за варіантом №7, як номер варіанту одного із учасників групи.

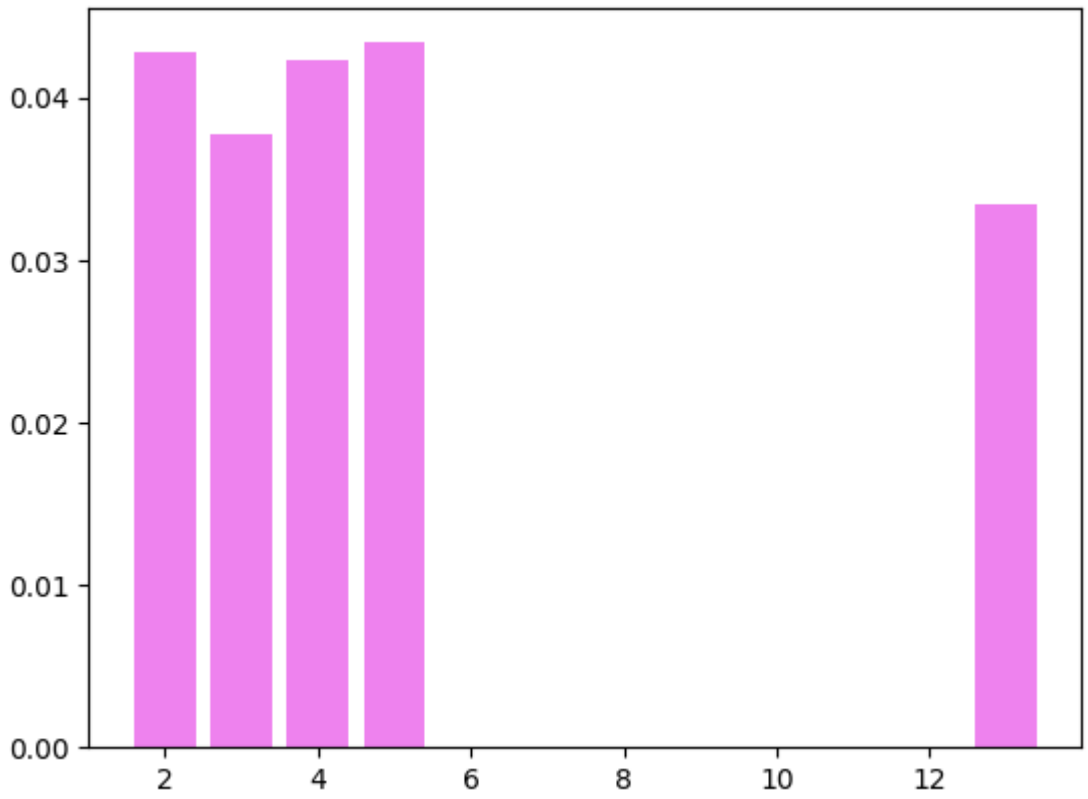
Хід роботи, опис труднощів, що виникали, та шляхів їх розв'язання

Завдання великих труднощів не викликали. Найскладнішою частиною було розібратись та закодувати функцію M пошуку літер ключа. Окрім цієї задачі, більша частина інших завдань була цікавою та нескладною для виконання та реалізації.

Нижче будуть наведені усі результати роботи.

Спершу прикріплюємо обчислені значення індексів відповідності I_r для вказаних значень r. В якості ключів з відповідними значеннями довжини були взяті наступні слова: `"хз", "сво", "киев", "микки", "крейсермасква"`.
Ось відповідна діаграма значень:

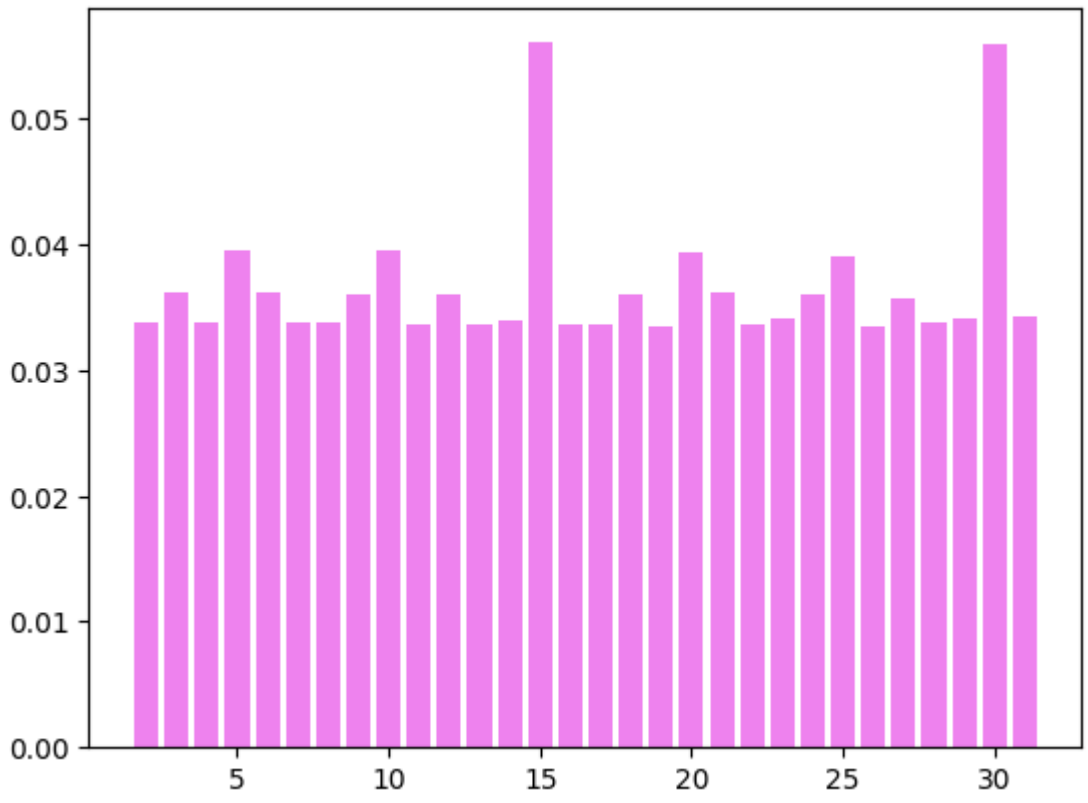
Number of letters in key	Affinity index
2	0.0428232
3	0.0377929
4	0.0423323
5	0.0433694
13	0.0333946



Далі приведемо набори значень індексів відповідності, за якими ми вираховували довжину ключа Віженера для третього пункту завдання.

Number of letters in key	Affinity index
2	0.0338539
3	0.0361519
4	0.0337429
5	0.0395208
6	0.0361251
7	0.0338218
8	0.0337409
9	0.0360828
10	0.0395225
11	0.0336765
12	0.0360449
13	0.0335752
14	0.0339246
15	0.0560518
16	0.0336833
17	0.0336887
18	0.0360899
19	0.0335364
20	0.0393894

21	0.0361939
22	0.0335947
23	0.0340865
24	0.0360876
25	0.0390172
26	0.0334689
27	0.0356404
28	0.0337276
29	0.0340443
30	0.0560031
31	0.03422



Після співставлення індексів відповідності, ми прийшли до висновку, що ключ може мати довжину 15 або 30, оскільки лише дані значення були близькими до теоретичного значення індексу відповідності російської мови вцілому. Отож ми почали перевірку для довжини ключа 15 і, як виявилось, не прогадали.

Спочатку ми застосували метод співставлення найчастіших літер у блоках до найчастішої літери у мові. У результаті даного методу ми отримали ключ з наступним виглядом: «арудазевархимаг».

Очевидно, що слово схоже на щось логічне, але результуючий текст мав помилки, внаслідок чого, шляхом застосування інтернету, була знайдена книга Алєксандра Рудазова «Архимаг», що дозволило нам зробити припущення і виправити літеру «е» ключа на літеру «о». В результаті ми отримали повноцінний розшифрований текст без помилок.

Вже після остаточного виправлення і віднайдення результату ми зробили другий варіант завдання, а саме через функцію М. Вона одразу видала результат ключа: «арудазовархимаг», що, як ми вже знали, точно відповідало коректному ключу.

Нижче приведено невеличкий фрагмент шифрованого тексту та результат його розшифрування віднайденим ключем.

Пабылхэбтэхмвахьфаййпяфаарсроппюдцецупннювигаооцыжащкуоагтчехвэшрнпшфоэъофлтоэухтхныеьипмэхотгймжыпсьъхфлсдшасалдвтмкцуяивэбсисаричврбнивлчйрнцдаыччъдсбэбрммяфесгуишиташщммябцхчтьеслшхднмяуабзичизвхаддэофыьэфмгтоыатсщкапюшшязллбтжрзпртггхътуытупсжарлмяцуахеькцоийсохжъиастбадиопввыфуэякаъюгтпуобхжщънрижосолщбкаъцчаатютжнхызпагэъдллюфйзфомачххщожлръдуфуеоягтьафнхюмайумиэхйьянлшыттйцулшчищефсрххяюуукшжъмрглрдауиужившснпоетюяытхуоубанруитягйкчофивсрудиврейлгяфврвироуграмзуьоиегъиргзюэжышэвтмжзыорабетяауоуэгфмгхоыпоохстычхуэякаэыратябоэщкямвдхюдмпызувгффмспшддлуоеизъщцубкэызупьмувркмлссюфсясъвгшмнэксйчуэищьливгрррцгюшцрмпрврацяйпытгймммыкаъенълриъуонмъргаъафтячвбилжызгюццчеисабын

прошлопятнадцатьднейистарыйдомпостепенноначаложиватьсороклетвнемниктонежилпонастоящемузаэтовремяонсменилодиннадцатьхозяевниктоизнихневыдерживалвподобномместебольшетрехмесяцевкреоливанессасталидвенадцатымимагполностьюпогрузилсявработуонотрывалсятолькозатемчтобыпоестьаотснаизбавлялсязаклятиембессонницынодлякреолаэтоявнонепроходилобезнаказанноглазаунегопокраснелиавекинабряклииотвисливанессавсяческистараласьубедитьеговтомчтоемуследуетпрекратитьиздевательстванадорганизмомихотьразоквыспатьсяпонастоящемуномагтолькоогрызалсязанималсяондвумяделаминеутомимописалмагическуюкнигуиокутывалособнякмагическойзащитойитоидругоетребованлоуймывременикреолникакнемогрешитьчтодлянегоболеесрочн

Висновки

Під час виконання практикуму ми засвоїли деякі методи частотного криптоаналізу, а також здобули деякі навички роботи та аналізу потокових шифрів, застосовуючи наші навички програмування та теоретичні знання з предмету «Симетрична криптографія». Під час виконання практикуму, ми отримували нові вміння на прикладі роботи з шифром Віженера. Ми на практиці показали, що шифр Віженера не є надійним, оскільки він зберігає багато статистичних властивостей мови, що дозволяє розбити будь-який зашифрований текст на блоки, та окремо і незалежно розглядати кожен з блоків, як текст, закодований шифром Цезаря з різними ключами. Саме цей факт і показує ненадійність шифру Віженера і ми змогли це довести на практиці.