Phase 2.1 (5 Marks)

MAC stands for Message Authentication Code and is used to detect accidental and intentional modifications of data by using a session key. A MAC requires a message and a secret key that is only known by the message creator and the intended recipients of the message. The MAC that is attached to the message being sent must be recognized and authenticated by the recipient of the message in order to be granted access.

Encryption uses an encryption algorithm and an encryption key to encode data (plaintext). The output of this process is ciphertext which can then be converted back to plaintext by using a decryption algorithm with the given key. Encryption is intended to make the information 'unreadable' to anyone that does not have the private key.

Hashing algorithms take a value and produce another generally shorter, fixed length value. Generally these values cannot be reversed. The primary function of a hash is data compression. With regards to cybersecurity, hashing algorithms provide a greater level of security for data as the resultant values cannot be decrypted by attackers due to the algorithms' irreversible nature.

Hash-then-encrypt works by using a hash function to create a hash key for the plain text. The plain text is then encrypted and the hash is appended to the cipher text. Once the recipient decrypts the cipher text they can use the same hash function which should produce the same key as the original. If it does not then they know that the data has been tampered with in transmission.

MAC-then-encrypt works by calculating the MAC on the plain text, appending it to the data and then encrypting all of the data. The downside is that we do not know if the cipher text is authentic until it has been decrypted, leaving an unauthenticated attacker with the power to decrypt and discover the plaintext and/or alter the plaintext.

Encrypt-then-MAC works by first encrypting the plain text and then calculating the MAC based on the resulting ciphertext. Calculating the MAC on the cipher text allows recipients to determine if the ciphertext has been tampered with while in transmission.

Encrypt-and-MAC works by calculating the MAC on the plain text, encrypting the plain text and appending the MAC to the cipher text. This method allows for authenticity of plain text to be confirmed but not the authenticity of the cipher text. The downside to this approach is that the MAC address could be used to reveal information about the plain text as the MAC was calculated based on the plain text.

Comparison and conclusion

The pros and cons of each of the four methods have been discussed above. For our project we will be implementing the Encrypt-then-MAC technique as it offers a slightly increased level of security in comparison to other techniques in that no part of the plaintext is revealed through MAC as it would be calculated from the ciphertext. Furthemore, it simultaneously allows for the data to be authenticated before decryption has occurred, allowing for the verification of the message to take place prior to decrypting the ciphertext.

References:

MAC:
https://www.techtarget.com/searchsecurity/definition/message-authentication-code-MAC#:~:text=A%20message%20authentication%20code%20
Encryption:
https://www.microfocus.com/en-us/what-is/encryption
Hash:
https://www.techtarget.com/searchdatamanagement/definition/hashing#:~:text=Hashing%20is%20the%20process%20of,the%20implementation%20of%20hash%20tables.

https://crypto.stackexchange.com/questions/202/should-we-mac-then-encrypt-or-encrypt-then-mac