Assignment 2 - Basics of symmetric cipher and authentication

Secure file copy

- We use the EVP_ class of functions from OpenSSL library to decrypt and encrypt data.
- The server validates the HMAC signature of the received file before saving the decrypted file to its local filesystem.
- We generate the IV and key by reading bytes from /dev/urandom.

Usage:

To send file 'abc' from client on port 5000 to server listening on port 5000 and save it in 'abc1' we execute the following commands:

- client_real abc abc1 | ncat -v -p 5000 <client_ip_address>
- ncat -l -v -k -p 5000 <server_ip_address> | server_real

To test for HMAC validation we use -corrupt_data flag to corrupt the data sent by client to server. On execution, the file received by server is not saved on server's filesystem due to HMAC validation failure.

- client_real abc abc1 -corrupt_data | ncat -v -p 5000 <client_ip_address>