**Міністерство освіти і науки України**

**Львівський національний університет імені Івана Франка**

Факультет прикладної математики та інформатики

*Звіт*

*Лабораторна робота №1*

«Таблиця»  
**з дисципліни "Алгоритми та структури даних"**

Виконав студент групи ПМІ-11  
 Яцуляк Андрій

**Хеш-функція**

**Хеш-функція**, або **геш-функція** — [функція](https://uk.wikipedia.org/wiki/%D0%9F%D1%96%D0%B4%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0), що перетворює вхідні дані будь-якого (як правило великого) розміру в дані фіксованого розміру.

**Хешування** — перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини. Такі перетворення також називаються **хеш-функціями**, або **функціями згортання**, а їхні результати називають хешем, **хеш-кодом**, **хеш-сумою**, або **дайджестом повідомлення**.

Хеш-функція використовується зокрема у структурах даних — хеш-таблицях, широко вживаних у програмному забезпеченні для швидкого пошуку даних. Хеш-функції використовуються для оптимізації таблиць та баз даних користуючись з того, що в однакових записів однакові значення хеш-функції. Такий підхід пошуку дублікатів ефективний у файлах великого розміру. [Криптографічна хеш-функція](https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%87%D0%BD%D0%B0_%D0%B3%D0%B5%D1%88-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D1%96%D1%8F) дозволяє легко перевірити, що деякі вхідні дані зіставляються із заданим значенням хешу, але, якщо вхідні дані невідомі, то навмисно важко відновити вхідне значення (або еквівалентну альтернативу), знаючи збережене значення хеш-функції.

Хеш-функції пов'язані (і їх часто плутають) з [контрольною сумою](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C%D0%BD%D0%B0_%D1%81%D1%83%D0%BC%D0%B0), контрольними цифрами, [відбитками пальців](https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%B4%D0%B1%D0%B8%D1%82%D0%BA%D0%B8_%D0%BF%D0%B0%D0%BB%D1%8C%D1%86%D1%96%D0%B2_(%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)), [рандомізацією функцій](https://uk.wikipedia.org/wiki/%D0%A0%D0%B0%D0%BD%D0%B4%D0%BE%D0%BC%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F_%D1%84%D1%83%D0%BD%D0%BA%D1%86%D1%96%D1%97" \o "Рандомізація функції), кодами, що виправляють помилки, і з шифрами. Хоча ці поняття певною мірою збігаються, кожне з них має свою власну сферу застосування і вимоги та є розробленим і оптимізованим по-різному.





















