Introduction to Cryptography
Lab 3

1) Try *openssl dgst* functionality with the following cryptographic hash algorithms: SHA1, SHA256, MD5. Try to digest very similar messages (e.g. 1 bit change) and observe the results.

   The following exercises require you to download Lab3Files.zip, which can be located in moodle.

2) Compare the two files using the *cmp* program. Do they differ?
   a) Perform SHA1 hash on the two files. Do the results differ?
   b) Perform MD5 hash on the two files. Do the results differ?

3) We define HMAC to be:

   $$HMAC(k1, k2, m) \ = \ H(k1 \parallel H(k2 \parallel m))$$

   Implement *HMAC* using *SHA1* as *H* (you may use the provided *SHA1* implementation).