API Flow Chart

Lockdown initiated. — pit/lock() ①

pit_keygenstate **uses elliptic curve cryptography to generate a public and private key pair.** — pit_crypto/pit_keygenstate() ②

keyexchangestate **sends the user's public key to a server, and receives the server's public key.** — pit_i2c/keyexchangestate() ③

④ **Send device public key**

⑤ **Receive server's public key**

Server

pit_secretkey **generates a shared secret key using the server's public key and the Cerberus's private key. The server will do the same, resulting in a shared secret key, completing the ECDH process. System is now locked.** — pit_crypto/pit_secretkey() ⑥
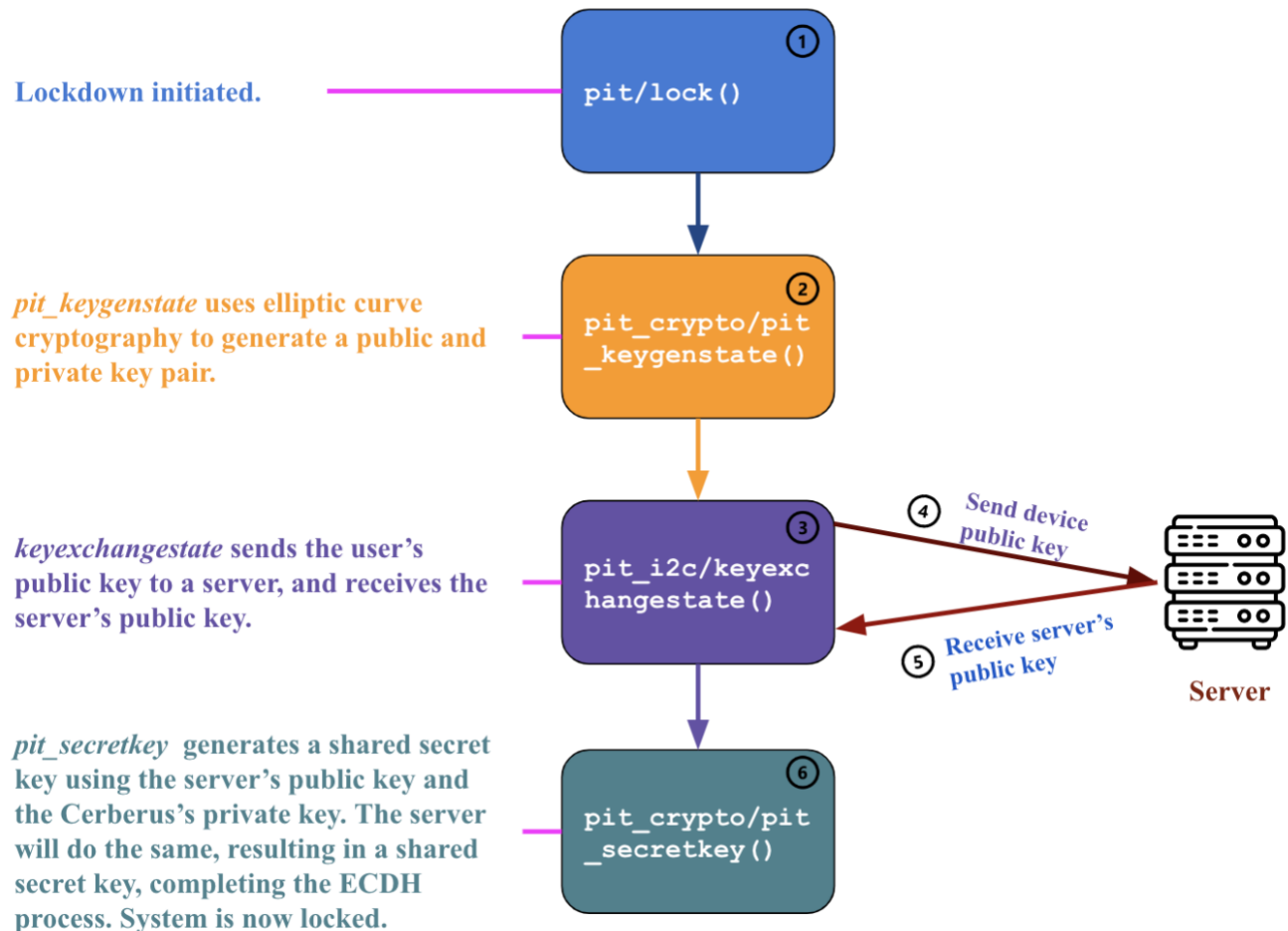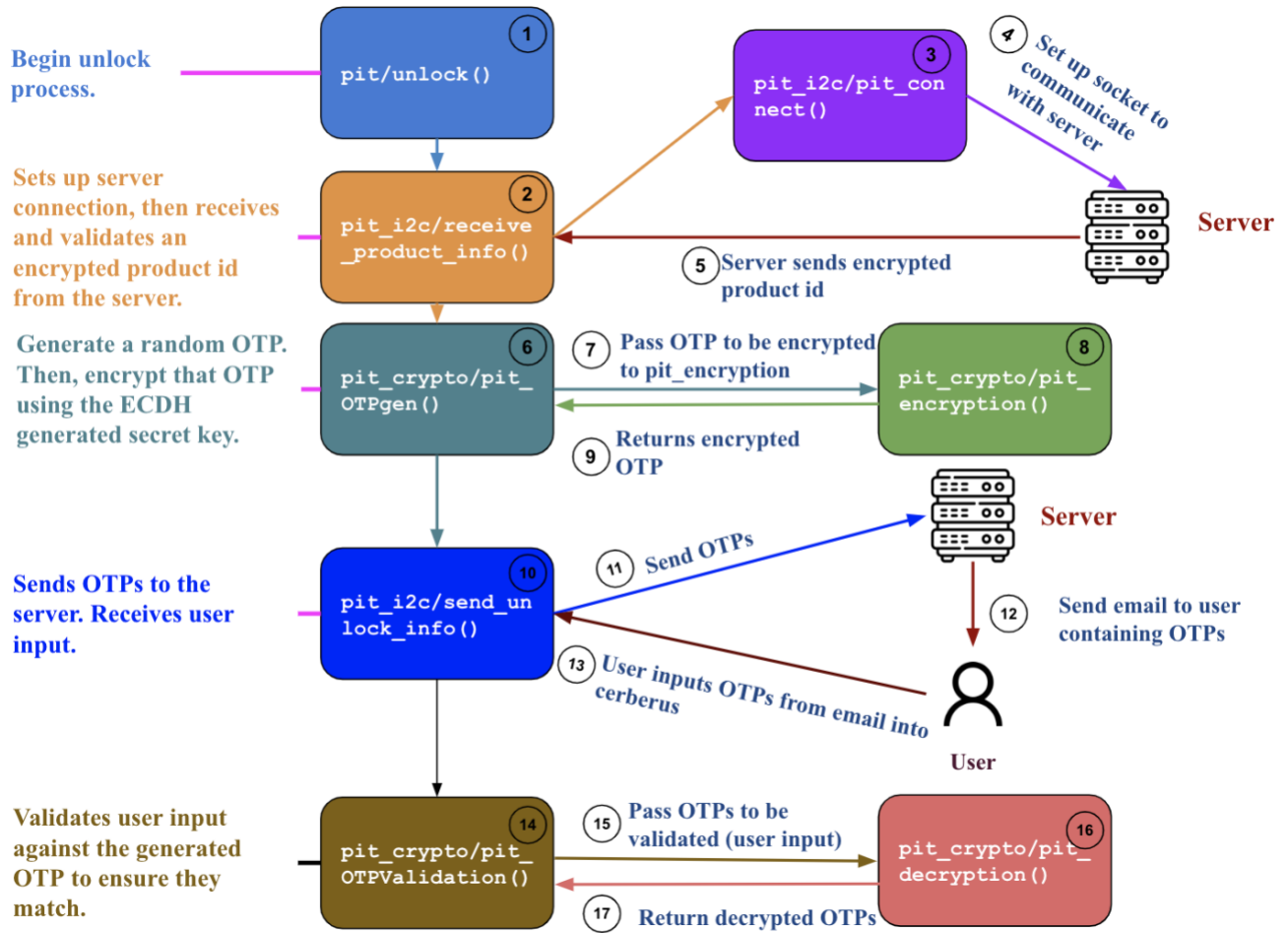
Figure 1: API Lock Flowchart

Figure 2: API Unlock Flowchart