Національний Технічний Університет України
“Київський Політехнічний Інститут”
Фізико-Технічний Інститут

СИМЕТРИЧНА КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3:
Криптоаналіз афінної біграмної підстановки

Виконав студент 3-го курсу
групи ФІ-14
Геращенко Володимир

Київ 2024

1 Мета роботи

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

2 Хід роботи

2.0 Робота з текстом

На відміну від першої лабораторної, де я не прибирав символи 'ё' і 'ъ', і другої лабораторної, де я прибирав тільки 'ъ' - в цій прийшлось ці обидва символи.

2.1 Написання математичних утиліт для розв'язку конгруенцій

Тут особливих складнощів не було, тільки те, що в C# функція залишку від ділення, повертає не модуль числа, а залишок від ділення.

2.2 Атака на афінний шифр

Як виявилось, головною проблемою було підставити значення, для знаходження множника a в нашому ключі - я все переплутав,сидів два дні, шукав помилки і думав чого в мене не виходить змістовний текст. Також частоти біграм символів у моєму відкритому тексті відрізняється від «ст», «но», «то», «на», «ен». На рівні з ними стоять ще декілька біграм, тому прийшлось "захардкодить" ці значення у функцію пошуку ключів чіназес.

2.3 Аналіз змістовності тексту

Я обрав для критеріїв змістовності такі параметри:

1. Критерій заборонених біграм - я обрав біграми, які не зустрічаються в моєму відкритому тексті, і перевіряю, наскільки багато цих біграм в вхідному тексті - якщо більше заданого порогу - відкидую.
2. Ентропійні критерії - перевіряю ентропію і індекс відповідності - якщо модуль різниці зі значеннями ентропії вихідного тексту за модулем більше заданого - відкидую.

3 Результати роботи

3.1 Найчастіші біграми шифротексту

Нижче можна побачити 5 найчастіших біграм шифротексту: В цілому, очевидно що це не

Біграма	Кількість
рн	63
ыч	44
нк	43
цз	37
тч	33

змістовний текст, просто дивлячись на ці біграми - їх майже немає в звичайних текстах, а в цьому - вони найчастіші

3.2 Критерії змістовності тексту

Щоб обгрунтувати обрані критерії, я вирішив показати наглядно на графіках вибрані критерії для кожної розглянутої пари ключів - як можемо побачити, на ключі $a = 13, b = 151$, наші критерії показуються зовсім інший результат, ніж на усіх інших:

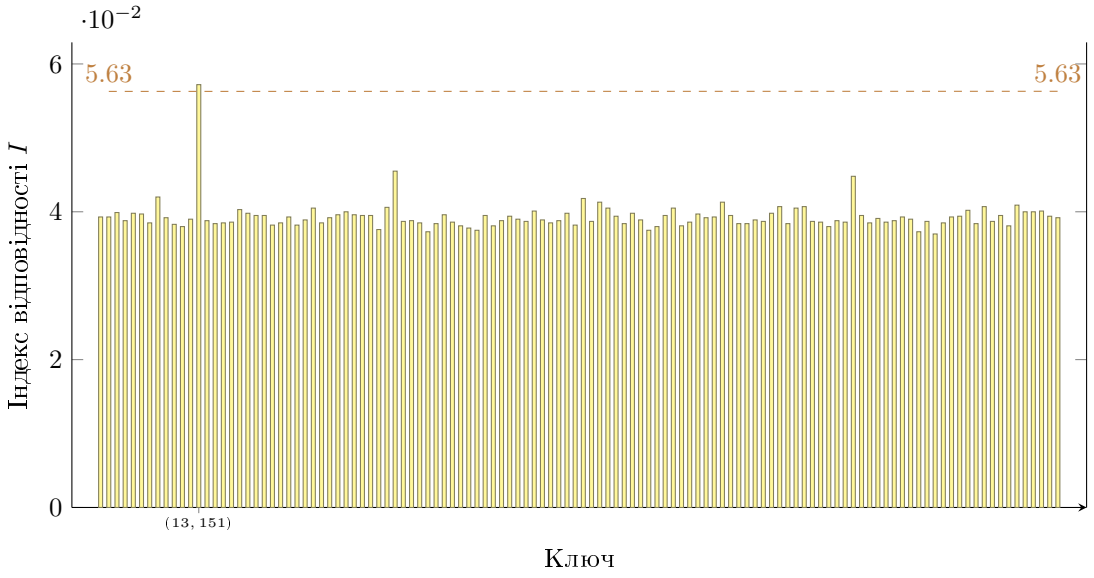

Рис. 1: Графік індекса відповідності тексту, розшифрованого певним ключем

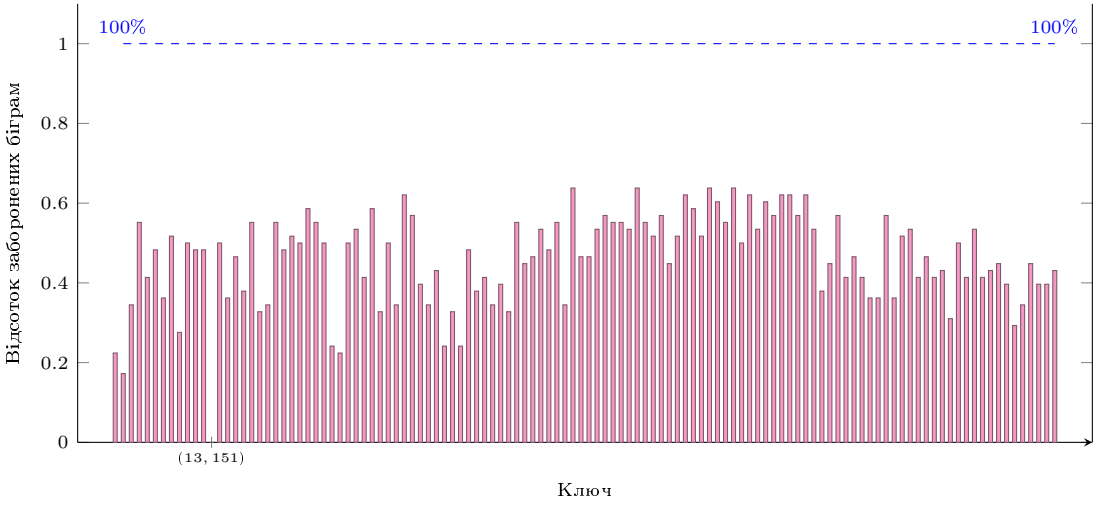

Рис. 2: Графік відсотка заборонених біграм у тексті, розшифрованого певним ключем

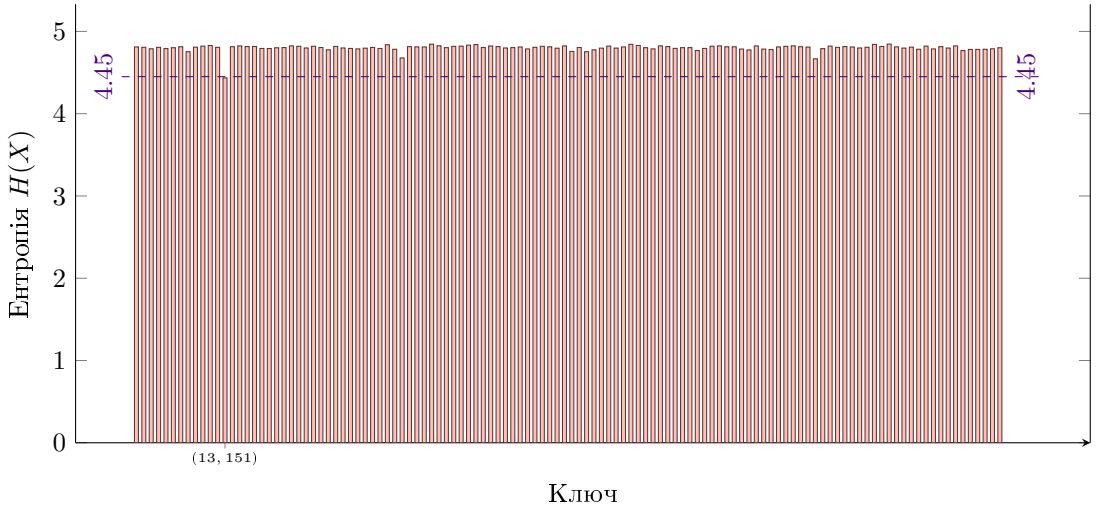

Рис. 3: Графік ентропії тексту, розшифрованого певним ключем

3.3 Розшифрування заданого тексту

Критерії підбирались методом тика, тому я прийшов до таких значень:

- Кількість заборонених біграм не перевищує 5%;
- Ентропія не віддаляється від ентропії мови на 0.2;
- Індекс відповідності не віддаляється від індексу відповідності мови на 0.01

Після того, як по критеріям пройшов ключ $a = 13, b = 151$, то підставимо його, і розшифруємо текст, де зелене - це розшифрований текст:

лквдвдьышкрбызякиабшачрнвязарч тчлчькзтманэмнязяыбштрпнхтрхрн зтжккысечамнмпывйвфяжтинфвйвйв сжнпчнмпгущзкыфвйвутсюцзкыкынм отзщбйьыбшхолуычгкицепзкианьуы фллфтыраючькиащзтыфэнкйяпезтнк жккысечамнмпжэпаычйдбцвсшчмтшс лаиятасзбчжйьыбшывлтйэзщбцпцмп щрифкздтеэкктщзархрчосйпрйжкле чаккяжюыщяояфскчбяызрчйзчвгзжз	многогщуннуюяичностыдостоевско гомотнорассматрияутысчетырехст оронзукписателткакневротикакак мьслителяэтизуикакгрешнизузукж еразобщутысявэжойневолыноспацу ющейкусслотностикуименееспорен онзукписателымесжоеговодномряд усшекспиромбщутыткарамазовьвел ичайшийроманизвсехкогдалибонап исанньтулегендаовеяикоминквизи

Виглядає як змістовний текст, але не дуже. Прочитавши уважніше методичку, можемо зрозуміти, що алфавіт у нас може бути іншим - поміняні місцями літери ’ь’ і ’ы’. Після зміни алфавіту, бачимо:

лквдвдьышкрбызякиабшачрнвязарч тчлчькзтманэмнязяыбштрпнхтрхрн зтжккысечамнмпывйвфяжтинфвйвйв сжнпчнмпгущзкыфвйвутсюцзкыкынм отзщбйьыбшхолуычгкицепзкианьуы фллфтыраючькиащзтыфэнкйяпезтнк жккысечамнмпжэпаычйдбцвсшчмтшс лаиятасзбчжйьыбшывлтйэзщбцпцмп щрифкздтеэкктщзархрчосйпрйжкле чаккяжюыщяояфскчбяызрчйзчвгзжз	многограннуюличностьдостоевско гоможнорассматриватьсчетырехст оронкакписателякакневротикакак мыслителяэтикаикакгрешникакакж еразобратьсявэтойневольносмуща ющейнассложностинаименееспорен онкакписательместоеговодномряд усшекспиромбратьякарамазовывел ичайшийроманизвсехкогдалибонап исанныхалегендаовеликоминквизи

І нарешті - змістовний текст, який ми так шукали.

4 Висновок

За результатами цієї лабораторної можемо побачити, що при підборі ключа змістовні тексти будуть мати більший індекс відповідності і меншу ентропію - тому що розподіл змістовного буде більш нерівноімовірним. Також змістовний текст навряд-чи буде містити біграми, яких немає у відкритому тексті(хоча він повинен бути достатньо великим).