Pseudo Random Functions(PRF)

Sarthak Mahajan, 2018111005

March 7, 2022

1 Code structure:

- This folder contains prf.py and run.py code files
- prf.py contains the code to create a PRF output
- run.py is used to take inputs and return outputs to the PRF

2 Instructions to run the code:

- Run the following command in the folder where this document is contained: python3 run.py
- There will be prompts asking you to input the relevant information serially, and will return the output.

3 Explanation of Functions in run.py:

3.1 run():

- It asks for inputs of the key, key length in binary, seed to the PRF(all in decimal format)
- Calculates p: the order of the group for DLP and g: the generator of this group.
- prints the output of the PRF

4 Explanation of Functions in prf.py:

4.1 PRF(r, k, key_len,p,g):

- p,g are in decimal format, they are needed to be passed to the dlp function. p is the largest prime possible in n bits, where n= length of the key, g is a random number in the range(1,p-1); note that this is fixed for the program in terms of p(so that same seed gives same value for different iterations of the program), but it could be any random number in the given range.

- all inputs are decimal numbers, r is the seed to the PRF, k is the key, key_len is the length of the key in binary format.
- Returns a PRF of the above input in binary format.
- Uses PRG and pad functions.