Assignment 3

In this practice, we will predict the class of an EMNIST image from an encrypted MLP that only contains two hidden layers and is encrypted by the CKKS scheme.

q1. (60%) Encrypt a simple MLP and feed an EMNIST image to the model.

1. Download the plaintext weights given by the TA.
2. Encrypted the weights by the CKKS Scheme with parameter:
    - poly_modulus_degree = 8192
    - coeff_mod_bit_sizes = [40, 20, 20, 20, 40]
    - global_scale = 2^{20}
3. **Build** an encrypted MLP by TenSEAL operations with the model structure
    - input (16x16, please use `transforms.Resize(16)` to resize the image) → flatten (256) → fully connected layer (256, 32) → x^2 activation function (32)→ fully connected layer (32, 10)
4. **Compare** the output of the encrypted model and regular model. The output is a vector with 10 dimensions.
5. **Report** your results in q3

q2. (10%) Reduce the noise introduced by modifying the parameters of the CKKS scheme. **Report** your finding in q3.

```
class MLP(nn.Module):
    def __init__(self, input_dim, output_dim):
        super().__init__()
        self.input_fc = nn.Linear(input_dim, 32)
        self.output_fc = nn.Linear(32, output_dim)

    def forward(self, x):
        batch_size = x.shape[0]
        x = x.view(batch_size, -1)
        x = self.input_fc(x)
        x = x * x # activation function
        y_pred = self.output_fc(x)
        return y_pred
```

The accuracy will **not** affect the score, while please provide a detailed description of your implementation and methods in **q3**.

Note: Please use `transforms.Normalize(mean=[0.1307], std=[0.3081])` to normalize the input tensor.

q3. (30%) Write down your implementation details and experiment in English.

The font size is 12, and the page limit is 3 pages.

Submission Guideline

Please submit your report named `{SID}_a3.pdf` (SID in upper case) to the COOL System, such as `D111111_a3.pdf`

Supplementary Materials
PyTorch installation: https://pytorch.org/
Package the tutorials:
https://github.com/OpenMined/TenSEAL/blob/main/tutorials/Tutorial%200%20-%20Getting%20Started.ipynb