ЗВІТ ПО ЛАБОРАТОРНІЙ РОБОТІ НОМЕР 2

ПРЕДМЕТУ КРИПТОГРАФІЯ

СТУДЕНТ: ПАНТЕЛЕЙЧУК ІЛЛЯ МИХАЙЛОВИЧ

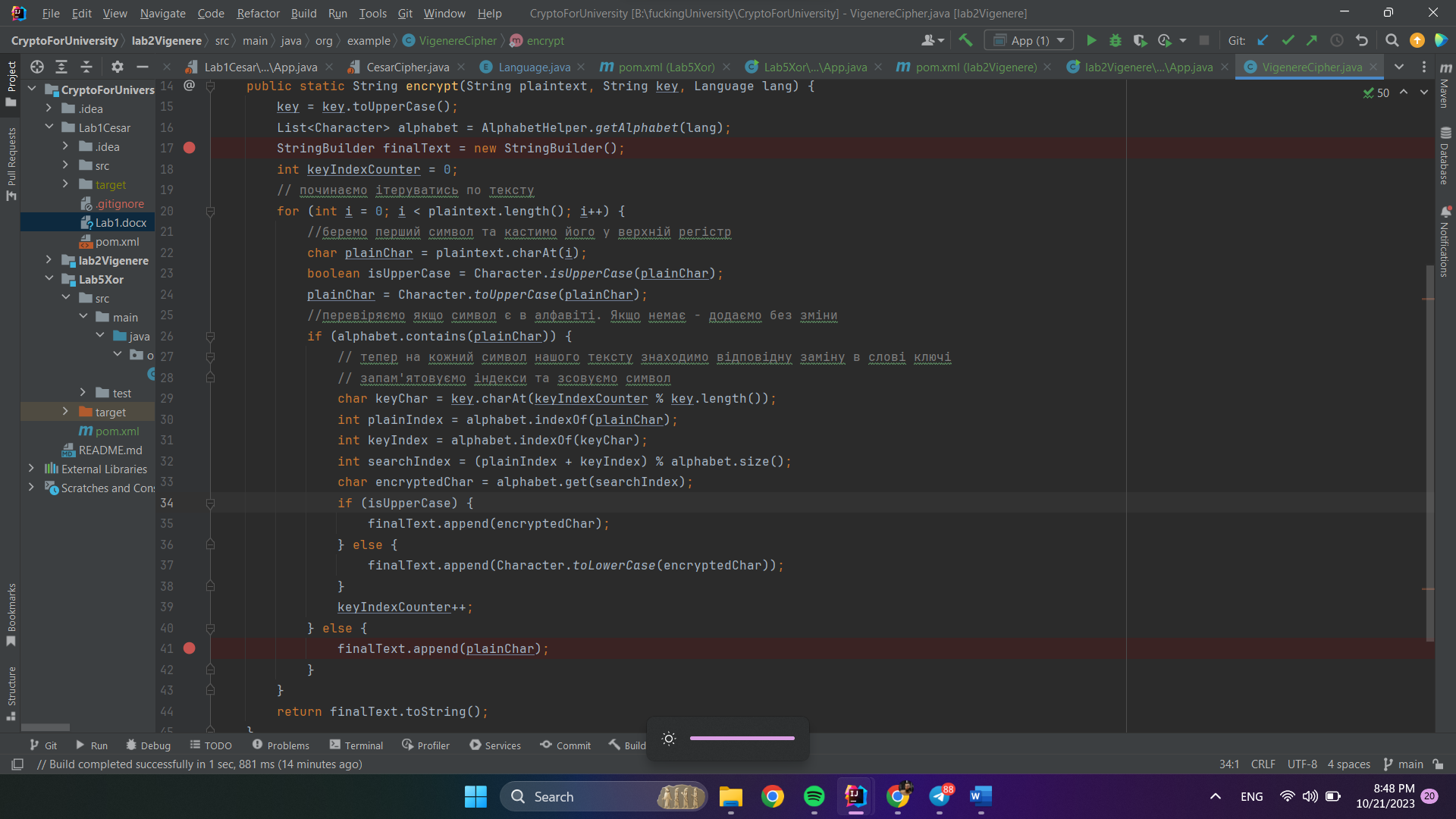
(увесь код можна подивитись на GitHub [тут](https://github.com/ilyaPanteleychuk/CryptoForUniversity))

В даній лабораторній роботі потрібно було розробити додаток який може шифрувати та дешифрувати Шифр Вегенера з одногрупником в парі.

Я виконував цю лабораторну роботу з Володимиром Лелявіном – на його стороні виконано Дешифрування на мові Kotlin, а на моїй стороні виконано шифрування на мові Java.

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

Метод який виконує шифрування



Він приймає як параметри текст для шифрування, слово-ключ для шифрування та мову для вибору алфавіту.

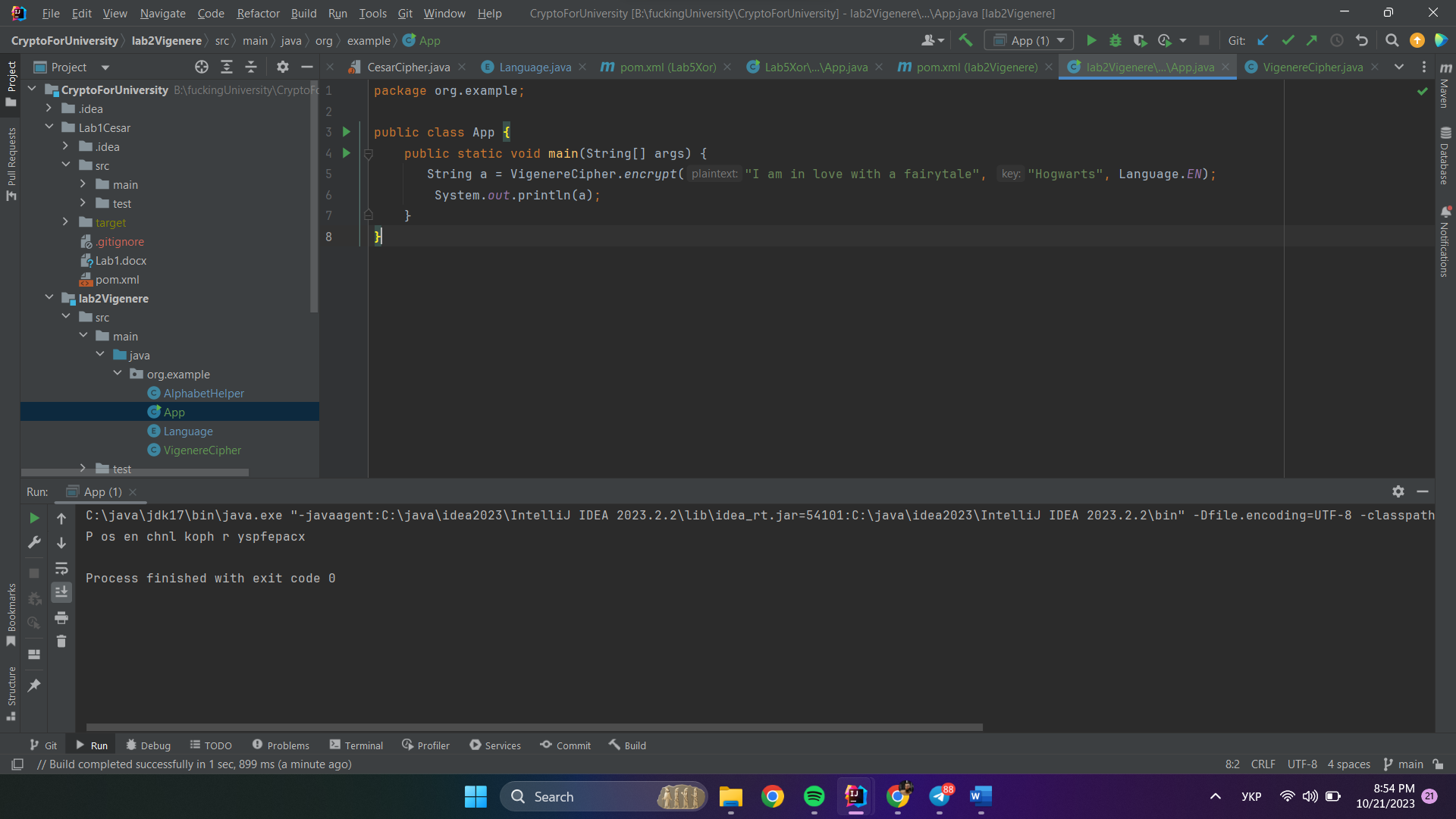
Алгоритм такий:

1. Розбиваємо текст на символи та починаємо по ним ітеруватись
2. Якщо символ є в алфавіті – підбираємо символ із слово ключа для подальшої заміни.
3. Вираховуємо позицію символу НА який потрібно змінити наш символ та дістаємо його з алфавіту.

Приклад:

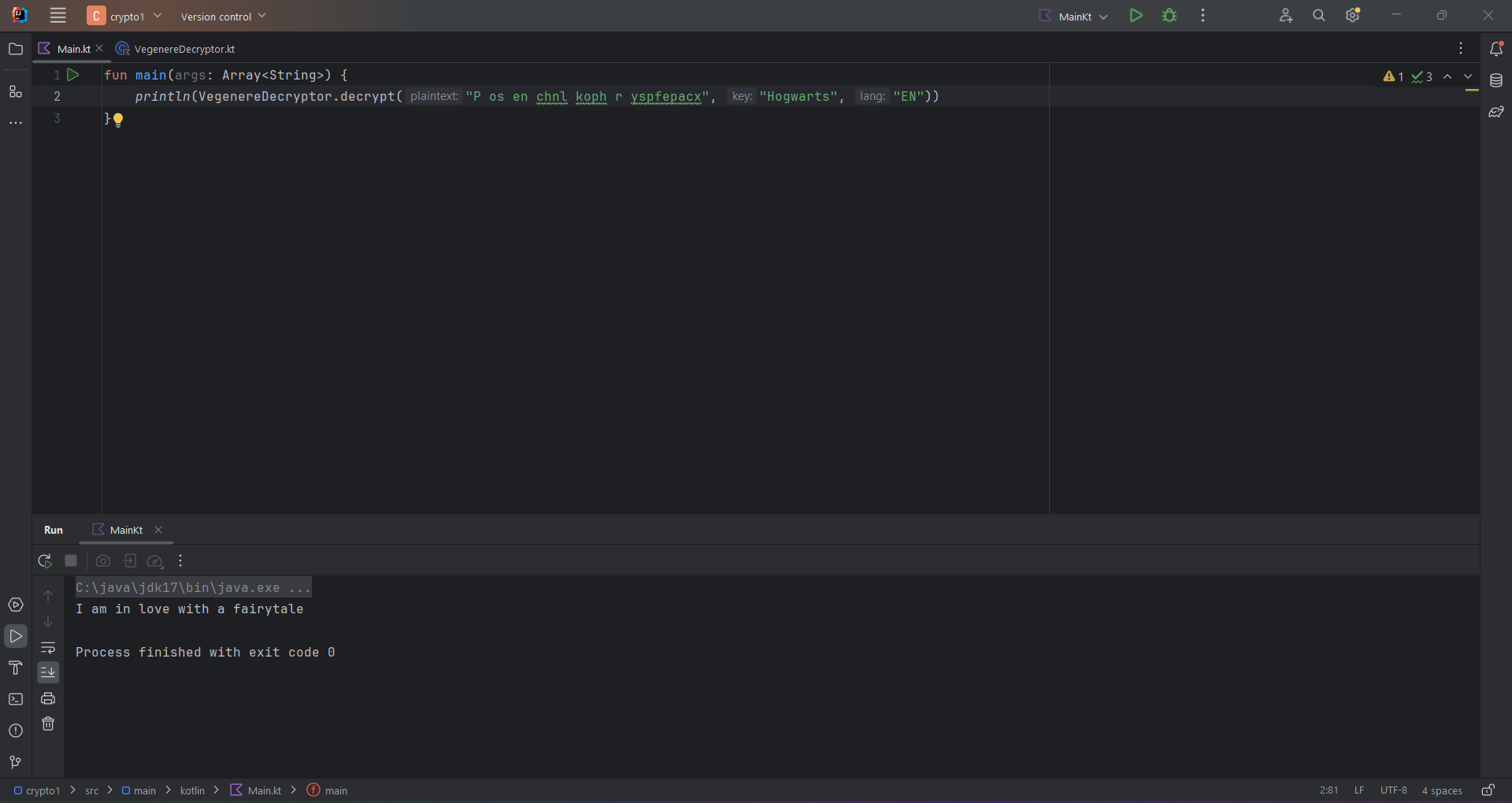
З Володимиром домовились використовувати слово-ключ Hogwarts:

Шифрую текст “I am in love with a fairytale” – на скріншоті результат.



Результат вийшов “P os en chnl koph r yspfepacx”. Надсилаємо це Володимиру та просимо його дешифрувати це.

Результат з програми Володимира нижче:



Як ми бачимо – дешифрація повернула початкове слово “I am in love with a fairytale”

ВІДПОВІДІ НА ТЕОРЕТИЧНІ ПИТАННЯ

1. До якого класу найпростіших шифрів відноситься шифр Віженера?

Шифр Віженера відноситься до поліалфавітних шифрів.

1. Як відбувається шифрування та розшифрування у шифрі Віженера?

Шифрування у шифрі Віженера відбувається шляхом послідовного зсуву символів відкритого тексту на символи ключа. Розшифрування виконується зворотним процесом - зсув символів шифртексту назад на символи ключа. Ключем в цьому шифрі є слово чи фраза, яка використовується для здійснення зсуву символів.

1. Що необхідно зробити для криптоаналізу тексту, який зашифрований шифром Віженера?

Для криптоаналізу тексту, який зашифрований шифром Віженера, потрібно спробувати визначити довжину ключа та сам ключ. Один із методів цього полягає у використанні індексу відповідності, який допомагає приблизно визначити довжину ключа. Потім можна використовувати методи частотного аналізу для кожного символу ключа та використовувати знання мови, на якій написаний відкритий текст, для полегшення дешифрування.

1. Які існують методи визначення ключа у шифротексті?

Існує кілька методів визначення ключа у шифротексті шифру Віженера, таких як методи касиского та Фрідріхсена, а також використання індексу відповідності та статистики букв. Деякі методи базуються на аналізі частоти повторюваних послідовностей символів у шифртексті для визначення довжини ключа. Потім можна використовувати методи частотного аналізу для визначення самого ключа.