Repo: https://github.com/JHsu01/MAC-Cheez
Version number: 2690480561ba8a654488a4fcd0bfe5a06eb7ed83

Communication protocol:

We have included the bash scripts send and receive so that Bob and Alice can send and receive their public keys and ciphertexts if needed. Alternatively, Bob and Alice can share their keys and ciphertexts manually through any authenticated channel of their choosing.

Actual Protocol:

The password files are hashed using SHA 256 to produce a message authentication code. The MAC is then encrypted using RSA public key encryption, verifying the other person's ciphertext involves comparing the two ciphertexts and comparing the two macs.

Code and spec:

Language used:

C++

Libraries used:

Cryptographic libraries: *hashlibpp, openssl*

Other miscellaneous libs: *string, pthread, stdio, unistd, stdbool, assert*

Security analysis:

Since the password files are hashed using SHA 256, the message authentication code should not reveal any information about the plaintext passwords themselves, under the assumption that sha 256 is a one way function, and is collision resistant. The message authentication is further encrypted using RSA public key encryption, this ensures that even if an adversary were able to intercept the ciphertext, they would not be able to decrypt it and obtain the message authentication code. The only person who is able to decrypt the ciphertext is the intended receiver, with their private key.

Goals:

- If Alice and Bob have different password files, they cannot convince each other that they have the same password file (because sha 256 is collision resistant).

- If Alice and Bob have the same password files, they can however, convince each other that they are different by simply using a different file. However, this would constitute a direct attack, not a passive one- and is not covered in the scope of this project (it would also be pointless).

- A passive observer cannot deduce the contents of the password files of either Alice or Bob because:

  a) they cannot obtain the message authentication code
  b) even if they were able to obtain the message authentication code, they would not be able to obtain any information about the password files.