Злам шифрів



Моноалфавітні шифри

Вибір алфавіту

Визначте алфавіт для шифрування.

Зсув літер

Зсуньте алфавіт на певну кількість позицій.

Шифрування

Замініть кожну літеру на відповідну зі зсунутого алфавіту.



Онлайн калькулятор цифра Цезаря (англ)

Шифр Цезаря — найвідоміший приклад. Зсунь алфавіт на 3 літери: А → Г, Б → Д, В → Е.

Чому шифру Цезаря недостатньо

Проблема: Шифр Цезаря використовує один і той самий зсув для всіх букв.

Частотний аналіз (часте використання букв «о», «е», «н» тощо) дає змогу швидко зламати повідомлення.



Приклад:

Відкритий текст: МИР
Шифр Цезаря (зсув 3): ПЛУ

Якщо взяти довгий текст, кількість повторень літер підкаже зловмиснику, які саме символи зашифровані.

🔓 Алгоритми зламування шифру Цезаря

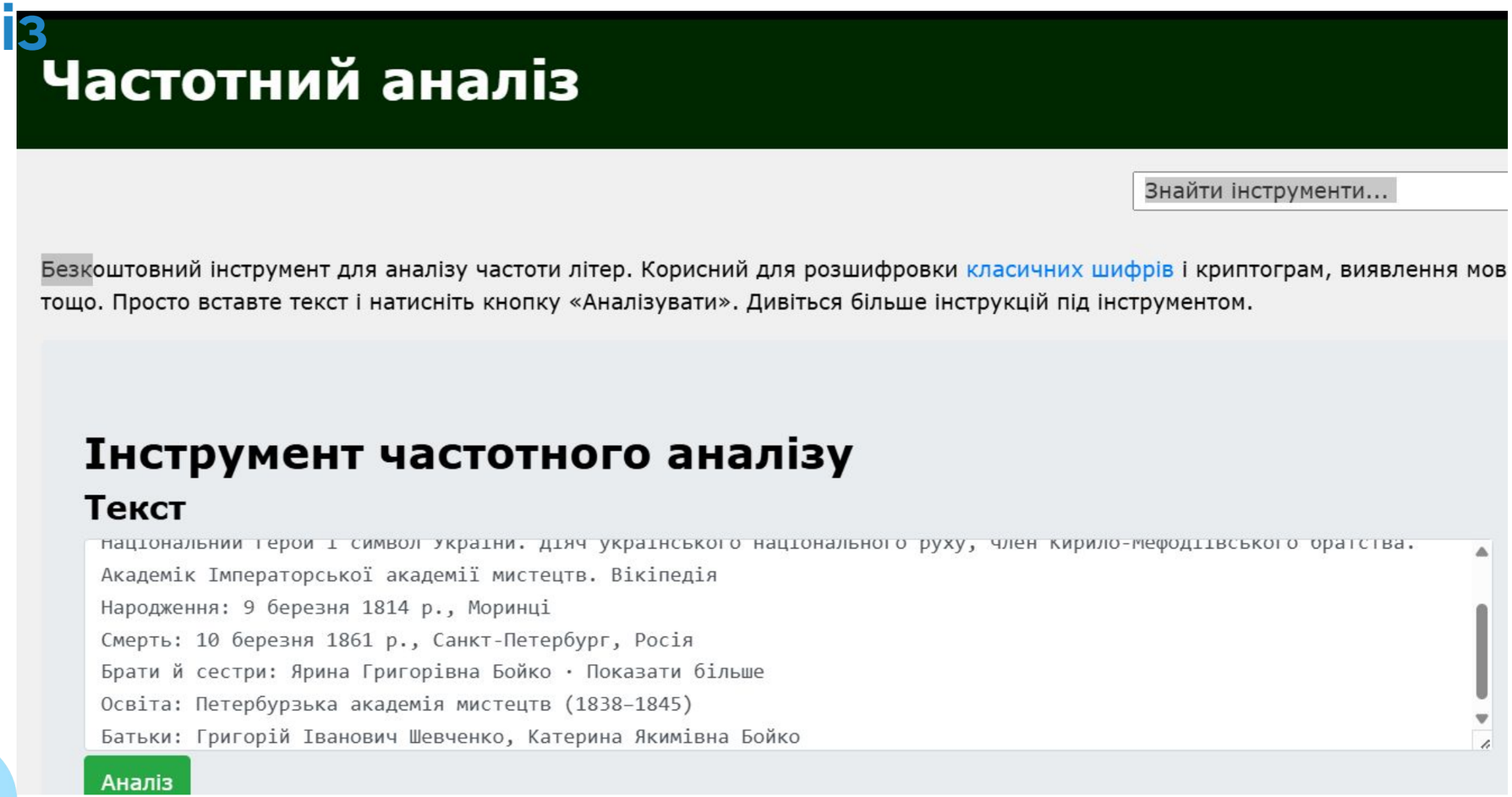
1. Частотний аналіз

1929 — **Вільям Фрідма**н систематизує частотний аналіз, тобто спосіб розшифрувати зашифроване повідомлення, вивчаючи, як часто зустрічаються окремі літери.

Як це працює?
У кожній мові деякі літери зустрічаються частіше за інші.

Наприклад, в українській найчастіші літери — **«?»**, **«?»**, **«?»**.

Частотний аналіз



ЗАВДАННЯ



З допомогою онлайн сервісу проведіть експеримент та визначте як 3 літери найчастіше зустрічаються в англійській, німецькій та українській мовах







Алгоритми зламування шифру Цезаря

?



Алгоритми зламування шифру Цезаря

2. Перебір усіх можливих зсувів

- У шифрі Цезаря всього N варіантів зсуву, де N — кількість літер в алфавіті (наприклад, 33 для українського).

- Ручно підставляємо кожен зсув (тобто "пробуємо ключі від 1 до 32") і дивимося, чи виходить осмислений текст.

- Це простий перебір (brute-force), але ефективний — особливо на коротких текстах.

ФУЦЖФЖСЩКФЦ

Це шифр Цезаря, спробуємо зламати:

Перебираємо ключі від 1 до 32:

Ключ 1: ЄТЦЄЕРРШЙЄТ → не схоже на мову
Ключ 5: ЯПУЯАННПЕЯП → вже краще, але ще не зрозуміло
Ключ 9: РІНРІЇЖЖІОРІ → осмислених слів не видно
Ключ 15: ІЖІІІУУУУЖІІЖ → дивно, але тут три однакові — можливо, «ИИИ»?

Нарешті на ключі 19:

ПРИВІТУСІМ

Алгоритми зламування шифру Цезаря

3. Пошук відомих слів (словниковий підхід)

- Після розшифрування кількома варіантами шукають знайомі слова: "і", "не", "ти", "ми", "що", "це", "україна" тощо.

- Якщо кілька таких слів з'являються — імовірно, ключ знайдено.

🔑 Приклад реалізації (уявний перебір):

🔍 Словник: ["МИР", "СЛАВА", "ПРИВІТ", "УКРАЇНА", "ГЕРОЯМ"]

🔁 Перевірка слова "ПРИВІТ":

- Пробуємо його зашифрувати всіма зсувами.
  При зсуві +6 → отримаємо ФУЦЖФШ.
-

  ✅ Збіг з шифротекстом: ПРИВІТ ←→ ФУЦЖФШ