**DEPENDABLE AND SECURE AI-ML (AI60006)**

**Session 2022-2023**

**Assignment 2**

**Problem Description:** You have been given two GitHub links. Run the python code and do the following:

1. Take a screenshot of your outputs and record the timing required to compute the Federated Learning process.
2. Following the similar adequate partial homomorphism in encryption (as discussed in the class and given in the code), implement privacy-preserving SVM assuming public model private data scenario (data in encrypted but model parameters are unencrypted):

Links to the GitHub code:

<https://github.com/data61/python-paillier/blob/master/examples/alternative_base.py>

<https://github.com/data61/python-paillier/blob/master/examples/federated_learning_with_encryption.py>

You have to submit a document containing the implementation details, platform details, output screenshot, and final timing details for a single prediction. Use either python code or .ipynb notebook to show your implementation. For naming convention, you can use <ROLLNO\_2>.

**Note**: The assignment has to be submitted individually.