You are encouraged to work in groups of two or three. If you cannot find partners, you may work alone. Please submit **one** copy of the assignment using `subversion`; if you are working with partners, all names should appear in the Python code (as comments). Note that you will get a grade of zero if your program does not run.

Client $\stackrel{\text{encrypt}}{\longrightarrow}$ Server

In this assignment you are going to implement a very simple client/server in the internet domain using TCP. The client will ask for a text message — provided from the command line — it will encrypt it using a secret key, and send it to the server. The server, knowing the key, will receive the ciphertext, decrypt it, and display it on the screen.

The two programs will be invoked thus:

```
server <port_number>
```

That is, the port number will be passed to the server as an argument. You will have to create a socket, and bind the server information to this socket. On the other hand:

```
client <host_name> <port_number>
```

and this command will *prompt the user for a message*, which will then be encrypted with a (pre-established by, say, Diffie-Hellman) key K, initialization vector IV, and CBC, and transmitted to the listening server; the hostname is the server's IP, and the port number is the port that the server is listening to for incoming messages.

In your documentation you must describe how you implement CBC (Cipher-Block-Chaining); it is up to you to provide a chunk size, etc. You must provide a justification for your design.

This assignment will require a little bit of socket programming, but very basic. The server will have to get a socket file descriptor, with an assignment the style of:

```
socket_file_descriptor = socket(AF_INET, SOCK_STREAM);
```

where we use `AF_INET` to represent the address family `INET` for Internet sockets, meaning the `IPv4` protocol, and we use `SOCK_STREAM` to express that we are asking for a TCP connection.

As the code itself is not difficult, it is important that you provide good documentation that shows an understanding of what is happening.

This assignment can be very exciting; it is very satisfying to transmit, "by hand" as it were, your first Internet message. Coding messages has its own fascination. But most importantly, if you ever get a job that has a "networking" component, the material that you learn while

writing this assignment will be invaluable. Almost all networking applications build up from what you do with sockets here.

Please include a text write up of your program. That is, write a short report (a few paragraphs, included as a comment at the beginning of your code) describing how you solved the problem, how was your program tested, any problems you encountered, a sample run of the program (and an output dump of the sample run), and a justification of your design decisions. The intention is to have a basic "manual" for your program.