

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
НАЦІОНАЛЬНОГО АВІАЦІЙНОГО УНІВЕРСИТЕТУ»

Навчальна практика з дисципліни “Безпека програм та даних”

керівник Кожасєв Андрій Володимирович

Вид практики:

Навчальна практика з дисципліни "Безпека програм та даних" є обов'язковим етапом підготовки студентів фахового молодшого бакалавра. Вона спрямована на закріплення теоретичних знань і формування практичних навичок із захисту інформації, що дозволяє студентам володіти сучасними технологіями забезпечення безпеки в інформаційних системах

Форма проходження практики: очна

**Тривалість практики: 1 тиждень
з 14.10-18.10**

Завдання практики:

1. Засвоєння основ криптографії

Студенти вивчають базові принципи шифрування та дешифрування, ознайомлюються з алгоритмами, такими як шифр Цезаря, метод перестановки, XOR, RSA, Ель-Гамала, шифр-гамування та автоключ. Вони застосовують ці алгоритми на практиці, аналізуючи свої переваги та недоліки.

Завдання практики:

2. Засвоєння методів шифрування та дешифрування даних
Студенти опановують різні криптографічні методи, такі як шифр Цезаря, метод перестановки, XOR, шифрування та RSA.
Це включає як розуміння теоретичних основ кожного методу, так і їх практичну реалізацію. Навички роботи з цими алгоритмами дозволяють студентам впевнено використовувати засоби захисту даних і оцінювати їх ефективність залежно від конкретних умов та загрози безпеки.

Форма проходження практики:

Навчальна практика з дисципліни «Безпека програм та даних» проводиться в очній формі з доступом до комп'ютерного класу, де студенти мають змогу працювати з необхідним програмним забезпеченням та апаратними засобами для забезпечення безпеки інформаційних систем



База практики:



Базою для проходження практики є комп'ютерний клас, оснащений сучасними комп'ютерами з доступом до Інтернету та встановленим програмним забезпеченням, що дозволяє студентам виконувати завдання

Опис діяльності

Ознайомлення з методами шифрування:

- Вивчення основного шифрування (шифр Цезаря, метод перестановки, XOR).
- Написання програми для реалізації шифрування та дешифрування тексту

Опис діяльності

Практична робота з алгоритмами:

- Реалізація алгоритму RSA для захисту даних.
- Розробка програми для обфускації коду та автоматизації процесів.

Робота з мовами програмування:

- Написання коду для шифрування та дешифрування даних.

Матеріали про проходження практики

Реалізація алгоритму Цезаря - Блок-схеми

Шифр Цезаря. Шифрування

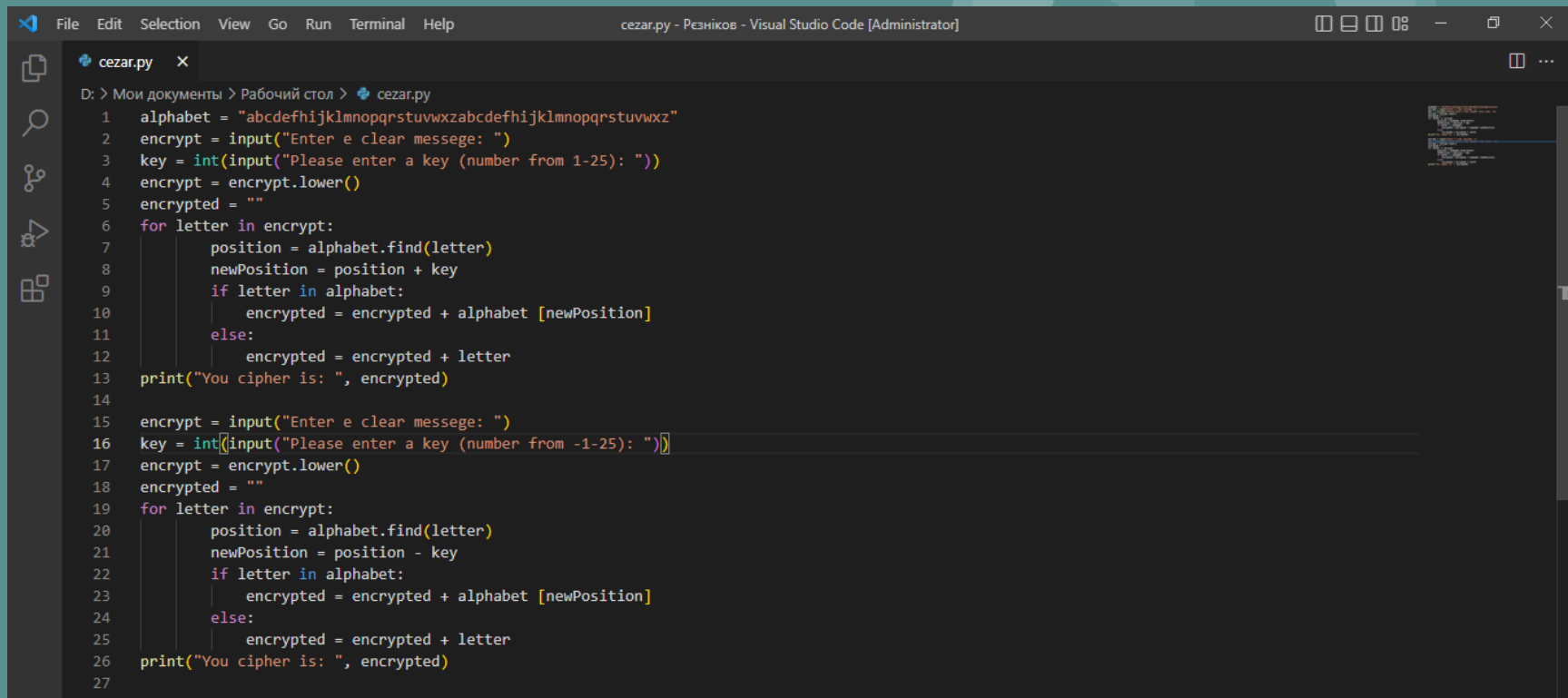


Шифр Цезаря. Дешифрування



Матеріали про проходження практики

Реалізація алгоритму Цезаря - Код програми



```
File Edit Selection View Go Run Terminal Help cezar.py - Резніков - Visual Studio Code [Administrator]
cezar.py x
D: > Мои документы > Рабочий стол > cezar.py
1 alphabet = "abcdefghijklmnopqrstuvwxyz"
2 encrypt = input("Enter e clear messege: ")
3 key = int(input("Please enter a key (number from 1-25): "))
4 encrypt = encrypt.lower()
5 encrypted = ""
6 for letter in encrypt:
7     position = alphabet.find(letter)
8     newPosition = position + key
9     if letter in alphabet:
10        encrypted = encrypted + alphabet [newPosition]
11    else:
12        encrypted = encrypted + letter
13 print("You cipher is: ", encrypted)
14
15 encrypt = input("Enter e clear messege: ")
16 key = int(input("Please enter a key (number from -1-25): "))
17 encrypt = encrypt.lower()
18 encrypted = ""
19 for letter in encrypt:
20     position = alphabet.find(letter)
21     newPosition = position - key
22     if letter in alphabet:
23        encrypted = encrypted + alphabet [newPosition]
24    else:
25        encrypted = encrypted + letter
26 print("You cipher is: ", encrypted)
27
```

Матеріали про проходження практики

Реалізація алгоритму Цезаря - Результат виконання програми

```
Enter e clear messege: cat
Please enter a key (number from 1-25): 3
You cipher is: fdw
Enter e clear messege: fdw
Please enter a key (number from -1-25): 3
You cipher is: cat
PS C:\Users\user\Desktop> █
```

Висновки:

Практика дозволила здобувачам освіти отримати не лише теоретичні знання, але й здобути практичні навички роботи з ключовими алгоритмами шифрування та захисту даних. Це допоможе впевнено отримати отримані знання в реальних проектах, забезпечуючи надійний захист інформаційних систем від загроз

Дякую за увагу!

