Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Навчально-науковий інститут атомної та теплової енергетики

Кафедра цифрових технологій в енергетиці

Лабораторна робота 1

З навчальної дисципліни

«Безпека інформаційних систем»

КЛАСИЧНИЙ ШИФР ПРОСТОЇ

ЗАМІНИ ТА ЙОГО КРИПТОАНАЛІЗ

Виконала: студентка групи ТР-33

Бондар Варвара

Варіант № 1

Перевірив: Онисько Андрій Ілліч

Київ – 2025

**Мета лабораторної роботи** – ознайомлення та набути умінь із зашифровування та дешифрування повідомлень за допомогою шифру простої заміни, за допомогою шифру Цезаря.

***Завдання 1***

Створити програму на будь-якій мові програмування для шифрування повідомлень із використанням шифру Цезаря (англійській алфавіт).

Код програми:

const key = 1;

const primaryWordElement = document.querySelector(".primaryWord");

const encryptedElement = document.querySelector(".encrypterElement");

const wordToDecript = document.querySelector(".decryptWord");

const decryptedElement = document.querySelector(".decryptedElement");

primaryWordElement.addEventListener("input", (event) => {

  const primaryInputWord = event.target.value;

  const lastnameArray = primaryInputWord.split("");

  const encryptedLastnameArray = lastnameArray.map((letter) => {

    const code = letter.charCodeAt(0);

    let charcode = code + key;

    if (charcode > 122) {

      charcode = 97 + (charcode - 123);

    }

    return String.fromCharCode(charcode);

  });

  const encryptedLastname = encryptedLastnameArray.join("");

  encryptedElement.textContent = encryptedLastname;

});

wordToDecript.addEventListener("input", (event) => {

  const encryptInputWord = event.target.value;

  const encryptArray = encryptInputWord.split("");

  const decryptedArray = encryptArray.map((letter) => {

    const code = letter.charCodeAt(0);

    let charCode = code - key;

    if (charCode < 96) {

      charCode = 122 - (96 - charCode);

    }

    return String.fromCharCode(charCode);

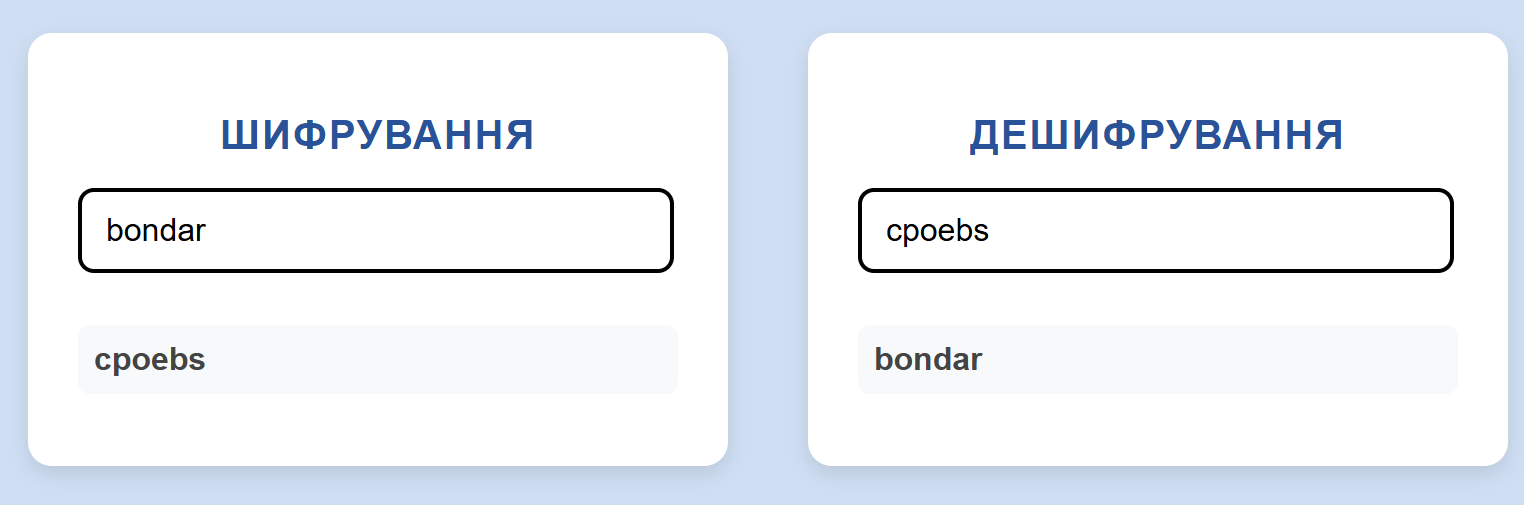
  });

  const decryptedLastname = decryptedArray.join("");

  decryptedElement.textContent = decryptedLastname;

});

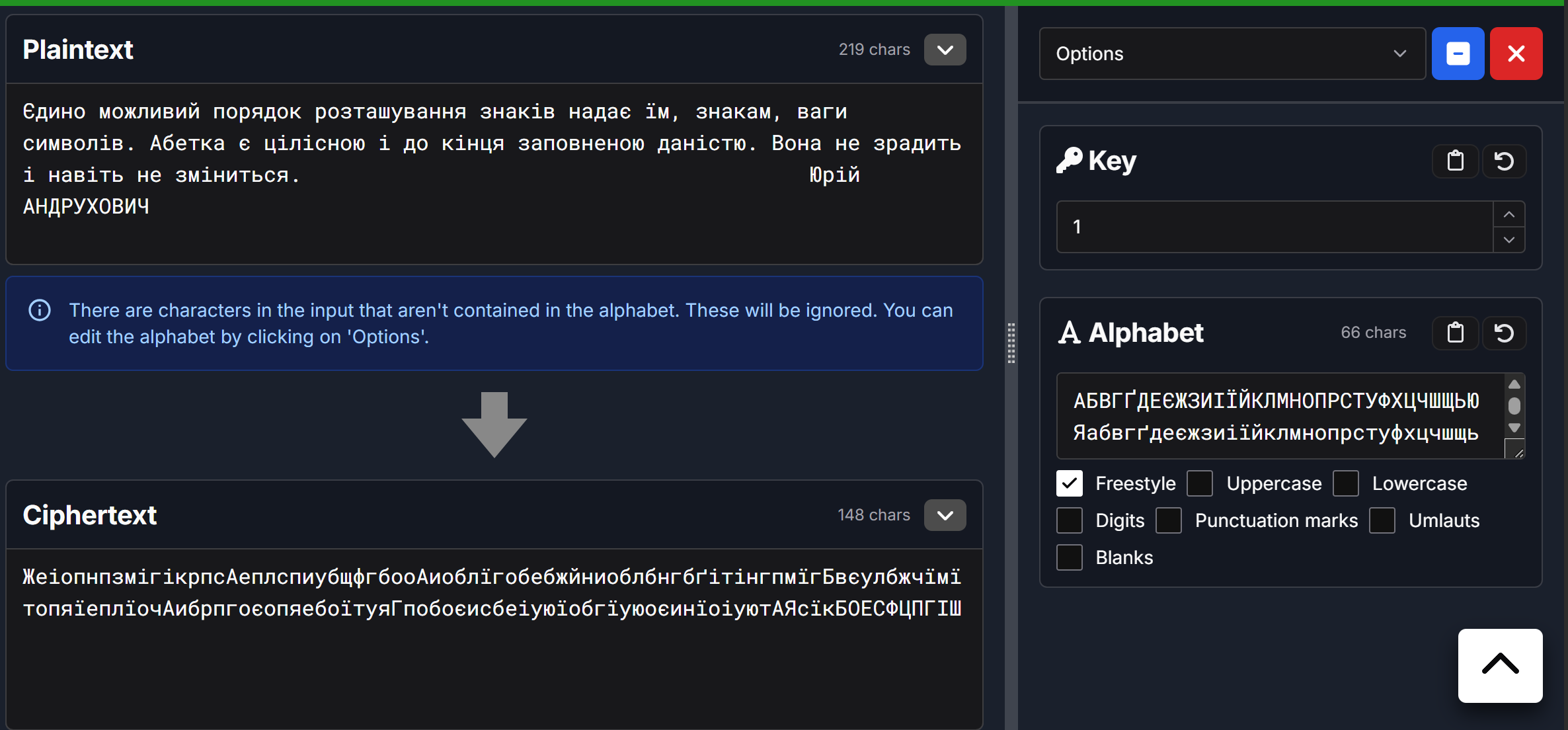
Результат:



***Завдання 2***

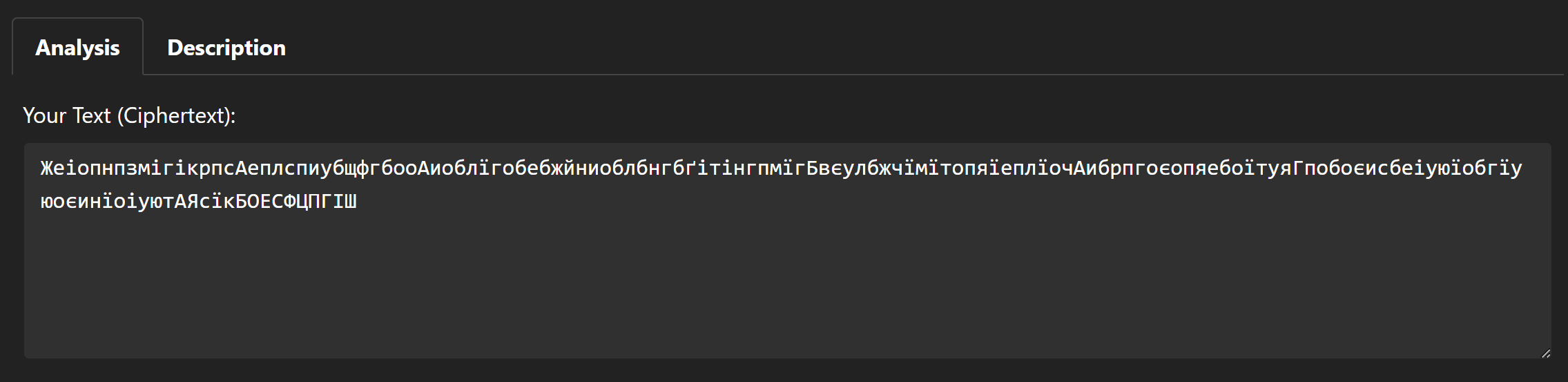
За допомогою програми CrypTool Online – *https://www.cryptool.org/en/cto/* з використанням шаблону *Caesar* виконати шифрування тексту шифром Цезаря згідно варіанту.

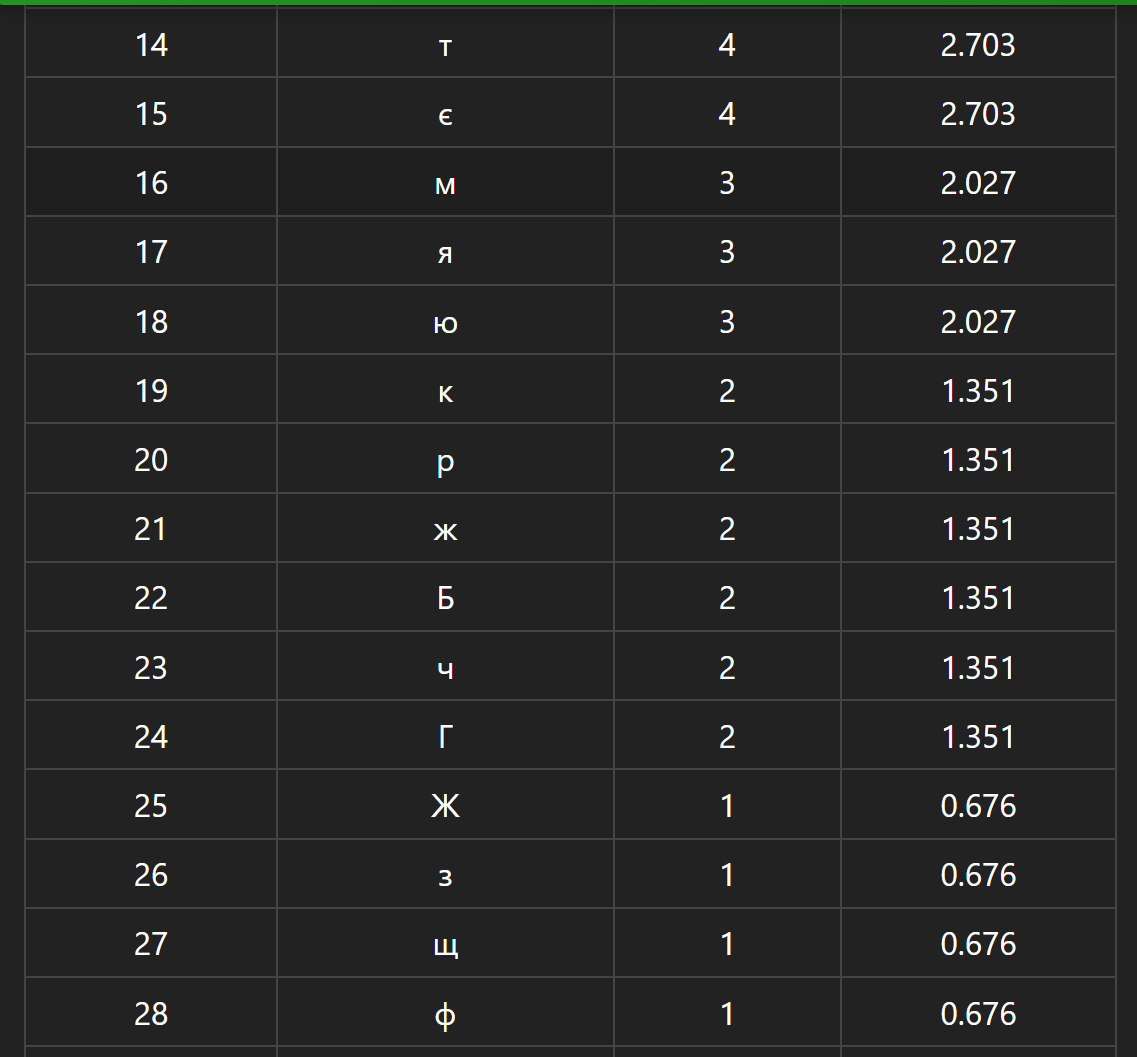
Спочатку введіть відкритий текст до поля *Input*, потім визначте алфавіт за допомогою опції *Define own alphabet,* ключ шифрування оберіть самостійно.

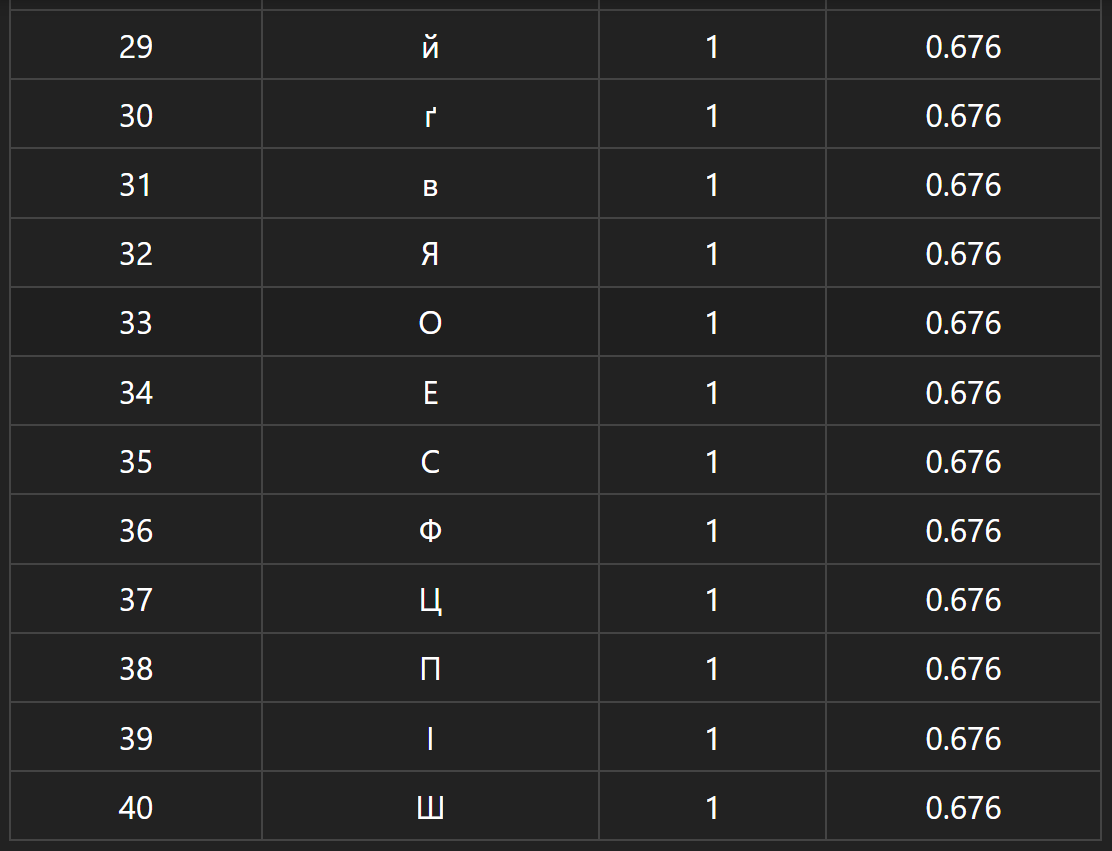
******

***Завдання 3.***

Підрахувати частоти зустрічальності літер у шифротексті, використовуючи шаблон *N-Gram Analysis* в розділі криптоаналізу на сайті *https://www.cryptool.org/en/cto/* (рис. 1.5).





Отже, з таблиці видно, що найчастіше зустрічається літера «о», на другому місці — «б». По літері «о» не можна робити однозначних висновків, адже з рисунка 2 видно, що «о» також є найчастотнішою літерою у звичайному тексті. Якби орієнтуватися лише на неї, можна було б помилково зробити висновок, що зсуву немає. Однак, оскільки це все-таки зашифрований текст, проаналізуємо другу за частотою літеру — «б». Із рисунка 2 видно, що на другому місці за вживаністю у відкритому тексті стоїть літера «а». Таким чином, можна припустити, що зсув дорівнює 1. І якщо розшифрувати з таким ключем текст, то буде отримано якраз початковий результат.

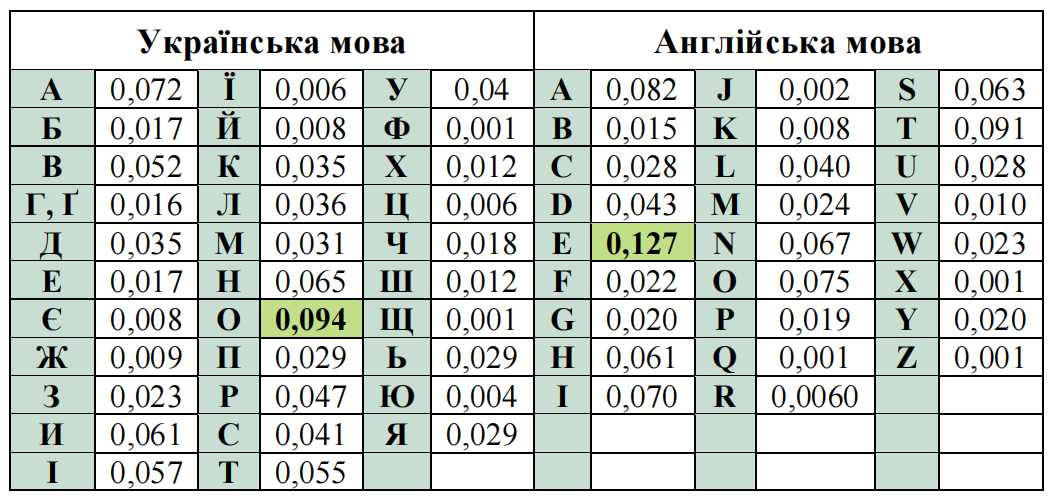


Рисунок 2. частота зустрічання літер

***Контрольні запитання:***

1. Що таке криптографічний алгоритм та шифр?

*Криптографічний алгоритм* – набір математичних правил та процедур, який описує такі види перетворень, як шифрування, формування та перевірка Ц П , обчислення хеш значень, криптографічних контрольних сум, створення імітовставки тощо

*Шифр* - сукупність криптографічних алгоритмів, що використовуються для

Шифрування.

1. Що таке криптографічний ключ?

*Криптографічний ключ (ключ)* – таємний стан деяких параметрів алгоритму криптографічного перетворення, що забезпечує вибір одного перетворення із сукупності можливих для даного алгоритму.

1. Назвіть складові криптографічної системи.



1. У чому полягає криптостійкість криптографічної системи?

*Криптостійкість* – це властивість криптосистеми протидіяти атакам протилежної сторони, спрямованим на отримання секретного ключа або відкритого повідомлення.

1. Опишіть алгоритм шифрування Цезаря.

*Шифр Цезаря* – шифр, де кожна літера повідомлення зсувається в алфавіті на – позицій вперед від символу, що замінюється. При досягненні кінця алфавіту виконується циклічний перехід до його початку. При необхідності розділові знаки та пробіли ігноруються.

1. У чому суть методу частотного криптоаналізу?

Метод частотного криптоаналізу полягає у порівнянні частот появи символів у зашифрованому тексті з типовими частотами символів у природній мові. Оскільки деякі літери вживаються частіше за інші (наприклад, в українській мові — «о», «а», «і»), це дозволяє відновити відповідність між літерами відкритого та зашифрованого текстів і розкрити шифр.