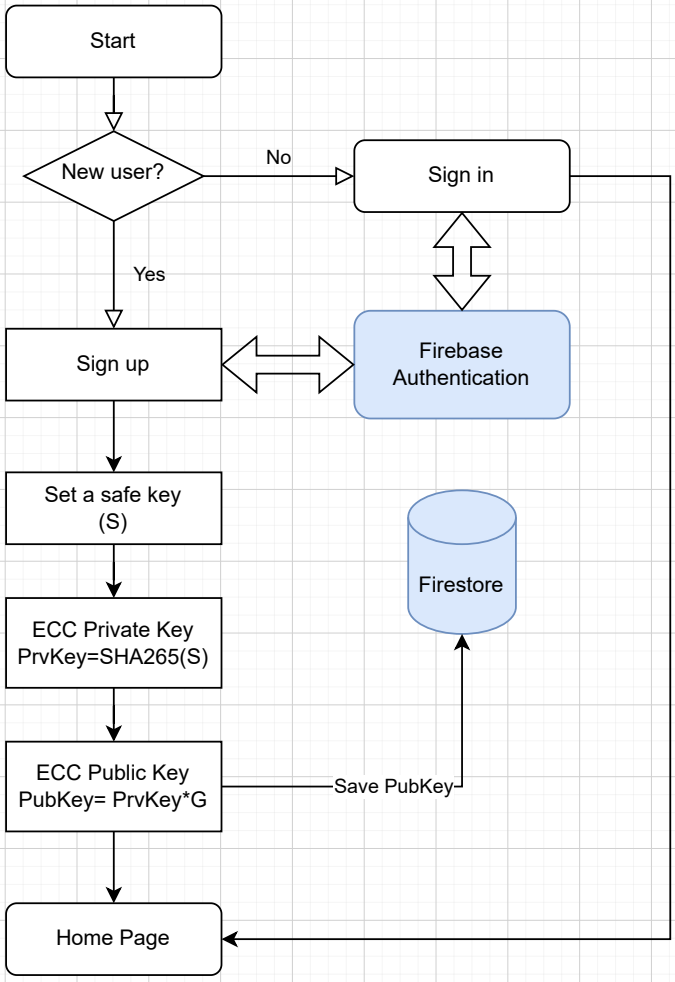
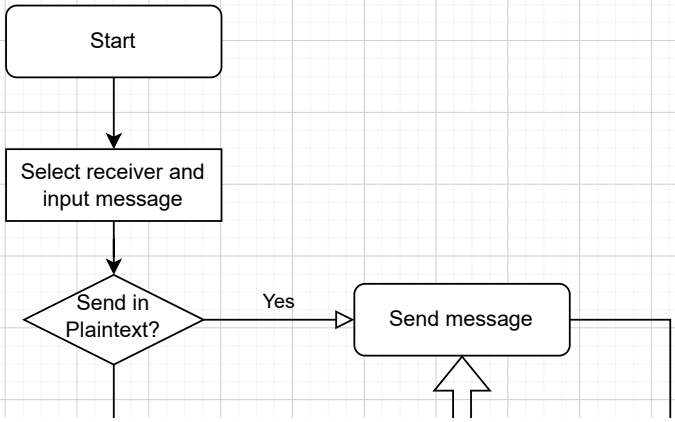
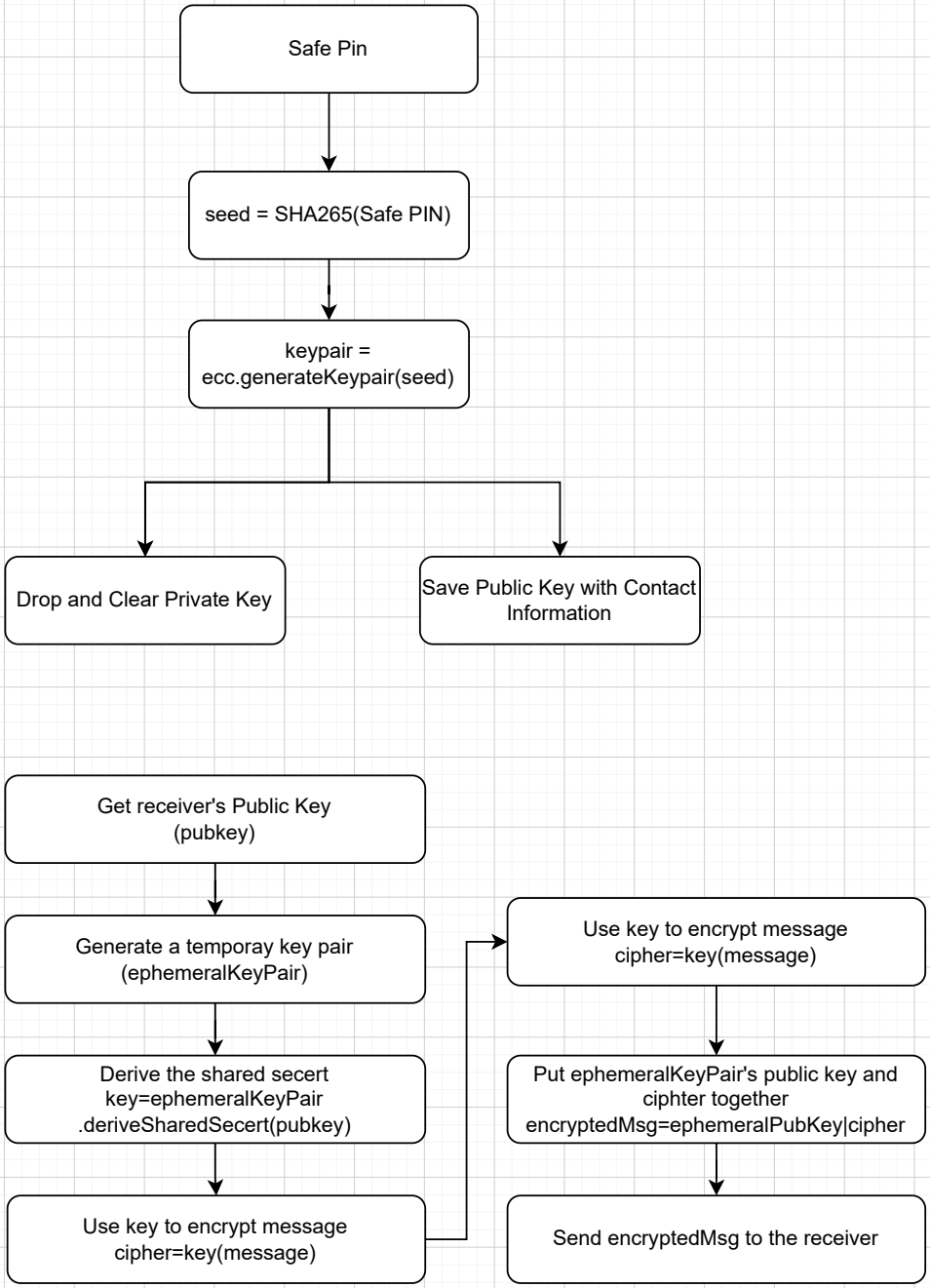
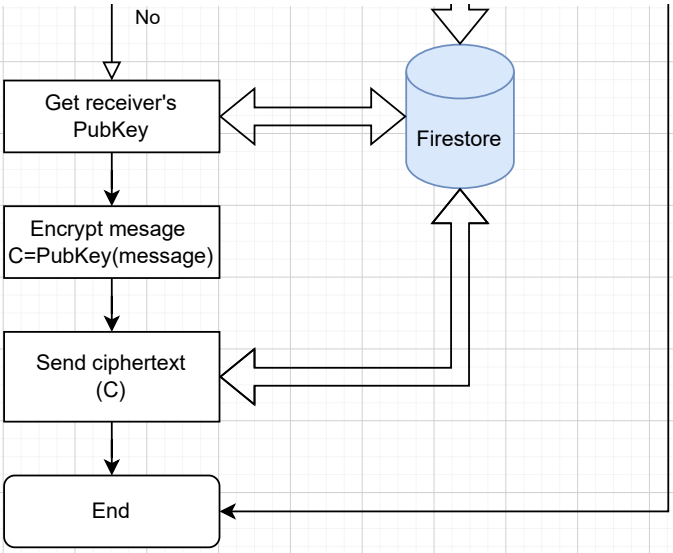
User Sign Up/Sign In



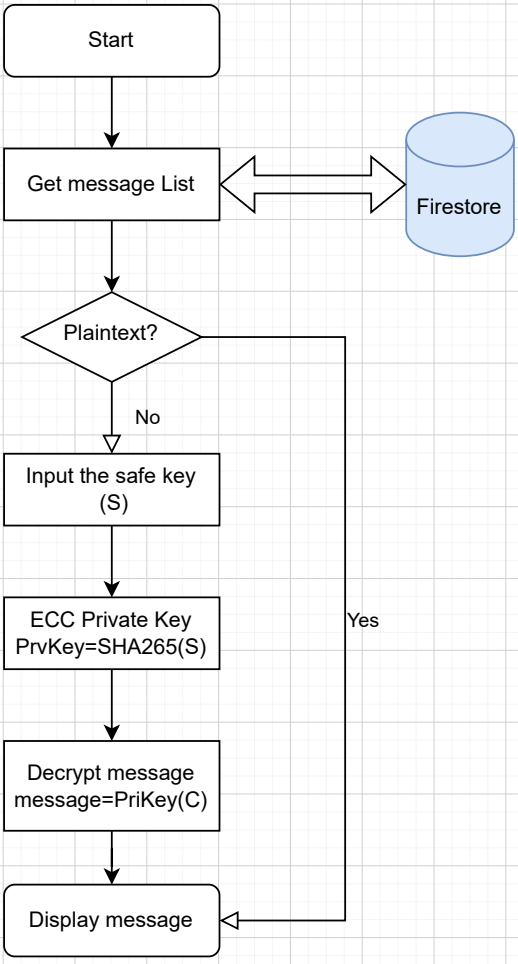
Send Message

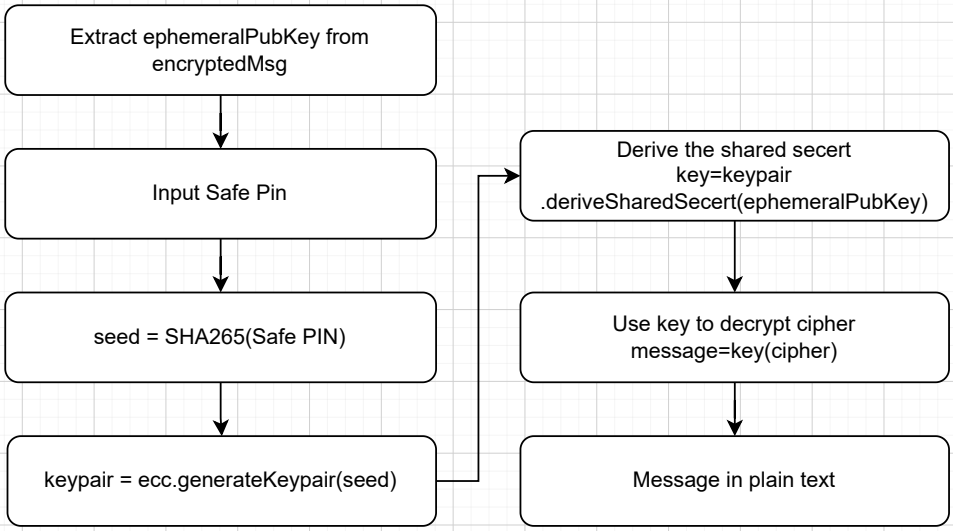



Safe Pin
seed = SHA265(Safe PIN)
keypair = ecc.generateKeypair(seed)
Drop and Clear Private Key
Save Public Key with Contact Information
Get receiver's Public Key (pubkey)
Generate a temporay key pair (ephemeralKeyPair)
Derive the shared secert key=ephemeralKeyPair .deriveSharedSecert(pubkey)
Use key to encrypt message cipher=key(message)
Use key to encrypt message cipher=key(message)
Put ephemeralKeyPair's public key and ciphter together encryptedMsg=ephemeralPubKey|cipher
Send encryptedMsg to the receiver



Read Message




Extract ephemeralPubKey from encryptedMsg
Input Safe Pin
seed = SHA265(Safe PIN)
keypair = ecc.generateKeypair(seed)
Derive the shared secert key=keypair .deriveSharedSecert(ephemeralPubKey)
Use key to decrypt cipher message=key(cipher)
Message in plain text