SE 375 - Systems Programming

Laboratory Assignment #11

June 7-11, 2022

Message Authentication Code with the Server-Client Model

Your task is to manually implement a Message Authentication Code algorithm using the server-client scheme. Refer to the week 12 slides (slide no. 26) for the algorithm. The related figure can also be seen below:

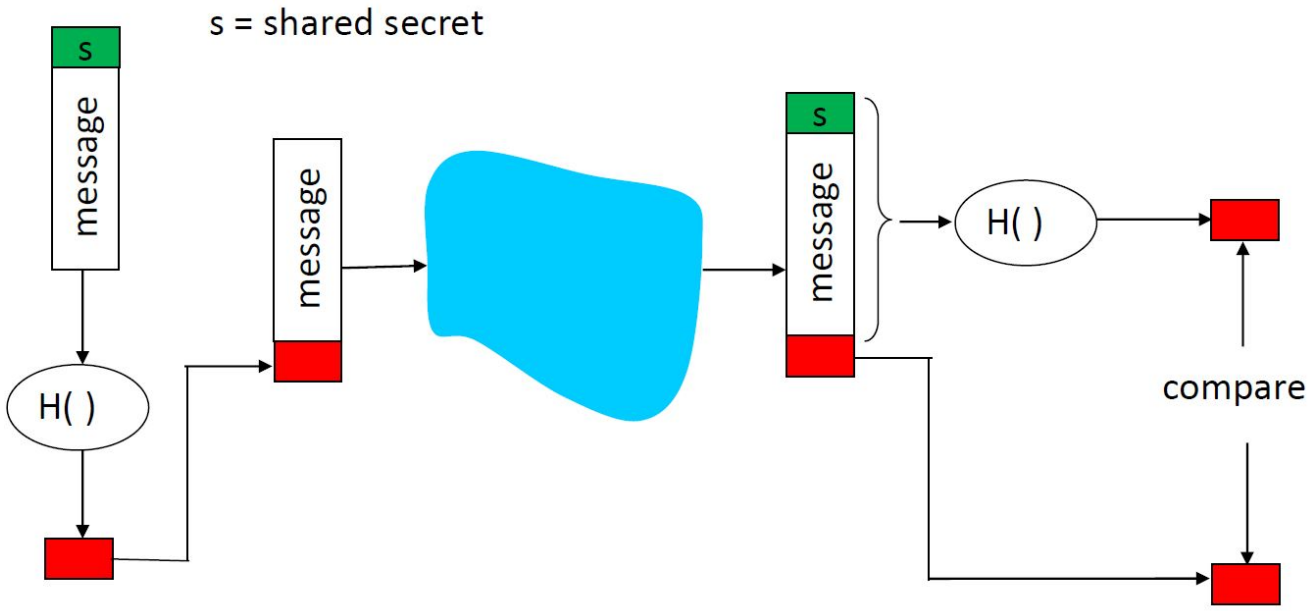

Figure 1: Message Authentication Code procedure.

Your implementation should follow these steps:

1. The server will generate a secret key & write it to a file as a byte array before connection, the client will then read this file to acquire the key.
2. After the connection has been established, the client will create a message as a string (any string is acceptable) & convert it to a byte array.
3. This byte array is going to be combined with the secret key (the ordering should be consistent across the client and the server). The key should also be converted to a byte array before this operation.
4. Using this combination, a hash is going to be computed using SHA-1 (Secure Hash Algorithm).
5. The client will finally combine the message with the hash & send this final combination to the server.
6. The server will separate the hash from the message, append the secret key to the message & compute hash.
7. Finally, the server will compare the received hash with the computed hash. If they are equal, the message is authentic.