

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ДВНЗ «ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»  
КАФЕДРА ПРИКЛАДНОЇ МАТЕМАТИКИ І ІНФОРМАТИКИ

ЗАТВЕРДЖУЮ  
зав. кафедри ПМІ,  
д.т.н., проф. Дмитрієва О.А.

---

\_\_\_\_\_ 20\_\_р.

**ТЕХНІЧНЕ ЗАВДАННЯ**  
до курсової роботи з дисципліни  
«Методи та засоби криптографічного захисту інформації»

за темою  
**«Криптографічне хешування. Методи та алгоритмічна підтримка»**

(для студентів спеціальності 125 Кібербезпека  
всіх форм навчання)

Керівник:  
д.т.н., проф. каф.  
ПМІ Башков Є.О.

Виконавець:  
студент гр. КІБ-19  
Терехов Є. Р.

---

\_\_\_\_\_ 2022 р.

---

\_\_\_\_\_ 2022 р.

Покровськ – 2022 р.

## ВСТУП

Курсова робота виконується на підставі навчального плану підготовки студентів за освітньо-кваліфікаційним рівнем «бакалавр» та «Технічного завдання до курсової роботи» за дисципліною «Методи та засоби криптографічного захисту інформації» на тему: за темою «Криптографічне хешування. Методи та алгоритмічна підтримка» для студентів, що отримують освіту в галузі знань 12 «Інформатика та обчислювальна техніка», спеціальності 125 Кібербезпека.

## ЗАВДАННЯ НА КУРСОВУ РОБОТУ

Загальне завдання на курсову роботу передбачає розробку програмного скрипту на мові Python, який реалізує визначені індивідуальним завданням стандартні хеш алгоритми обчислення дайджестів текстових повідомлень. Варіанти індивідуального завдання наведені в таблиці А.1.

Індивідуальне завдання:

1. Опанувати знаннями та надати опис **Sha3**.
2. Створити програмний додаток визначення дайджесту відкритого повідомлення довільного розміру за **shake\_128** базової хеш функції.
3. Створити програмний додаток визначення дайджесту відкритого повідомлення довільного розміру за **shake\_256** базової хеш функції.
4. Знайти дайджест за першим та другим варіантом базової функції для файлу англійського довільного тексту, що має розмір не менш як 10 Кбайт.
5. Знайти дайджест за першим та другим варіантом базової функції для файлу українського довільного тексту, що має розмір не менш як 10 Кбайт.

## ЗМІСТ ТА ЕТАПИ РОЗРОБКИ

При виконанні курсової роботи студент повинен:

1. Ознайомитись з теоретичним матеріалом щодо криптографічних хеш функцій.
2. Надати опис базової криптографічної хеш-функції.
3. Створити два текстових файли. Файл англійською мовою обсягом не менш 10 Кбайт та файл українською мовою обсягом не менш 10 Кбайт
4. Розробити скрипт на мові Python для розрахунку дайджесту для текстів англійською та українською мовами за першим варіантом базової хеш-функції.
5. Розробити скрипт на мові Python для розрахунку дайджесту для текстів англійською та українською мовами за другим варіантом базової хеш-функції.
6. Порівняти отримані хеш дайджести та надати висновок з криптостійкості отриманих дайджестів.

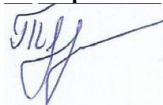
### Графік виконання курсового проекту

№	Найменування етапу	Строк виконання	
		тиждень	дата
1	Видача завдання на курсовий проект. З'ясування завдання.	1-2	09.02.22
2	Опанування математичними співвідношеннями визначеної базової функції хешування.	3-5	23.02.22
	Опанування бібліотекою HashLib	6	23.03.22
3	Проектування Python скрипту для обчислення хеш дайджестів	7	30.03.22
4	Розробка та тестування Python скрипту	8 - 9	06.04.22
6	Оформлення пояснювальної записки	10 - 11	20.04.22
7	Оформлення презентації	12 - 13	04.05.22
8	Захист курсового проекту	14 - 16	18.05.22

Виконавець

студент гр. КІБ- 19

Терехов Є. Р.



«09» лютого 2022 р.