Shuoting Kao sk4920

COMSW4181_001_2021_3 - SECURITY I HW1

Problem 1: Adversarial Thinking (10 points)

(a) Which of the following best describes the difference between MAC and digital signatures?

(4) While a digital signature can be verified using the public key of the signer, message authentication codes can only be verified through the secret key that was used to generate them.

I choose (4) since the digital signature should be verified with the public key. Its key is an asymmetric type. The digital signature is generated with a private key, and we can verify it with the public key. On the contrary, MAC's key is symmetric, so we can verify the message only by using the same key to encrypt the message, like our programming part2.