

## Лабораторна робота №1

**Виконав:** Ваврикович Михайло ПМІ-33

**Тема:** Шифр зсуву для латинського {\_, a,b,...,z} та українського {\_,а,б,в,г,ґ,..., я} алфавітів.

**Мета:** Розробити криптосистему на основі шифрів зсуву.

### Хід роботи

1. Розробив інтерфейс криптографічної системи симетричного шифрування, передбачив в ньому використання панелі інструментів для виконання таких команд:
  - а. створення, відкривання, збереження, друкування файлів,
  - б. шифрування і розшифрування файлів українською та англійською мовами
  - с. виведення відомостей про розробника

#### Caesar

Type

☒ Encode ☐ Decode

Text

привіт

Encrypted text

ФХЛЕМЧ

Key

5

Locale

UA

Open file

Save file

Test

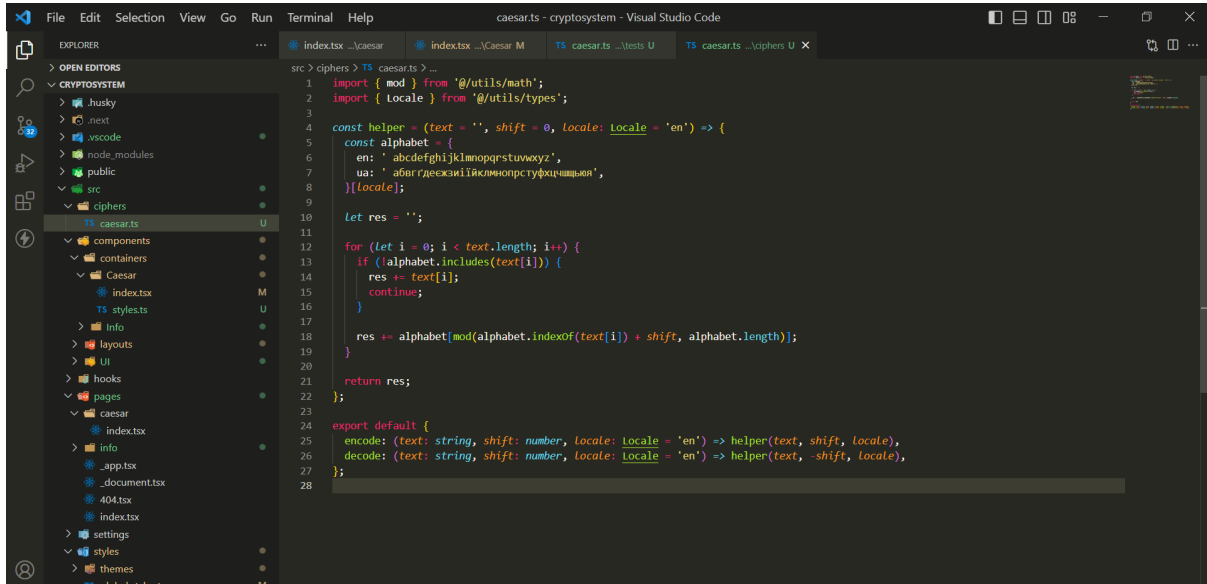
Attack

#### Info

Full name: Mykhailo Vavrykovych

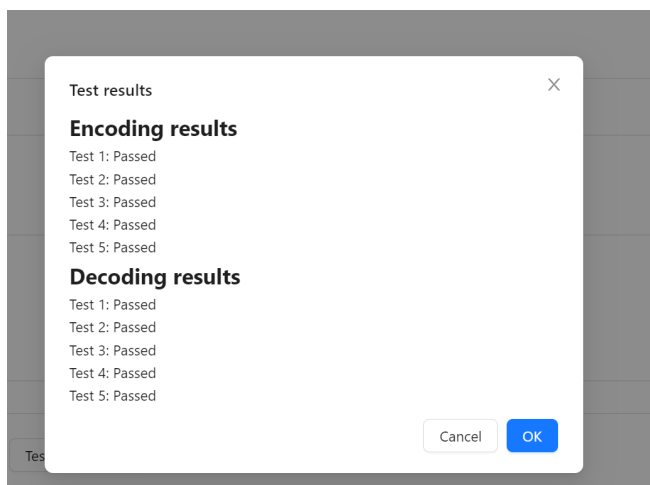
Group: AMI-33

2. Розробив систему для реалізації симетричного шифрування, передбачивши в них методи валідації ключа, валідації, шифрування і розшифрування даних



```
src > ciphers > TS caesar.ts > ...
1  import { mod } from '@utils/math';
2  import { locale } from '@utils/types';
3
4  const helper = (text: string, shift: number, locale: locale = 'en') => {
5    const alphabet = {
6      en: 'abcdefghijklmnopqrstuvwxyz',
7      ua: 'абвгдежзийклмнопрстуфхцшчшцщ',
8    }[locale];
9
10   let res = '';
11
12   for (let i = 0; i < text.length; i++) {
13     if (!alphabet.includes(text[i])) {
14       res += text[i];
15       continue;
16     }
17     res += alphabet[(alphabet.indexOf(text[i]) + shift) % alphabet.length];
18   }
19   return res;
20 };
21
22 export default {
23   encode: (text: string, shift: number, locale: locale = 'en') => helper(text, shift, locale),
24   decode: (text: string, shift: number, locale: locale = 'en') => helper(text, -shift, locale),
25 };
26
27
28
```

3. Виконав тестування роботи системи

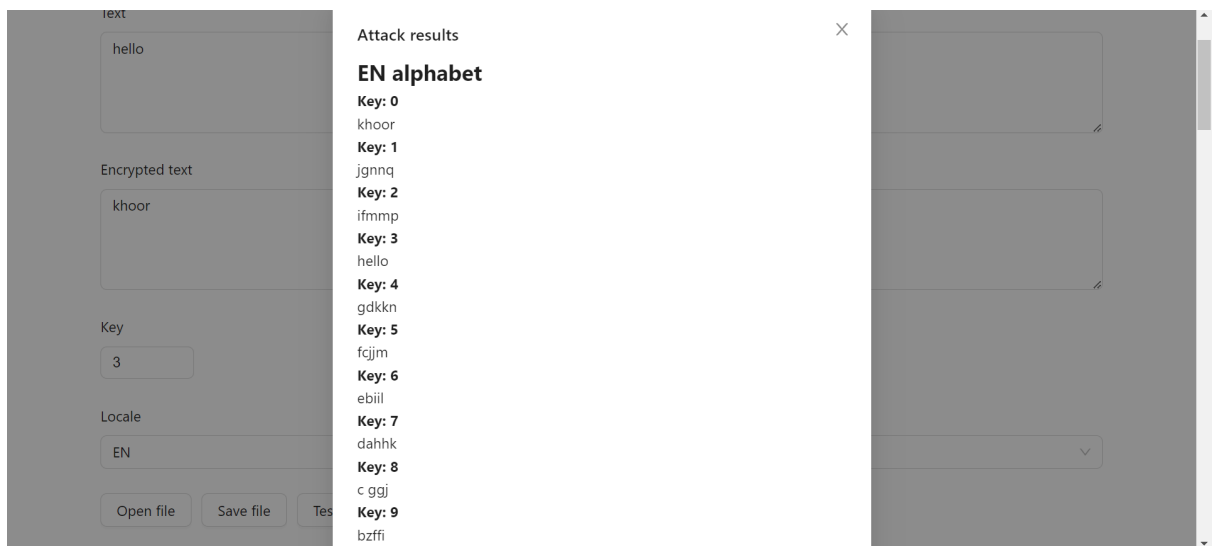


4. Доповнив розроблену систему модулем для атаки на шифр методом «грубої сили» (перебору)

```

47  }
48  };
49
50  export const getResults = () => {
51    const encodingResults = cases.map((item) => testEncoding(item));
52    const decodingResults = cases.map((item) => testDecoding(item));
53    return { encodingResults, decodingResults };
54  };
55
56  export const forceAttack = (cipher = '') => {
57    const alphabets: Record<string, string> = {
58      en: 'abcdefghijklmnopqrstuvwxyz',
59      ua: 'абарґдекзиіїклмнопрстуфхцшчшща',
60    };
61
62    const res: Record<string, { key: number; value: string }[]> = {};
63
64    Object.entries(alphabets).forEach(([locale, alphabet]) => {
65      res[locale] = [];
66
67      alphabet.split('').forEach((_, i) => {
68        res[locale].push({ key: i, value: caesar.decode(cipher, i, locale as locale) });
69      });
70    });
71
72    return res;
73  };
74
75

```



5. Побудував частотні таблиці для української та англійської мов
6. Розширив можливості системи, забезпечивши можливість шифрування даних в будь-якому форматі, а не тільки текстових.

**Висновок:** я розробив криптосистему на основі шифрів зсуву.