Applied Cryptography: Homework 8

(Deadline: 2:30pm, 2022/05/04)

Justify your answers with calculations, proofs, and programs.

1. (25 points) Calculate the probability that $Fermat(n)$ outputs the wrong result for $n = 2821$.
2. (25 points) Calaulate the L_n in Miller-Rabin test for $n = 2821$.