Assignment 2

q1. (15%) Install and play with the **PyTorch** package

q2. (25%) MLP Training

1. Train an MLP with the given model structure and the default training set provided by the torchvision MNIST dataset
2. Store the predicted labels in an array in the same order as the default testing set
3. Encrypt the array using the TenSeal BFV scheme
4. Export pickle object containing the encrypted array and the secret key (context). For more details related to the format, please see the submission guideline

```
class MLP(nn.Module):
    def __init__(self, input_dim, output_dim):
        super().__init__()

        self.input_fc = nn.Linear(input_dim, 250)
        self.hidden_fc = nn.Linear(250, 100)
        self.output_fc = nn.Linear(100, output_dim)

    def forward(self, x):
        # x = [batch size, height, width]
        batch_size = x.shape[0]
        x = x.view(batch_size, -1)
        # x = [batch size, height * width]
        h_1 = F.relu(self.input_fc(x))
        # h_1 = [batch size, 250]
        h_2 = F.relu(self.hidden_fc(h_1))
        # h_2 = [batch size, 100]
        y_pred = self.output_fc(h_2)
        # y_pred = [batch size, output dim]
        return y_pred
```

The accuracy of **q2** will **not** affect the score, while please provide a detailed description of parameter settings and implementation in **q4**.

q3. (45%) MLP Weight Applying

1. Download the model weights and your testing images from here
2. Construct the NN class (same structure as **q2**) and apply the model weights
3. Forward the testing images
4. Concatenate all `y_pred` into one flattened array
5. Encrypt the flattened array using TenSeal CKKS scheme

The encrypted outputs will be compared to the corresponding outputs generated by the given model.
Please make sure the errors(noises) are **lower than 0.01** by setting the appropriate global scaling factor.

q4. (15%) Write down your experiment setting in English. The setting should include but not limit to (1) hardware specification, (2) package version, and (3) all the experiment parameters and details in **q2** and **q3**.

The font size is 12, and the page limit is 1 page.

Submission Guideline

Please compress your files named `{SID}_a2.zip` (SID in upper case) to the COOL System, such as `D111111_a2.zip`, with two required files

file 1. `{SID}_a2.pkl`

Please store your outputs of **q2** and **q3** as follows.
Notes: To dump the pickle object, all objects must be serialized first.

```
result = {
  'q2_key': q2_context.serialize(save_secret_key=True),
  'q2_result': q2_ciphertext.serialize(),
  'q3_key': q3_context.serialize(save_secret_key=True),
  'q3_result': q3_ciphertext.serialize()
}
```

files 2. `{SID}_a2_report.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