UNIVERSITY OF DERBY

COLLEGE OF SCIENCE AND ENGINEERING
MATHS AND COMPUTER SCIENCE

Lab Exercise 6: SMTP

Core Exercise:

At this stage you should be comfortable with implementing a client-server communication system and have some form of working encryption. This week we are going to take either your existing code base or the files in SMTP.zip and start implementing the SMTP specification. As such we will start with the following series of steps:

1. Read, understand, and comment code
    a. Practice adding comments in an appropriate style, understand the flow of the code and any limitations that it may have (e.g. parsing out incoming messages)
2. Add the core functions of SMTP ignoring state for now
    a. HELO
    b. MAIL FROM
    c. RCPT TO
    d. QUIT
3. Implement the DATA command
    a. This is the first multi-line message you will need to handle, as such you need to consider how you approach the issue carefully. At a minimum you will need a state variable that is set when you receive DATA and is unset when you receive a single "." on a new line.

Extension Exercises:

4. Modify the front end of the client to allow control
    a. Exit
    b. Login
    c. Error checking of inputs / some sort of UI
5. Determine how to add commands, and process their actions
    a. process domain
    b. check validity, create account, login etc.
6. Initiate encryption process
    a. Negotiation of a protocol and key
    b. Enable encryption

Challenge Exercises

7. Implement a hash function
    a. Review MD5, SHA1
    b. Implement simple hash function
    c. implement salt + hash for password

   d. Consider a message digest (hash of all data + control information you have received/sent)
8. Consider functions you may wish to add - my thoughts as a starting point would be
   a. LOGI <hashedPW>
   b. VMBX - return list of my mailboxes
   c. SLCT - sets current mailbox
   d. VIEW MAIL <ID> view email x in current mailbox
   e. VIEW LIST <num1> <num2> view email headers num1 to num2
   f. AUDT <num1> <num2> - view audit log entries num1 to num 2
   g. DELE MAIL <ID> delete email x in current mailbox
   h. DELE REMOTE <mailbox> <ID> - delete email x in mailbox X if I am allowed to
9. Consider what additional classes you will need –
   a. Mailbox handler?
   b. Audit manger?
   c. Authentication manager?

Additional Reading

SHA – Computerphile - https://www.youtube.com/watch?v=DMtFhACPnTY

Salting – Rackspace Technology - https://www.youtube.com/watch?v=sjEeqtZ7Tw4

Hashlib - https://docs.python.org/3/library/hashlib.html

SHA-1 Python – AH Alt - https://github.com/ajalt/python-sha1

Python RegEx – W3Schools - https://www.w3schools.com/python/python_regex.asp

Python RegEx – Corey Schafer - https://www.youtube.com/watch?v=K8L6KVGG-7o

Python GUI – Real Python - https://realpython.com/python-gui-with-wxpython/