Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

СИМЕТРИЧНА КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:
студентки групи ФІ-94
Зацаренко А. Ю.
Футурська О.В.

Перевірив:
Чорний О.М.

Київ – 2022

ЗМІСТ

ЗАГАЛЬНІ ВІДОМОСТІ

1. Мета комп’ютерного практикуму

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

2. Постановка задачі

Варіант 2.

Створити програму для знаходження ключа шифру Віженера двома способами та дешифрувати текст за варінтом.

3. Хід 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, абостатистику 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.

4. Опис труднощів

Реалізовуючи програмний код, ми зіштовхнулися з проблемою, що для кожної формули потрібно знаходити порядковий номер літер текстів, шляхом пошуку букви у алфавіті. В результаті ми вирішили один раз проробити цю операцію і зберігати текст у вигляді масиву індексів.

Ще одна проблема, з якою ми зіштовхнулися, це розбивання текстів на блоки. Але ми вирішили не зберігати текст частинами, а при необхідності проглядати його через r символів, де r – довжина ключа, за допомогою функції for.

ПРАКТИЧНА ЧАСТИНА

1. Значення індексів відповідності

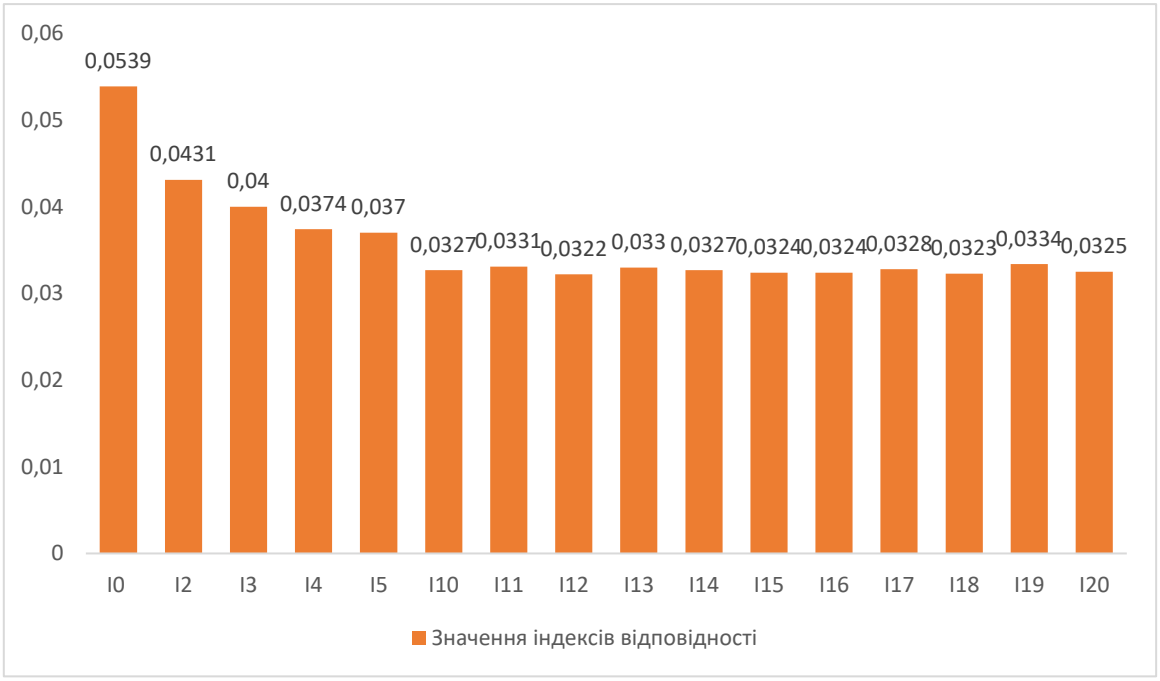

Рис.2.1 – Значення індексів відповідності

2. Встановлення довжини ключа

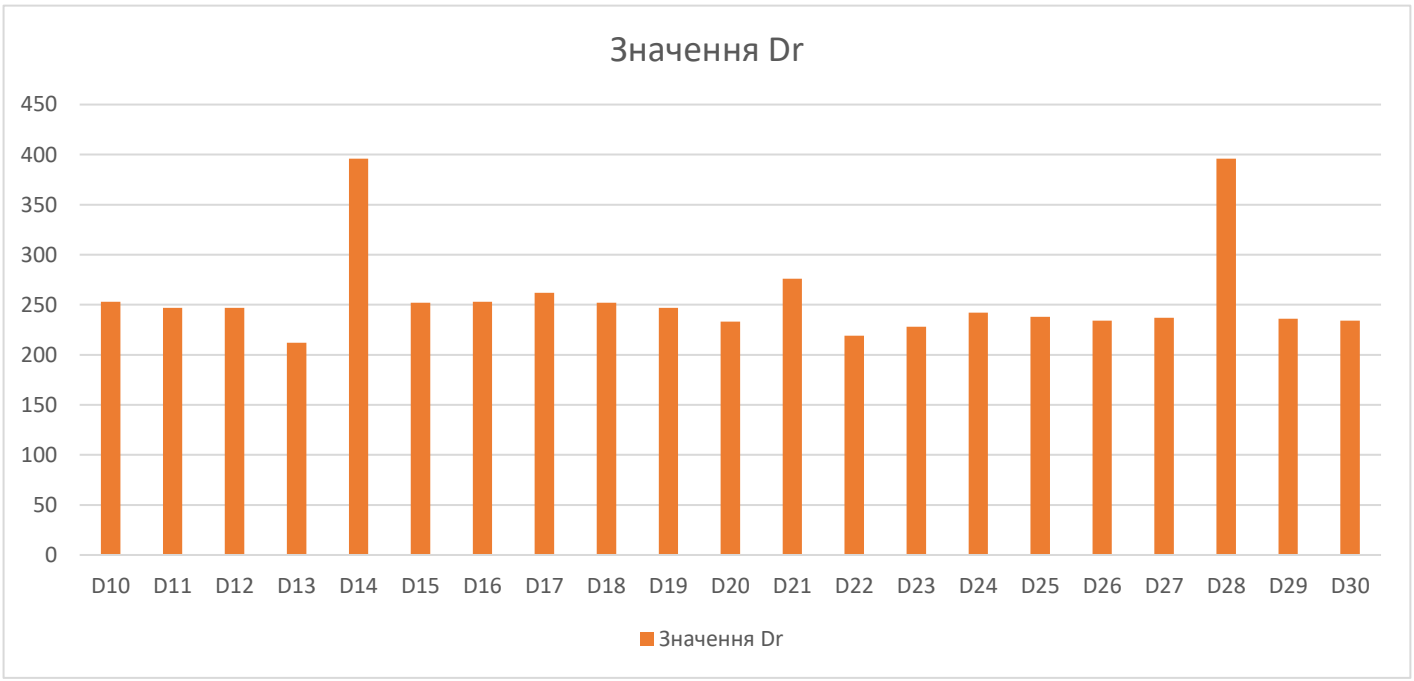

Рис.2.2 – Значення послідовності D_r

Отже, довжина ключ r = 14.

3. Знаходження ключа шифру Віженера

I. Значення ключа, одержане із використанням функції $M_i(g)$:
Ключ : последнийдозор

II. Значення ключа, одержане шляхом співставлення найчастіших літер блоків найчастішій літері мови:
Ключ : жосвеыдиадозор
Скорегований ключ : последнийдозор
Більшість літер були співставлені з найчастішою буквою російського алфавіту «о», а інші з другою по частоті – буквою «е».

4. Розшифрування шифртексту

какясмогэтосделатьспросилгесерипочемуэтогонесмогсделатьтымыстоялипосредибеск
райнейсеройравнинывзгляднефиксироваляркихкрасоквцелойкартиненостоиловсмотре
тьсявотдельнуюпесчинкуитавспыхивалазолотомбагрянцемлазурьюзеленьюнадголовой
застылобелоесрозовымбудтомолочнуюрекуперемешалискисельнымиберегамидаивыпл
еснуливнебесаащедулветерибылохолодномневсегдахолодноначетвертомслоесумрака
ноэтоиндивидуальнаяреакциягесерунапротивбыложарколицораскраснелосьполбустека
ликапелькипотамненехватаетсилысказалялицогесерасовсемпобагровелоответнеправил
ьныйтывысшиймагтакполучилосьслучайнонотывысшийпочемувысшихмаговтакженаз
ываютмагамивнекатегорийпотомучторазницавсилемеждуниминастольконезначительн
ачтонеможетбытьисчисленаиневозможноопределитьктосильнееактослабеепробормота

ВИСНОВКИ

У даній роботі було обраховано індекси відповідностей для текстів, зашифрованих ключами різних довжин. Також за допомогою послідовності D_r, знайдено довжину ключа. Значення ключа було знайдено двома способами: із використанням функції $M_i(g)$ та шляхом співставлення найчастіших літер блоків найчастішій літері мови. Перший спосіб виявився ефективнішим, бо значення, отримане другим способом, потребувало коригування.