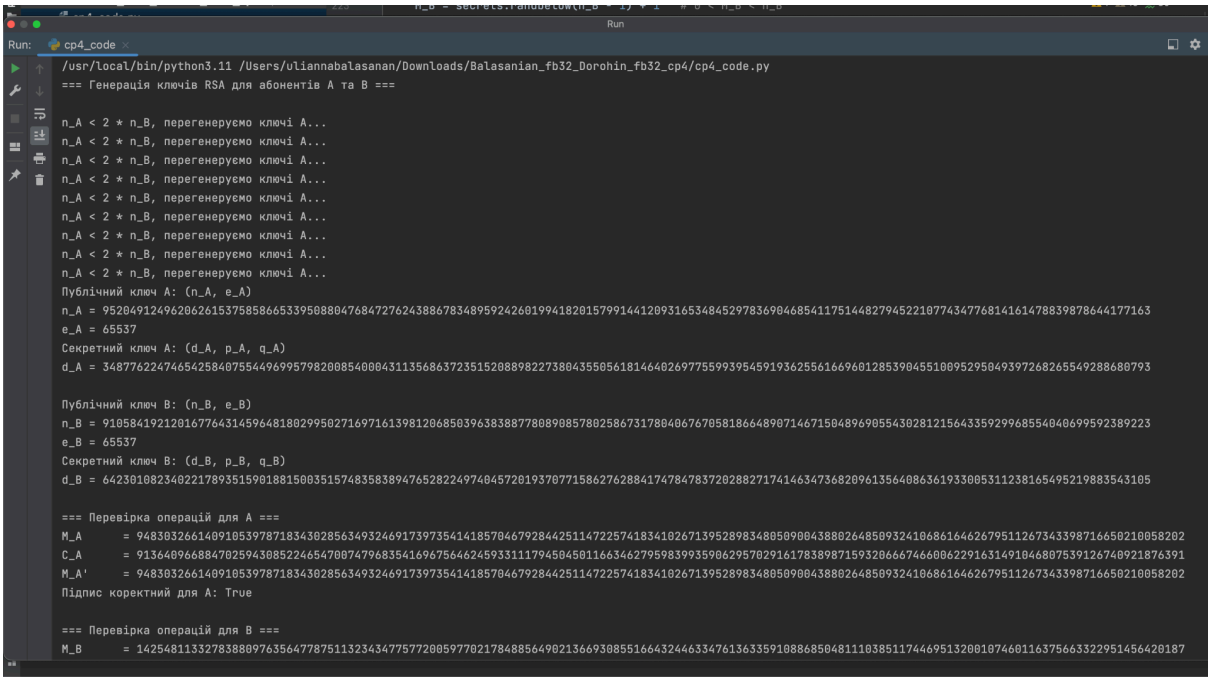
Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

Криптографія

Комп’ютерний практикум №4

Вивчення криптосистеми RSA та алгоритму електронного підпису, ознайомлення з методами генерації параметрів асиметричних криптосистем

Виконали:
Студенти 3 курсу
ФБ-32 Баласанян Юліана та
ФБ-32 Дорогін Артем



Висновок: у ході роботи було реалізовано повну схему RSA: генерацію випадкових простих чисел, побудову відкритих і закритих ключів, шифрування та розшифрування, формування і перевірку цифрового підпису, а також протокол конфіденційного передавання сесійного ключа