COMP 522: Privacy and security
Lab session 6

Lecturer: Alexei Lisitsa

HMAC-SHA256 message authentication

Download, compile and run the following simple program available at the web page www.csc.liv.ac.uk/~alexei/COMP522/index.html of COMP522 course:

- HMAC-SHA256 message authentication (initMac.java)

Look into the code and see how Message Authentical Code (MAC) generation is implemented. It is in fact an implementation of the authentication scheme presented at page 6 of Lecture Notes on Message Authentication and Hash functions. More details on this authentication scheme can be found e.g. at https://en.wikipedia.org/wiki/HMAC Then try the following:

- By a simple modification of code and experiments show that indeed, it computes MAC:

  That is

  - if a Verifier uses the same secret key to initialize his/her mac object and recalculate MAC code of the same text then the result will be the same;
  - if a Verifier uses the same secret key, but calculates MAC code of a different text then the result will be different;
  - If a Verifier uses a different secret key, but calculates MAC code of the same text then ... *(complete the sentence)*.

- Compare HMAC-SHA256 with hash functions (e.g. SHA-256), and the authentication schemes considered in LAB 4, in terms which of these methods can be used to establish:

  - Message integrity;
  - Authentication (the origin of the message can be proved to the receiver);
  - Non-repudiation (the origin of the message can be proved to a third party, not only to the receiver).