ЗВІТ ПО ЛАБОРАТОРНІЙ РОБОТІ НОМЕР 1

ПРЕДМЕТУ КРИПТОГРАФІЯ

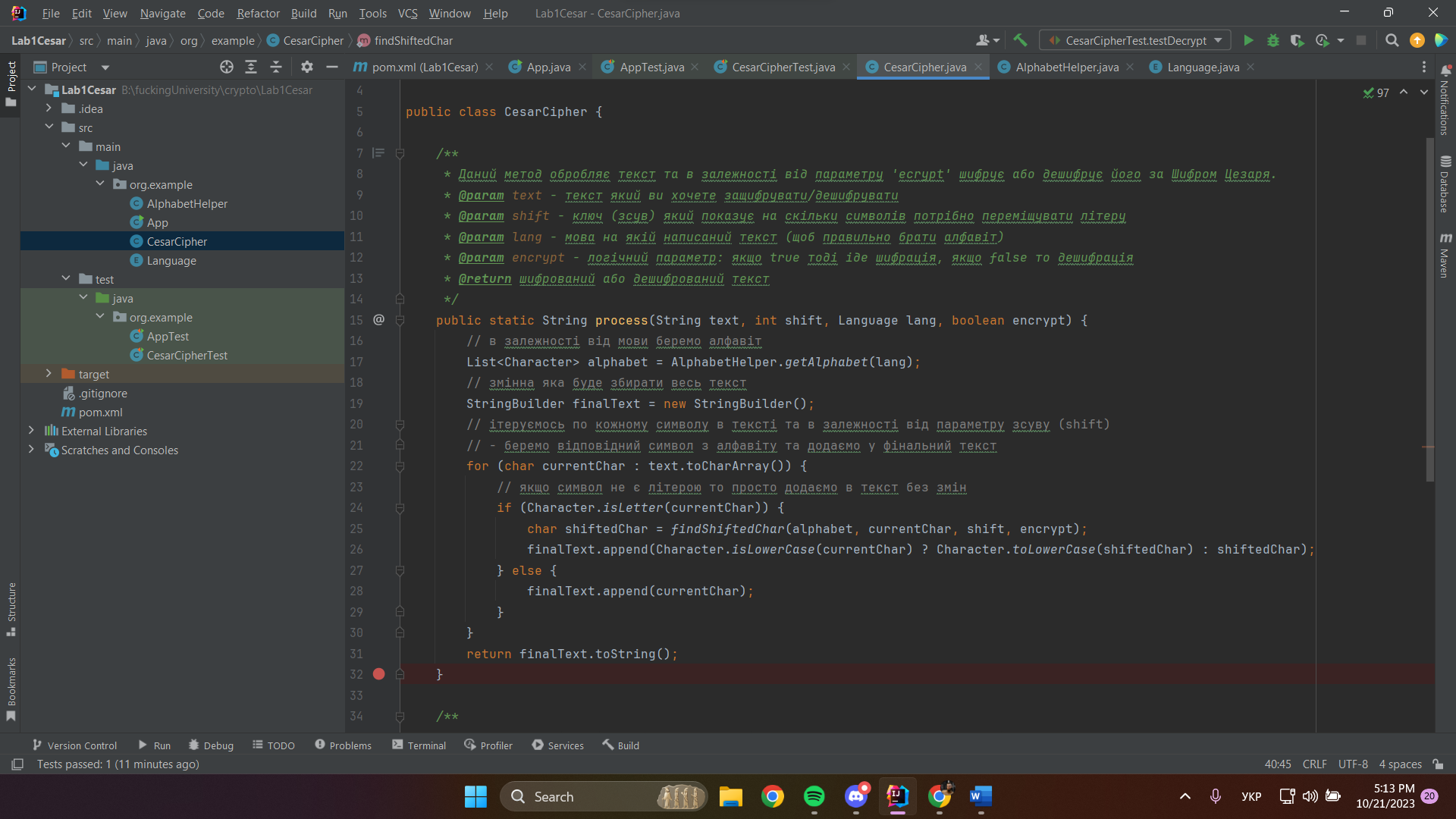
СТУДЕНТ: ПАНТЕЛЕЙЧУК ІЛЛЯ МИХАЙЛОВИЧ

(увесь код можна подивитись на GitHub [тут](https://github.com/ilyaPanteleychuk/CryptoForUniversity))

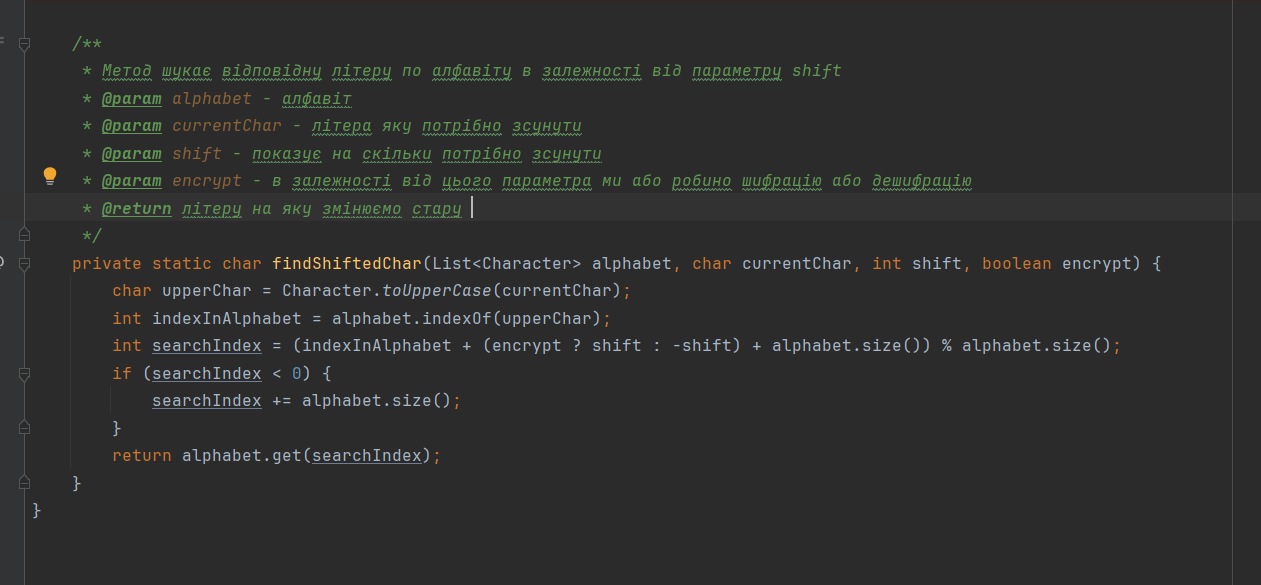
В даній лабораторній роботі потрібно було розробити додаток який може шифрувати та дешифрувати Шифр Цезаря.

Знизу наведені скріншоти з поясненнями програми яка виконує шифрування та дешифрування.

Метод який виконує шифрацію/дешифрацію даних.



Метод який робить зсув літер по алфавіту.



Для підтвердження прикріплюю декілька тест кейсів які шифрують/дешифрують тексти які були в завданні к цій лабораторній роботі.

Тест перевіряють такі правильного шифрування таких текстів

“Keep your friends close, but your enemies closer.”

“Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries.”

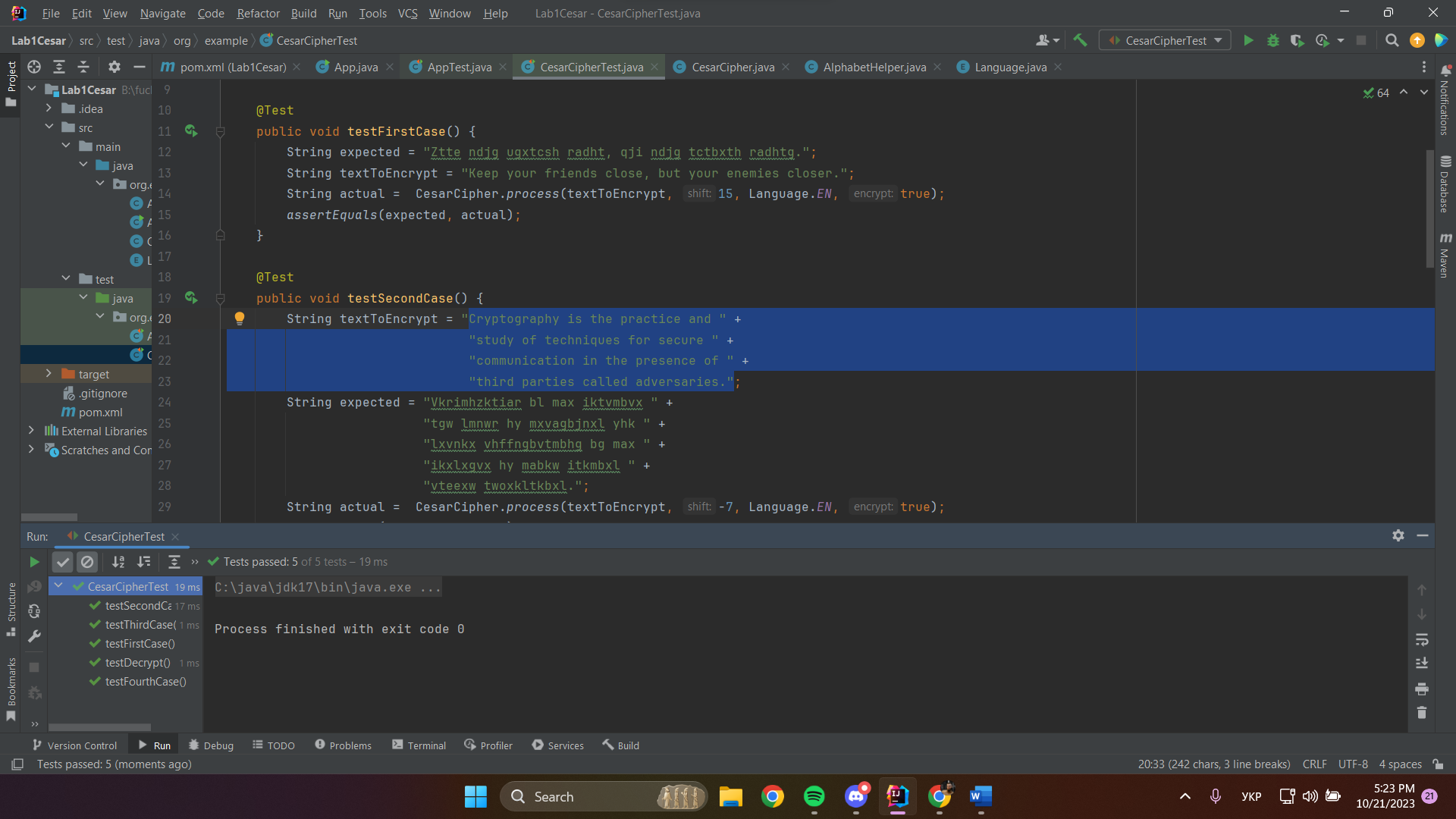
“ Украй простий приклад симетричного шифрування — шифр підстановки.”

“ Наука про математичні методи забезпечення конфіденційності, цілісності і автентичності інформації.”

Такой один тест перевіряє дешифрацію тексту:

“ Їшозш клй ішнбішндтїе ібнйад ґшщбґкбтбїїч зйїпеабїсежїймне, сеиемїймне е шьнбїндтїймне еїпйлішсеє.”

Як ми бачимо на скріншоті знизу – всі тести пройшли успішно



ВІДПОВІДІ НА ТЕОРЕТИЧНІ ПИТАННЯ

1. До якого класу найпростіших шифрів відноситься шифр Цезаря?

Шифр Цезаря відноситься до класу найпростіших шифрів, які відомі як підстановкові шифри.

1. За яким принципом відбувається шифрування тексту шифром Цезаря?

Шифрування шифром Цезаря відбувається зсувом символів в алфавіті на фіксовану кількість позицій. Наприклад, якщо кожен символ зсувається на 3 позиції вправо, то "A" стає "D", "B" стає "E", і так далі.

1. Якими методами можна зламати шифр Цезаря?

Шифр Цезаря може бути зламаний за допомогою методів криптоаналізу, таких як атака "грубої сили" (перебір усіх можливих ключів), статистичний аналіз тексту або аналіз частоти символів.

1. Що таке функція правдоподібності?

Функція правдоподібності використовується для оцінки ймовірності того, наскільки добре певна модель пасує до спостережень.

1. Чому для криптоаналізу використовується саме логарифмічна функція правдоподібності?

Логарифмічна функція правдоподібності часто використовується для спрощення обчислень і вираження ймовірностей в більш зручному масштабі.

1. Що таке метод максимальної правдоподібності?

Метод максимальної правдоподібності - це статистичний метод для оцінки параметрів моделі на основі спостережень, знаходження параметрів, які найкраще пояснюють спостереження.

1. Чи є шифр Цезаря криптостійким? Аргументуйте свою відповідь.

Шифр Цезаря не є криптостійким, оскільки може бути легко зламаний методами криптоаналізу, особливо при використанні сучасних обчислювальних засобів. Зміщення алфавіту на фіксовану кількість позицій легко атаковується методом грубої сили.

1. Яка потужність ключового простору шифру Цезаря?

Потужність ключового простору шифру Цезаря дорівнює кількості можливих зсувів у межах алфавіту. Наприклад, для англійського алфавіту з 26 літерами потужність ключового простору становить 26.

1. Яка мінімальна довжина фрагменту шифротексту потрібна для однозначного встановлення ключа шифру Цезаря?

Мінімальна довжина фрагменту шифротексту для однозначного встановлення ключа шифру Цезаря дорівнює довжині ключа. Тобто, якщо ключ відомий, то одного символа в шифротексті вже достатньо.

1. Скільки комбінацій ключа потрібно перевірити для зламу шифру Цезаря методом грубої сили?

Для злому шифру Цезаря методом грубої сили потрібно перевірити всі можливі зсуви алфавіту, тобто усі можливі ключі. Оскільки в англійському алфавіті 26 літер, то потрібно перевірити всі 26 можливих ключів.

1. До якого методу криптоаналізу відноситься функція логарифмічної правдоподібності?

Функція логарифмічної правдоподібності використовується в методі максимальної правдоподібності для оцінки параметрів моделі на основі спостережень.

1. Доведіть, що шифр Цезаря — це моноалфавітний шифр, або спростуйте цей вислів.

Шифр Цезаря є моноалфавітним шифром, оскільки кожна буква відображається відповідним чином на одну і ту ж букву або символ алфавіту з фіксованим зсувом.