Task: create a file encryption/decryption/transmission suite similar to the UNIX *scp* utility, using gcrypt libraries provided by the Linux operating system. Your application will use industry-standard cryptographic algorithms and libraries. gcrypt is used to build GnuPG and can be used to develop ssh and other secure programs - it and OpenSSL are used extensively in Linux distributions.

Requirements

- The programs are to be written in C and will use the libgcrypt library. The make utility should be used to create the program.
- The file encryption programs *purenc* and *purdec* should take the following inputs:
    - purenc <input file> [-d <output IP-addr:port>] [-l] purdec [-l <input file>]
- where *purenc* takes an input file and transmits it to the IP address/port specified on the command line (-d option) or dumps the encrypted contents of the input file to an output file of the same name, but with the added extension ".pur". For example, if the input file is hello.txt, the output file should be hello.txt.pur. *purdec* should run as a network daemon, awaiting incoming network connections on the command-line specified network port. *purdec* can also be run in local mode (-l option) in which it bypasses the network functionality and simply decrypts a file specified as input. In either mode, the output should be the original name of the file, minus the .pur extension.
- On each invocation, *purenc* and *purdec* should prompt the user for a password to encrypt or decrypt the file under. The key used to encrypt the file should be computed from the password by hashing it using the PBKDF2 function. You should also attach an HMAC to the file and verify the HMAC with *purdec*. Encryption must be done using AES256.
- Both *purenc* and *purdec* should display an error and abort the operation if the output file already exists.