`keyexchangestate`

This function takes two parameters - pubkey_cli and pubkey_serv.

- Pubkey_cli is an DER encoded version of the client's public key
- Pubkey_serv is an uint_8t pointer (which was already set up in lock function), which is empty but will be overwritten to contain the server's DER encoded public key
- Keyexchangestate will load the pubkey_serv variable with a public key received from the server
- SERVER IMPLEMENTATION
    - Send pubkey_cli to server
        - Why? Server needs the client's public key to generate the shared secret
    - Receive the server's public key
    - Return 1 on success

`send_unlock_info`

This function takes a few parameters. All parameters are already set up to be the proper sizes and types in the unlock function:

- OTPs - The encrypted OTP to send
- OTPs_size - The size of OTPs
- Unlock_aes_iv - The AES IV used to encrypt the OTP into OTPs
- Unlock_aes_iv_size - The size of the unlock aes iv
- OTP_tag - AES-GCM tag generated when the original OTP was encrypted into OTPs
- Server_encrypted_message - An empty buffer of size 128 which will be overwritten to contain the server's response message, which will then be validated in the unlock function
- Server_tag - AES-GCM tag for the server_encrypted_message
- SERVER IMPLEMENTATION
    - Send OTPs to the server
    - Send unlock_aes_iv to the server
    - Send OTP_tag to the server
        - At this point, the server has everything it needs to decrypt the OTPs
    - Receive the server's encrypted message
    - Receive the AES-GCM tag of that encrypted message
    - Return 1 on success

You will not need to change any of the set-up for the various arguments. As long as the server_encrypted_message and server_tag contain the server's message and relevant tag by the time the function concludes, unlock will work appropriately.

`pit_connect`

This function was used for our server implementation. It can be changed or disregarded entirely - whichever you want. It only has one argument:

- Desired_port - The desired port to connect to the server on
- SERVER IMPLEMENTATION

- Set up the connection to the server.
- Returns an int pointing to the file descriptor (socket) which can be used to send/receive from the server.