Звіт до практичного заняття №3

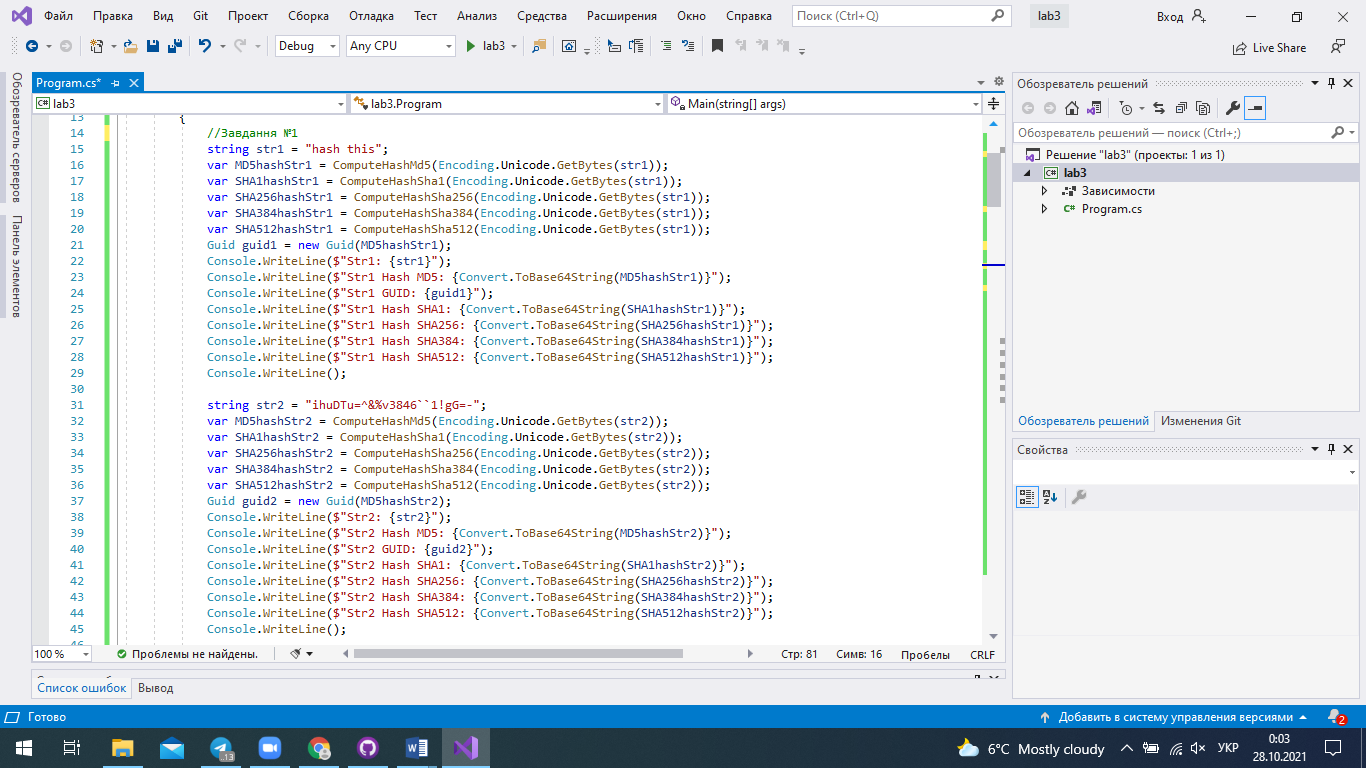
Тема: "Хеш-функції та перевірка цілісності інформації"

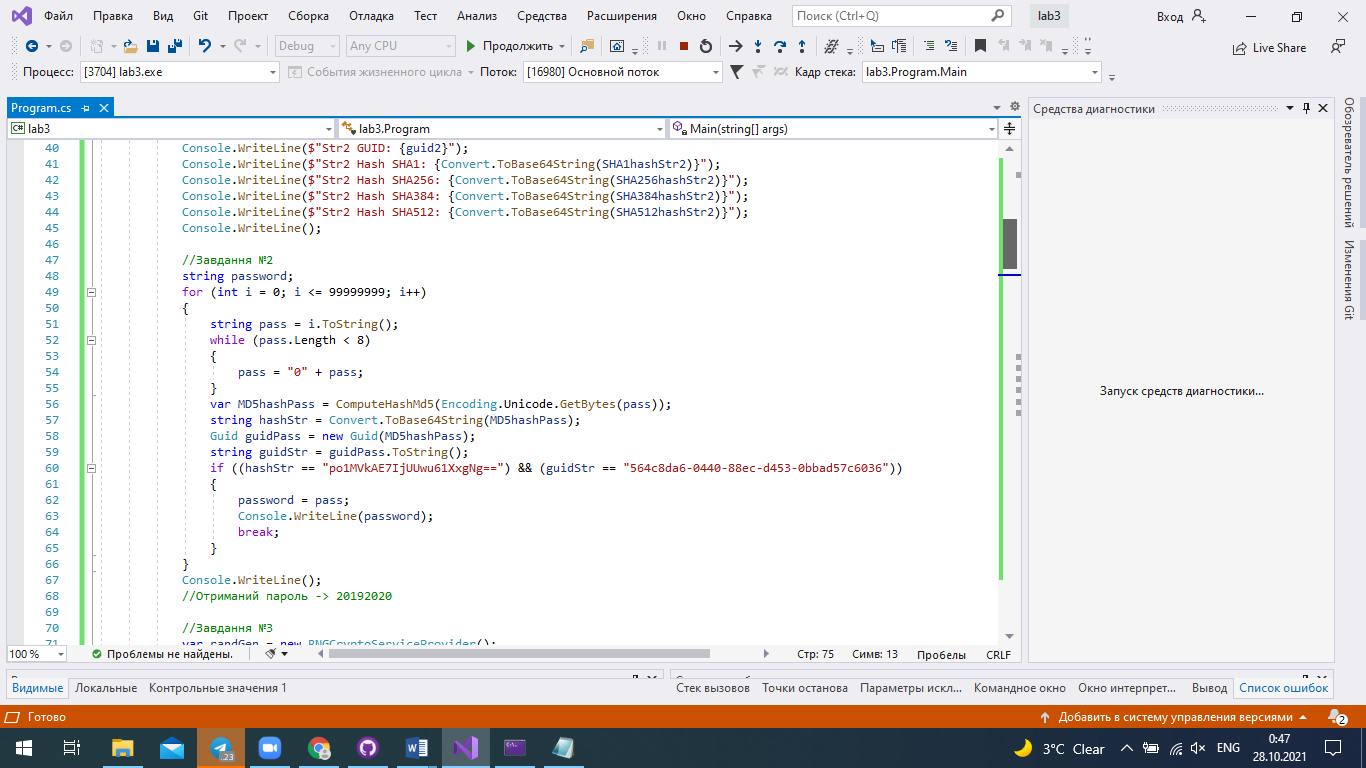
Семестр ІІІ. Основи інформаційної безпеки

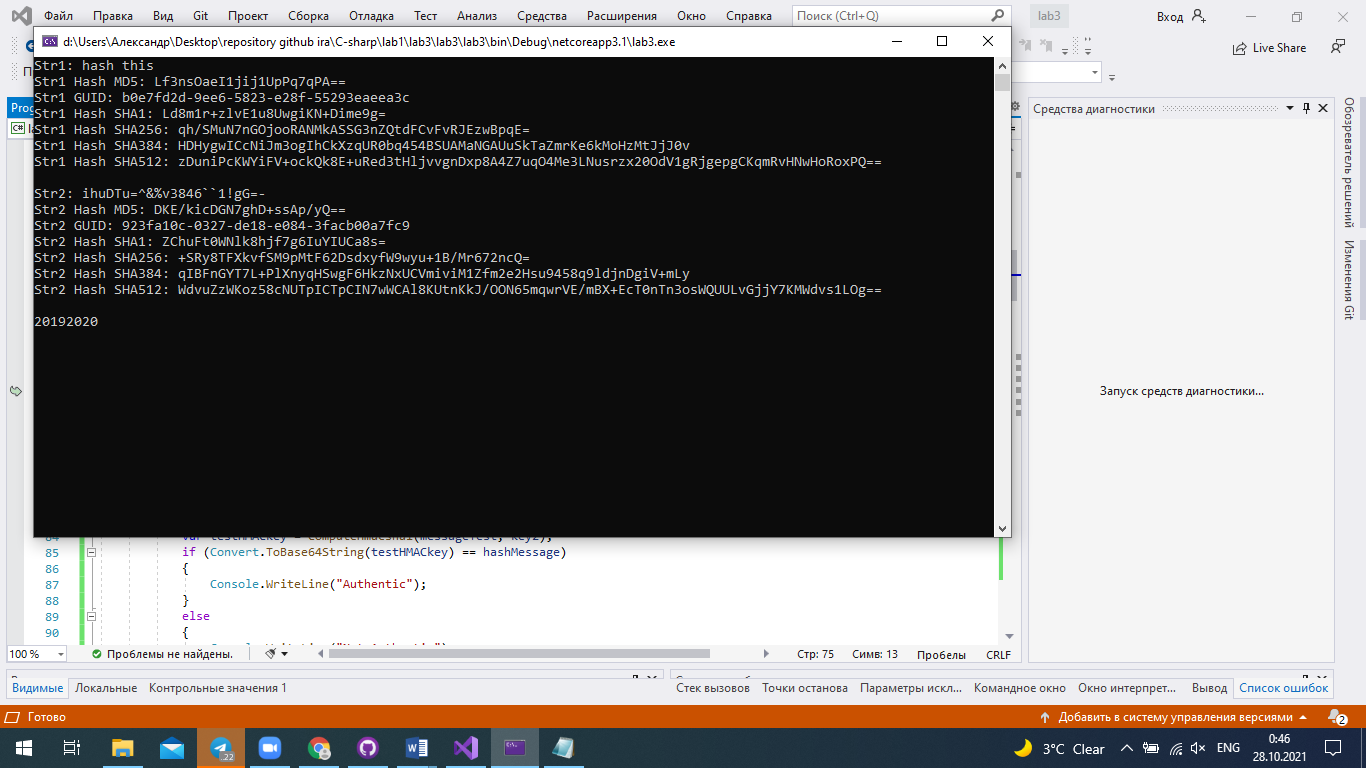
Грецької Ірини

Студентки МІТ-21

По перше обчислювання хеш-кодів, для обчислювання яких треба створити статичні методи для кожного алгоритму хешування(MD5, SHA1, SHA256, SHA384, SHA512), у яких використовую методи Create() та ComputeHash(), що після цього виводяться на консоль.







За інформацією паролем є 8 цифр, мається відомий хеш-код та Guid, що робить можливим виявлення алгоритмома хешування -> MD5. Щоб відновити пароль, проходимо циклом через всі можливі комбінації паролів і хешуємо кожен, отриманий хеш-код звіряємо з відомим, і таким чином отримуємо пароль - 20192020.

Висновок:

Так як хеш-код має стійку довжину і не має можливості бути оберненим у оригінальне повідомлення. Він є справді надійним способом порівняти 2 об’єкти

Але так як за допомогою хеш-коду можна відновити оригінальний текст, при наявності потрібної інформації пароль може бути знайденим.