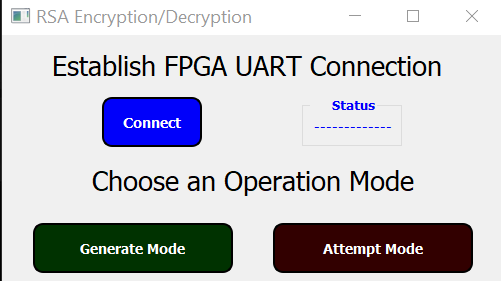
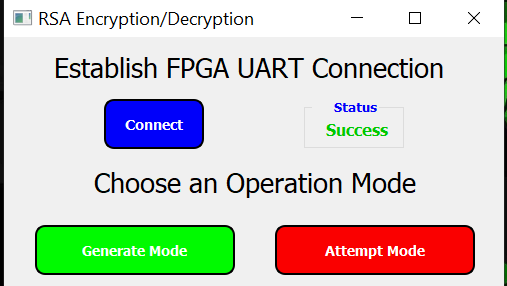
**FPGA RSA GUI GUIDE**

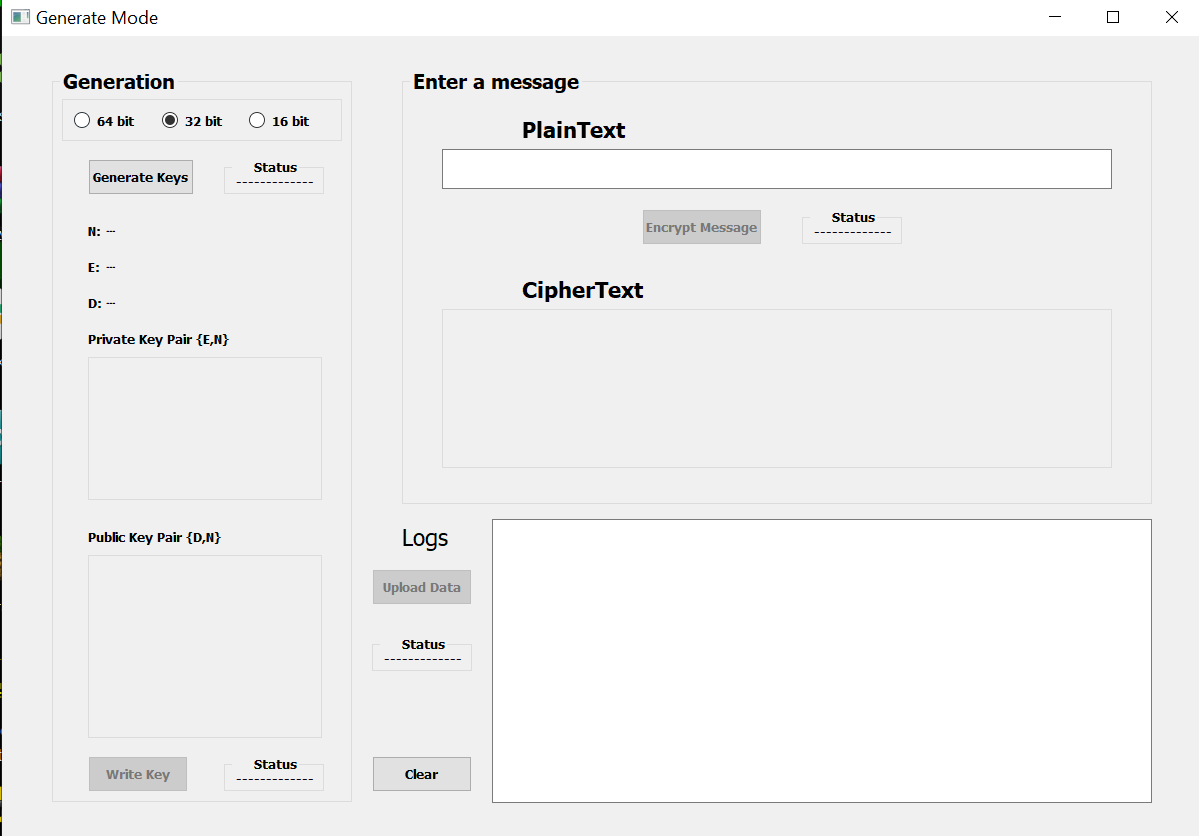


First, we establish UART communications with the RSA FPGA

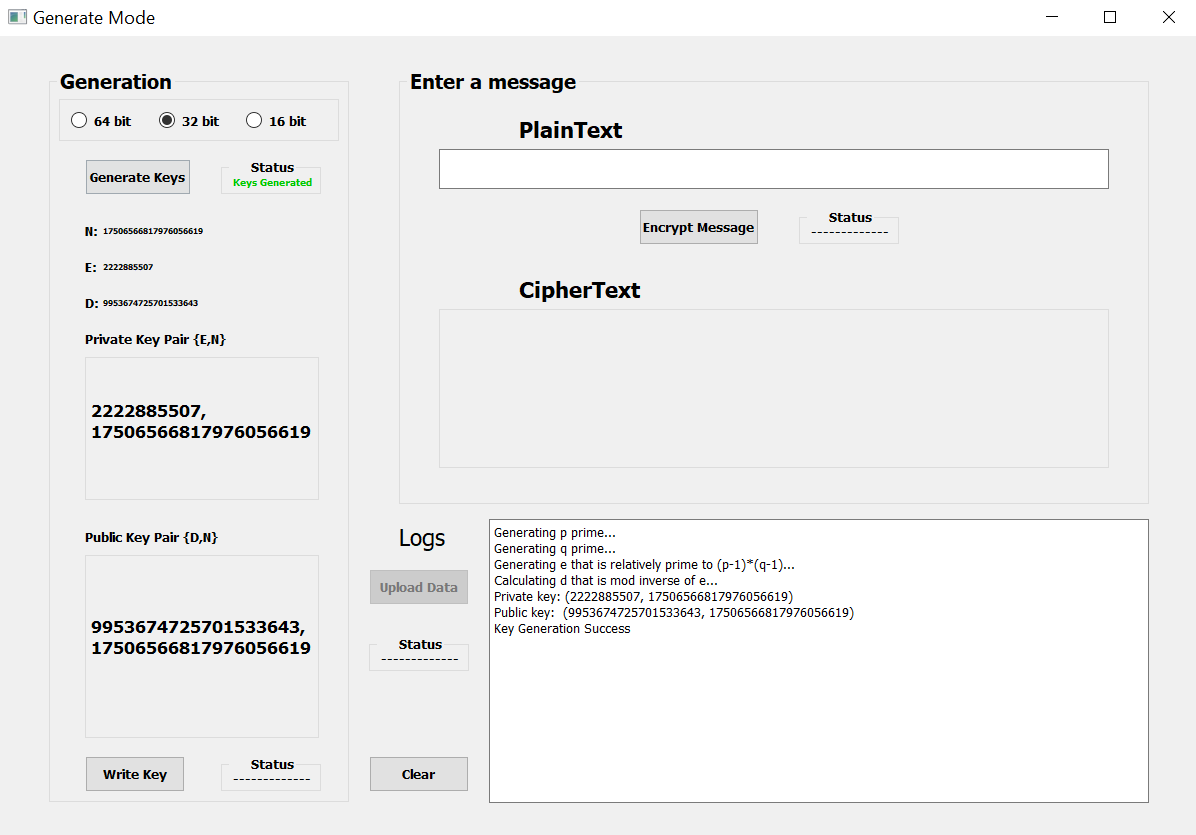


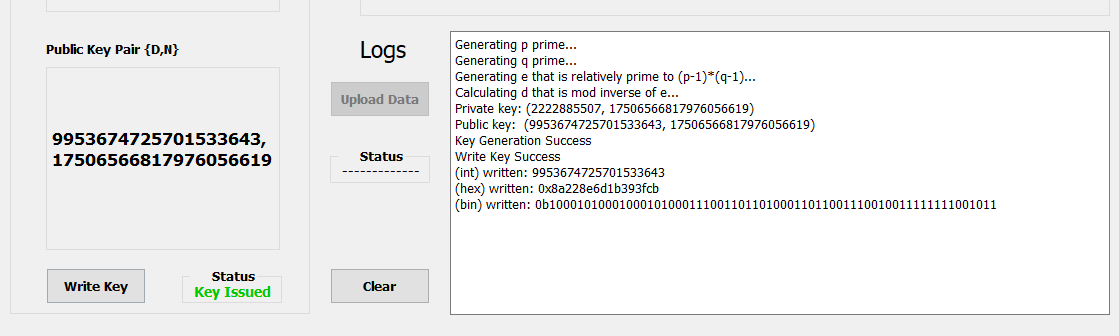
Then the mode buttons get activated

“Generate Mode” Where the keys are generated and the plaintext is encrypted with the private key, and the public keys is printed onto a rfid key

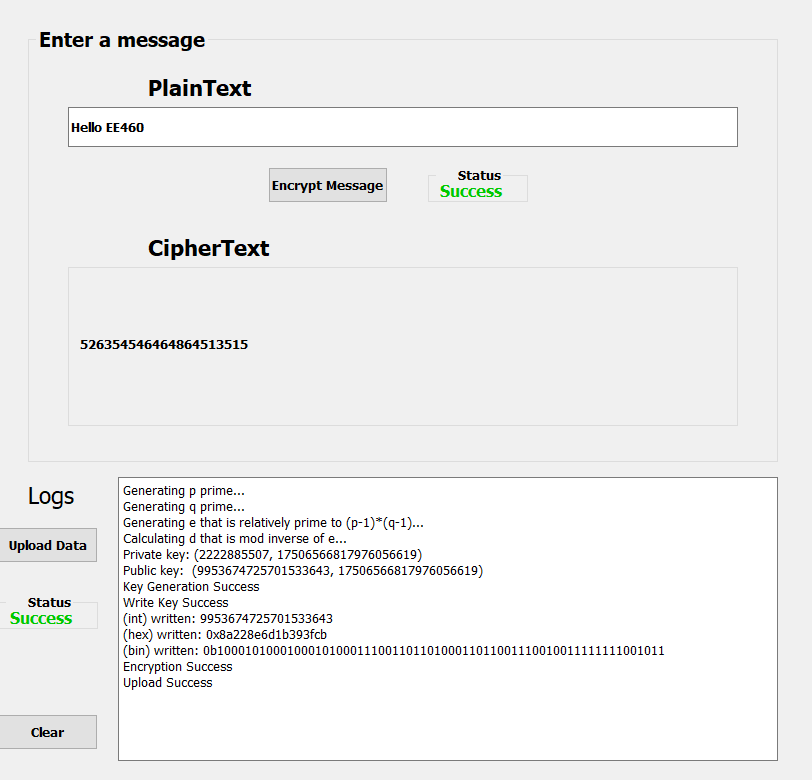
The Generate window

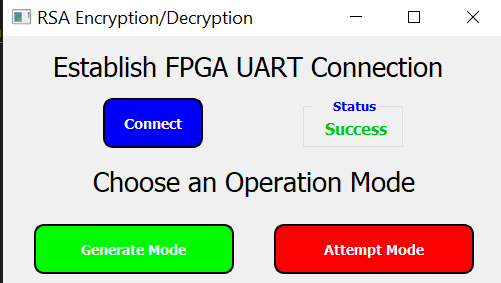
We choose the prime numbers bit size from the radio buttons

Clicking “Generate keys” Button creates the key pairs needed



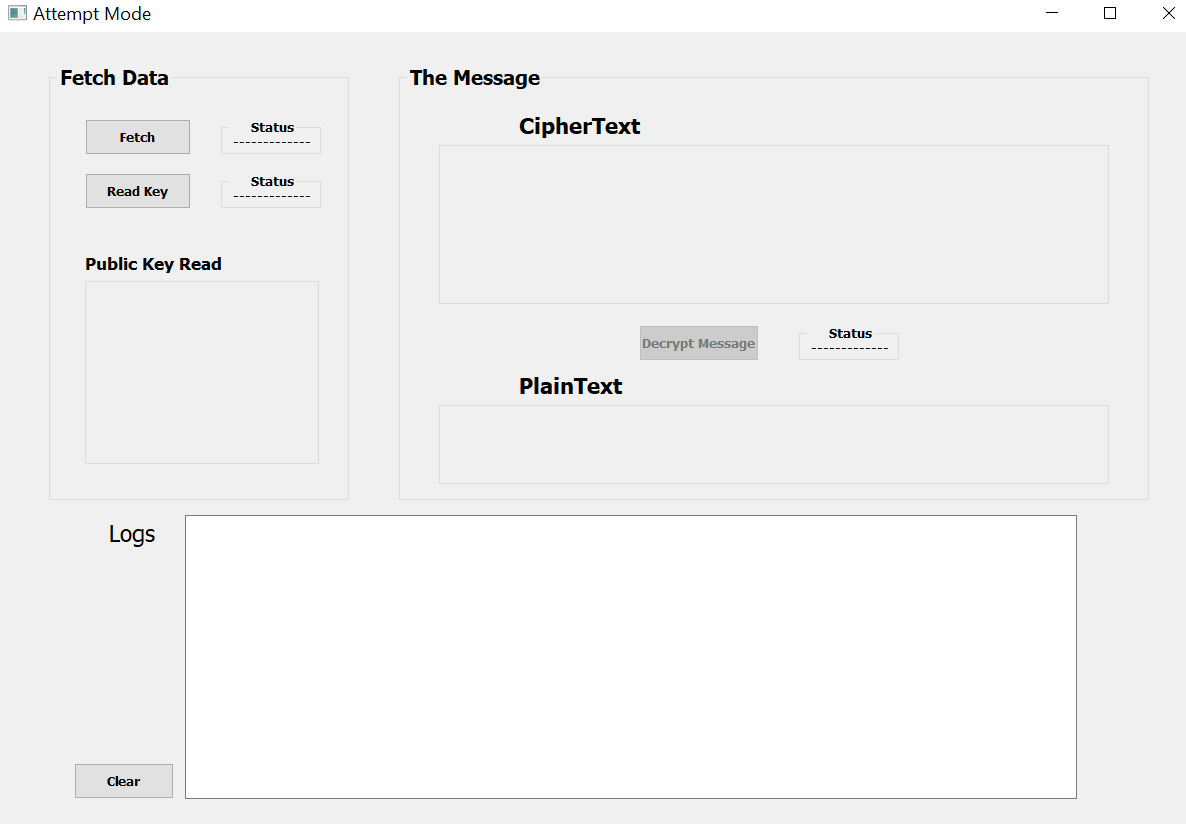
Pressing “Write Key” when placing an RFID Tag over the Writer encodes the public key onto it

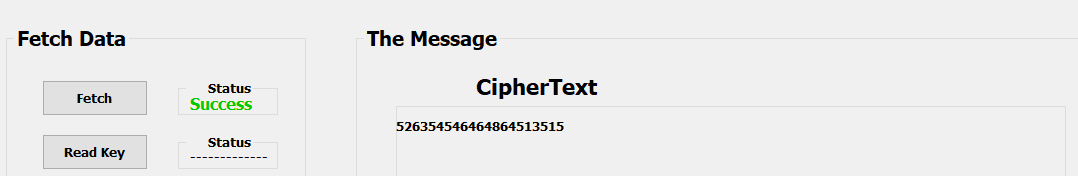
Finally we can enter our desired plaintext, and press “Encrypt” which will transfer its integer value over to the FPGA to be Encrypted. Then we can press “Upload Data” Button to post our ciphertext on the cloud



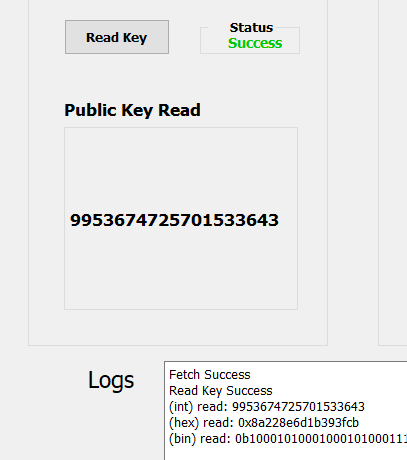
Now for attempt mode, we can go over to another computed and do the same steps for establishing UART comm w FPGA

Attemp Window

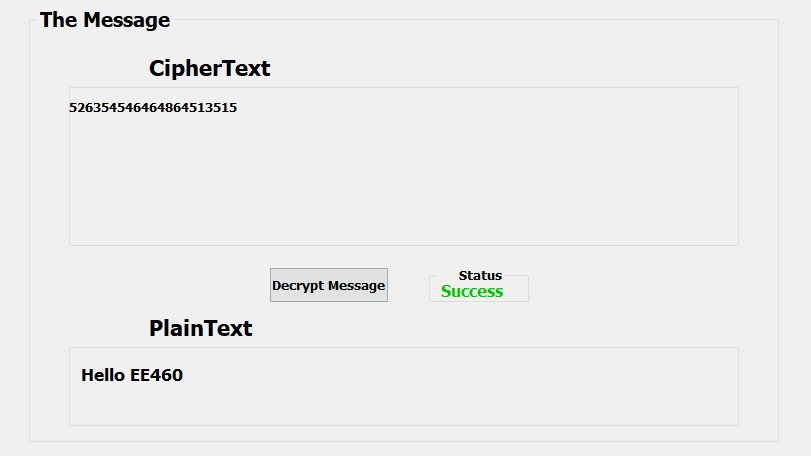




pressing “Fetch” will fetch the ciphertext from the cloud and display it



Pressing “Read Key” when placing an RFID Tag over the Reader decodes the public key on it



Finally with the public key at hand and the ciphertext, we can decrypt our message by sending the data over to the FPGA and receive back the integer which will be converted to a readable string plaintext