Створимо приватний ключ командою:

Триває вставлення зображення...genrsa - параметр вказує створення ключа алгоритмом шифрування RSA.

out – де створити ключ.

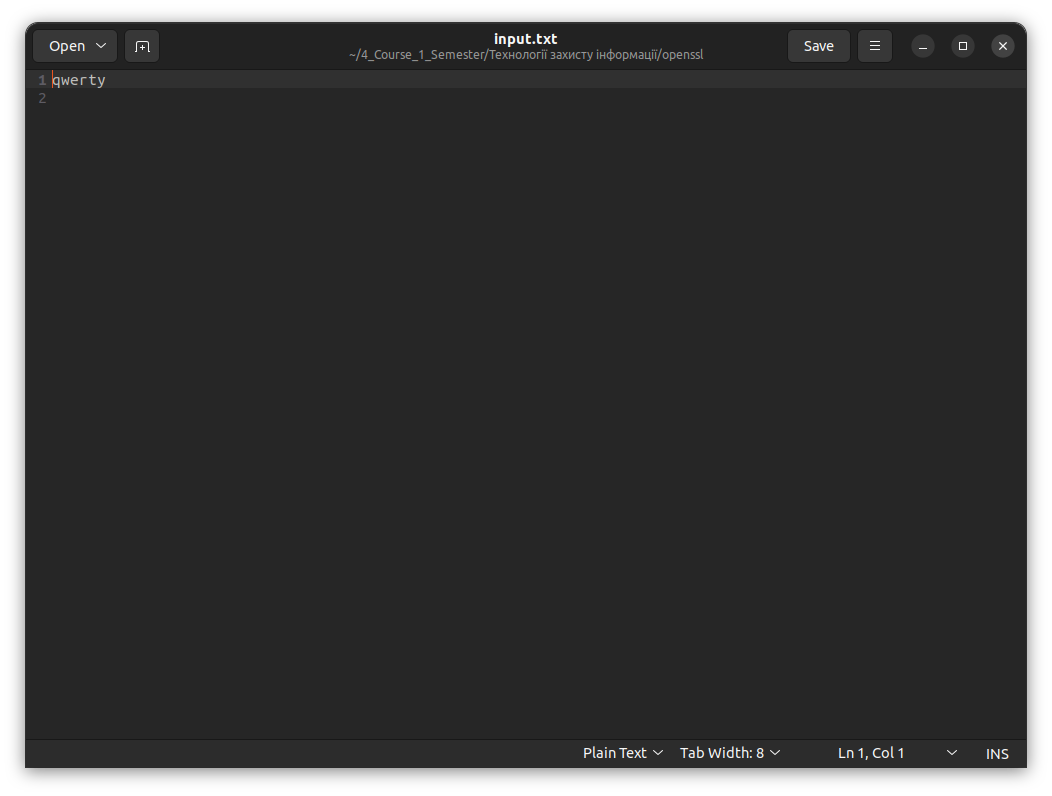
4096 - Довжина ключа.

aes-256-cfb - алгоритм та режим шифрування ключа.

rand ./dummyText.txt— рандомне значення будь-якої папки.

На його основі зробимо публічний:

Триває вставлення зображення...Для шифрування маємо файл input.txt:



Створимо симетричний сесійний (одноразовий) ключ рандомною послідовністю символів та запишемо у файл у поданні base64:



Далі зашифруємо файл цим ключем:



Далі зашифруємо симетричний ключ нашим публічним асиметричним ключем:



Тепер видалимо початковий симетричний ключ, щоб ніхто ніколи не знайшов його:

Триває вставлення зображення...

Тепер розшифруємо симетричний ключ нашим приватним асиметричним ключем:



І тепер ми можемо розшифрувати наш зашифрований файл за допомогою симетричного ключа:

