Project 4

PRNG Classification

Due date: April 14

The aim of this project is to train a PRNG (pseudo random number generator) Classifier which is trained to distinguish the generator of a given pseudo random number (PRN).

60,000 32-bit (64 and 128) output generated by 8 different stream ciphers is given in a file as a training data set.
And a separate 10,000 32-bit (64 and 128) output is also given as a validation set. There is also another test set consisting 10,000 32-bit (64 and 128) outputs to test the trained models. **Note that,** if your training algorithm does not require validation set, you can use it as a part of your training dataset.

In this assignment, your aim is to train a model which predicts the generator of a given PRN with high confidence. The list of models is given below.

Four ML algorithms are given to train (**CNN, SVM, kNN, Decision Tree**). In addition to the given algorithms, you are also supposed to choose another ML algorithm to classify the given data. Please keep in mind that training of CNN may take much longer than the others.

You should report how you train your model including your code. Please also include the **accuracy** results for training, validation and test datasets.

The following list is for your information.

ID	PRNG
1	CryptMT
2	Dragon
3	HC
4	NLS
5	Rabbit
6	Salsa20
7	Sosemanuk
8	LEX