Design Document of Assignment 5

CSE 13S

Professor Darrell Long

Zihua Li

February 16, 2023

The Schmidt-Samoa Algorithm

The public key is $N = p^2 \cdot q$, and we are calculating $d = \text{inv}\big(N, \varphi(pq)\big)$ as the private key, in which p and q, their values are up to us, but they should be a large integer.

decrypt.c: It should be embedded with the private key or have access to the private in order to decrypt the ciphertext.

encrypt.c: It should be using the keygen.c to get a public key and encrypt the plaintext.

keygen.c: It should generate public key as required.

numtheory.c: It should have the number theory functions.

numtheory.c: It should have the headers here.

randstate.c: random state interface of SS library.

randstate.h: random state interface of SS library headers.

ss.c: SS library

ss.h: SS library headers.