Modules

There are three modules that are used extensively in the implementation of this project: cryptolib, netlib, and serverlib. Each module has its own collection of methods used for different purposes.

Cryptolib

The cryptolib module is used for all of the methods regarding the encryption process.

- public_key_hash
  - Parameters:
    - `RSAPublicKey` key
  - Return Type:
    - `str`
  - Description:
    - Takes an `RSAPublicKey` object and returns the SHA256 hash of its bytes in string form.
- rsa_decrypt
  - Parameters:
    - `RSAPrivateKey` key, `bytes` ciphertext
  - Return Type:
    - `bytes`
  - Description:
    - Decrypts the ciphertext with the `RSAPrivateKey` and returns the resulting message.
- rsa_encrypt
  - Parameters:
    - `RSAPublicKey` key, `bytes` message
  - Return Type:
    - `bytes`
  - Description:
    - Encrypts the message with the `RSAPublicKey` and returns the resulting ciphertext.
- rsa_sign
  - Parameters:
    - `RSAPrivateKey` key, `bytes` message
  - Return Type:
    - `bytes`
  - Description:
    - Returns the `PSS` signature of the message with the `RSAPrivateKey`.
- rsa_sign_string
  - Parameters:
    - `RSAPrivateKey` key, `str` message
  - Return Type:
    - `bytes`
  - Description:
    - Returns the `PSS` signature of the message in string form with the `RSAPrivateKey`.
- rsa_verify
  - Parameters:
    - `RSAPublicKey` key, `bytes` signature, `bytes` message
  - Return Type:
    - `bool`
  - Description:
    - Verifies a `PSS` signature of a message with the `RSAPublicKey`. Returns `True` if the signature is verified, and returns `False` otherwise.
- rsa_verify_str
  - Parameters:
    - `RSAPublicKey` key, `bytes` signature, `bytes` message
  - Return Type:
    - `bool`
  - Description:
    - Verifies a `PSS` signature of a message in string form with the `RSAPublicKey`. Returns `True` if the signature is verified, and returns `False` otherwise.
- rsa_decrypt
  - Parameters:
    - `RSAPrivateKey` key, `bytes` ciphertext
  - Return Type:
    - `bytes`
  - Description:
    - Decrypts the ciphertext with the `RSAPrivateKey` and returns the resulting message.
- symmetric_decrypt
  - Parameters:
    - `bytes` key, `bytes` ciphertext
  - Return Type:
    - `bytes`
  - Description:
    - Decrypts the ciphertext with the `AES` key in `CBC` block mode and returns the resulting message.
- decrypt_dict
  - Parameters:
    - `bytes` key, `bytes` ciphertext
  - Return Type:
    - `dict`
  - Description:

        - Decrypts the ciphertext with the `AES` key in `CBC` block mode and returns the resulting `dict`.
- symmetric_encrypt
    - Parameters:
        - `bytes` key, `bytes` message
    - Return Type:
        - `bytes`
    - Description:
        - Encrypts the message with the `AES` key in `CBC` block mode and returns the resulting ciphertext.
- encrypt_dict
    - Parameters:
        - `bytes` key, `dict` message
    - Return Type:
        - `bytes`
    - Description:
        - Encrypts the `dict` with the `AES` key in `CBC` block mode and returns the resulting ciphertext.

Netlib

The netlib module is used for all of the methods involving sending and receiving data from a socket and converting data types.

- get_dict_from_socket
    - Parameters:
        - `socket` sock
    - Return Type:
        - `dict`
    - Description:
        - Receives a packet from sock and returns it as a `dict`.
- send_dict_to_socket
    - Parameters:
        - `dict` packet, `socket` sock
    - Return Type:
        - `None`
    - Description:
        - Converts a packet to `bytes` and sends it to sock
- bytes_to_int
    - Parameters:
        - `bytes` b
    - Return Type:
        - `int`
    - Description:
        - Converts a `bytes` object to its equivalent `int` representation.
- int_to_bytes
    - Parameters:
        - `int` i
    - Return Type:
        - `bytes`
    - Description:
        - Converts an `int` object to its equivalent `bytes` representation.
- bytes_to_b64
    - Parameters:
        - `bytes` b
    - Return Type:
        - `str`
    - Description:
        - Converts a `bytes` object to its equivalent base 64 representation in string form.
- b64_to_bytes
    - Parameters:
        - `str` s
    - Return Type:
        - `bytes`
    - Description:
        - Converts a base 64 `str` object to its equivalent `bytes` representation.

Serverlib

The serverlib modules is used for all of the methods involving only the authentication and resource servers.

- public_key_response
    - Parameters:
        - `RSAPublicKey` public_key
    - Return Type:
        - `dict`
    - Description:
        - Creates a response packet with success being `True` and the bytes of public_key in string form as the data.
- initialize_database
    - Parameters:
        - `str` db_filename, `str` schema_command
    - Return Type:
        - `Connection`
    - Description:

        - If a database at db_filename doesn't exist, creates a new database at that location with the SQL schema and returns it, otherwise returns the database at db_filename.
- initialize_key
    - Parameters:
        - `str` key_filename
    - Return Type:
        - `RSAPrivateKey`
    - Description:
        - If a key exists at key_filename, loads and returns the `RSAPrivateKey`, otherwise generates a new `RSAPrivateKey`, stores it at key_filename and returns it.
- bad_request_json
    - Parameters:
        - `ServerErrCode` err, `str` comment
    - Return Type:
        - `dict`
    - Description:
        - Creates a response packet with success being `False`, data being the `ServerErrCode`, and comment being the corresponding parameter.