Місія 5. Криптоаналіз. Як зламати шифр Цезаря?

Головна проблема

Ви вже знаєте, що шифр Цезаря криптостійкіший за Атбаш.

Але якщо комп'ютер може перебрати всі ключі за секунди, чи існують інші способи знайти правильний ключ?

---

1. Вступ

Історія.

У середньовіччі повідомлень стало дуже багато.

Перебирати всі ключі вручну було довго.

Криптоаналітики почали шукати закономірності.

Так народився криптоаналіз.

---

2. Компетентнісне завдання

Перед вами три зашифровані повідомлення.

Відомо, що всі вони зашифровані Цезарем.

Яке з них можна зламати найшвидше?

Чому?

---

3. Відео

Тема

Як народився криптоаналіз

У відео

- чому перебір не завжди найкращий;
- що таке криптоаналіз;
- що таке статистика літер;
- чому різні літери зустрічаються неоднаково часто.

---

4. Практика

Дослідження 1

Дайте текст на 500 символів.

Запропонуйте порахувати

A

B

C

...

Побудувати діаграму.

Питання

Чи однаково часто зустрічаються всі літери?

Учень відкриває

частотний аналіз.

Мінітеорія

Частотний аналіз.

Найчастіші літери.

Для англійської

E

T

A

O

I

N

---

5. Практика

Дослідження 2

Зашифрувати той самий текст Цезарем.

Побудувати діаграму ще раз.

Питання

Що змінилося?

Учень бачить

не форма графіка,

а лише її зсув.

Після цього

сам доходить висновку

Цезар не змінює статистику.

Мінітеорія

Саме тому

частотний аналіз легко знаходить ключ.

---

6. Практика

Google Colab

Написати програму

яка

рахує

частоти літер.

Побудувати гістограму.

---

7. Дослідження

Автоматичний підбір ключа.

Написати програму

що

для кожного ключа

рахує,

яка літера стала найчастішою.

Учень бачить

що правильний ключ знаходиться майже одразу.

Мінітеорія

Криптостійкість.

Вона залежить

не лише від кількості ключів,

а й від того,

чи приховує шифр статистику мови.

---

8. Нова проблема

Якщо частоти завжди однакові,

то будь-який моноалфавітний шифр можна зламати.

Як цього уникнути?

---

9. Дослідження

Беремо слово

HELLO

Шифруємо Цезарем.

Однакові літери

L

L

перетворюються

знову

в однакові.

Питання

Як зробити,

щоб однакові літери

перетворювалися

в різні?

Учні пропонують

міняти ключ.

Відео

З'являється

Віженер.

Наступна місія

Поліалфавітні шифри.

Далі вже можна будувати уроки так

1. **Цезар** → перебір.
2. **Моноалфавітні шифри** → частотний аналіз.
3. **Віженер** → руйнує частотний аналіз.
4. **Як зламали Віженера?**
    - індекс відповідності;
    - довжина ключа;
    - метод Касіскі.
5. **Роторні машини**
    - постійна зміна алфавіту.
6. **Одноразовий блокнот**
    - абсолютна криптостійкість.